BINGHAM CENTRE FOR THE RULE OF LAW

New Zealand Independent Review of Intelligence and Security

Response by the Bingham Centre for the Rule of Law

Lawrence McNamara & Justine Stefanelli

Response by the Bingham Centre for the Rule of Law, 13 August 2015

www.binghamcentre.biicl.org

CONTENTS

A. Introduction

1. This submission primarily addresses the Review's interest in international and comparative experience with intelligence and security by providing materials relevant to the UK, with a view to, particularly, paragraphs 2 and 10 of the Review's terms of the reference.

2. The Bingham Centre for the Rule of Law was launched in December 2010 and is an independent research institute devoted to the study and promotion of the rule of law worldwide. Its focus is on understanding and promoting the rule of law; considering the challenges it faces; providing an intellectual framework within which it can operate; and fashioning the practical tools to support it. The Centre is named after Lord Bingham of Cornhill KG, the pre-eminent judge of his generation and a passionate advocate of the rule of law. It is part of the British Institute for International and Comparative Law, a registered charity based in London.

3. The Bingham Centre has undertaken a range of work relating to national security and the rule of law, particularly in the UK. This submission brings together parts of that work that may be of particular relevance to the NZ Independent Review.

4. This submission was prepared by Dr Lawrence McNamara, Senior Research Fellow and Deputy Director of the Bingham Centre for the Rule of Law, and Justine Stefanelli, Maurice Wohl Associate Senior Research Fellow in European Law at the Bingham Centre for the Rule of Law.

B. Oversight mechanisms: parliamentary, executive and judicial

5. Oversight of security and intelligence agencies is, of course, a fundamental component of transparency and accountability with regard to the activities of the state. The Independent Review's terms of reference (paragraph 2) envisage, appropriately, a breadth of mechanisms at work in oversight, referring as they do to safeguards at operational, judicial and political level.

6. A broad base of oversight mechanisms is both welcome and important. The use of parliamentary committees (however constituted) is a familiar and important issue in this area, and will inevitably and rightly be a key focus of the Review. However, there are numerous other important – at least equally important and possibly moreso in some circumstances – mechanisms and processes which enhance and promote transparency and accountability of the agencies, and help to ensure that states and their agencies comply with their legal obligations. In the UK, the most significant debates in recent years have revolved around matters including:

    - Parliamentary oversight processes
    - Judicial oversight, both of the issuing of warrants and through legal actions at the Investigatory Powers Tribunal

- The value of independent inquiries (eg, conducted by a judge, a retired judge, senior lawyer or retired civil servant), and
- Actions in the civil courts and the procedures which govern the use of security-sensitive matters in those actions.

We address all four of these areas below.

7. In this submission we provide the Review with material that we hope it will find of assistance, in line with its tasks under paragraphs 2 and 10 of its terms of reference. With the exception of our submission to the New Zealand Law Commission, the following material relates to UK experience and does not speak directly to the New Zealand context. However, given the strong parallels between the jurisdictions and issues involved, and the close consideration of these matters by the Bingham Centre, we hope the materials will assist the Review in its work.

8. The following paragraphs provide links to a range of published material by the Bingham Centre and the authors of this submission. We have attached as appendices three pieces that may be of most relevance to the Review's work.

C. Parliamentary oversight

9. The Bingham Centre has examined parliamentary oversight of the UK agencies on three occasions that may be of particular interest.

   a. **Submission to the Cabinet Office Consultation on the Justice and Security Green Paper** (6 January 2012)

      This submission covers almost the full range of matters raised by the 2011 Green Paper. The parts relevant to parliamentary oversight are at:

      - Paragraphs [71]-[80]
      - Recommendations 14-15 (page 30).

      Issues of relevance to the New Zealand review may include points relating to the make-up of the panel, appointment of membership, and access to materials, compellability of witnesses, and decisions about reporting.

      Document:

      Bingham Centre Submission to the Cabinet Office Consultation on the Justice and Security Green Paper
      Available at: http://bit.ly/1L8oOzz

   b. **Detention, Interrogation and Security: Oversight and Accountability** (5 March 2015)

      This panel debate, which was convened by the Bingham Centre, brought together a group of experts to consider the implications for the UK of the

United States Senate Select Committee on Intelligence report on the CIA's detention and interrogation programme, published in December 2014. The panellists were:

- The Rt. Hon. Sir Malcolm Rifkind QC MP, Intelligence and Security Committee, Parliament
- Sir Daniel Bethlehem KCMG QC, 20 Essex Street and former principal Legal Adviser of the UK Foreign & Commonwealth Office
- Clare Algar, CEO, Reprieve
- Professor John Gearson, Professor of National Security Studies & Director, Centre for Defence Studies, King's College London
- Sapna Malik, Partner, Leigh Day

The discussion elicited different views about the best and most effective mechanisms for oversight and accountability.

The summary report of the event provides a detailed summary of panellist comments.

The publication by McNamara & Stefanelli provides an analysis of the views and identifies the five core issues that emerged and which are contentious.

Documents

- *Bingham Centre summary report of event*
  Available at: http://bit.ly/1J1PECP

- *L McNamara & J Stefanelli, 'CIA Interrogations: What have we learned in the UK', UK Human Rights Blog, 3 April 2015*
  Available at: http://bit.ly/1NsGwLv

The McNamara & Stefanelli piece is attached to this submission as Appendix A.

c. **Submission to the UK Investigatory Powers Review** (October 2012)

The Bingham Centre made a major submission to the most recent UK review of investigatory powers (the review by the Independent Reviewer of Terrorism Legislation, David Anderson QC, the report of which, *A Question of Trust*, was published in July 2015). Issues relating to parliamentary oversight are at:

- Paragraph [54]
- Recommendation x (page 28).

Document

Bingham Centre submission to the UK Investigatory Powers Review (October 2014):

Available at: http://bit.ly/1r8e5fQ

The submission is attached to this submission as Appendix B.

D. Judicial and executive oversight of investigatory powers

10. The Bingham Centre's submission to the UK Investigatory Powers Review was informed by an expert event attended by over 80 people working the in the field. It considered a wide range of areas related to investigatory powers and the oversight and accountability of the agencies that exercise them, including the following:

    - Investigatory powers and the rule of law
    - A single comprehensive statutory framework
    - Interception of communications
    - Communications data
    - Intrusive surveillance, directed surveillance and covert sources
    - Encryption keys
    - Oversight
    - Retention of communications

    The submission made a range of recommendations with respect to all these matters.

11. The Bingham Centre's submission may be of particular relevance to the New Zealand Review's consideration of its terms of reference in paragraph 4 regarding private communications, as well as the wider issues under other parts of the terms of reference.

The adoption of the Bingham Centre's recommendations by the UK Independent Review

12. The Bingham Centre's recommendations were well received by the UK Independent Reviewer. Among the issues of particular note, Mr Anderson QC followed the Bingham Centre's proposals when he recommended the replacement of the existing oversight Commissioners with a single comprehensive oversight body, more clearly drafted legislation governing surveillance powers, greater scope for the oversight body to refer cases to the Investigatory Powers Tribunal, and the introduction of a right of appeal from the Tribunal on points of law.

Document

Bingham Centre submission to the UK Investigatory Powers Review (October 2014):
Available at: http://bit.ly/1r8e5fQ

The submission is attached to this submission as Appendix B.

E. Independent inquiries

13. In the **Detention, Interrogation and Security: Oversight and Accountability** debate on 5 March 2015, there was much discussion over the issue of whether a judge-led inquiry would be more effective than an inquiry led by the Intelligence and Security Committee of Parliament (ISC).

14. As we explained in *CIA Interrogations: What have we learned in the UK* (cited above in paragraph 9b) the ISC has been criticised in the past, for example, in relation to the Binyam Mohamed case where the ISC did not discover some relevant evidence and nor was it given that evidence. This led to claims that it had been misled by MI5. However, under the Justice and Security Act 2013 the ISC acquired new powers: intelligence agencies cannot refuse to provide information, the ISC can enter premises at Thames House, GCHQ, Vauxhall, etc., to examine information; and the ISC has oversight of operations in addition to policy, resources, and administration. These changes could arguably remedy the earlier shortcomings, though considerable doubts were still expressed about whether they were sufficient to make the ISC an adequate and appropriate investigatory body. On the other hand, a judge-led inquiry would have the advantage of independence, and the perception of impartiality, plus the ability to compel witnesses. However, there was still no certainty that a judicial vehicle would solve all concerns.

Documents

- *L McNamara & J Stefanelli, 'CIA Interrogations: What have we learned in the UK', UK Human Rights Blog, 3 April 2015*
  Available at: http://bit.ly/1NsGwLv

- *R (Mohamed) v Secretary of State for Foreign & Commonwealth Affairs* [2009] EWHC 152 (Admin) (04 February 2009)
  Available at:
  http://www.bailii.org/ew/cases/EWHC/Admin/2009/152.html

- *D Leigh and R Norton-Taylor, 'Binyam Mohamed: How MI5 misled parliament's intelligence and security committee', The Guardian (11 February 2010)*
  Available at: http://bit.ly/1IKd02W

- *Justice and Security Act 2013*
  Available at:
  http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted

  The McNamara & Stefanelli piece is attached to this submission as Appendix A.

F. Special jurisdictions: the Investigatory Powers Tribunal

15. The Bingham Centre submission to the Independent Review of Investigatory Powers (cited above in paragraphs 9-12) addressed the special jurisdiction of the UK Investigatory Powers Tribunal. The relevant parts of the submission are:

    - Paragraphs [47]-[53]
    - Recommendation ix (page 28).

16. While these paragraphs and the recommendations are obviously specific to the UK context, they may be of interest to the New Zealand Review with regard to the analysis of the extent to which the tribunal does and does not provide an adequate safeguard and the types of substantive and procedural protections which would see safeguards comply with the rule of law and protect individual rights.

Document

Bingham Centre submission to the UK Investigatory Powers Review (October 2014), available at: http://bit.ly/1r8e5fQ

The submission is attached to this submission as Appendix B.

G. Established jurisdictions: closed material proceedings in civil cases – the Justice and Security Act

17. The use of traditional legal processes has come under increasing scrutiny in recent years. In the UK there was great debate surrounding the expansion of the use of closed material proceedings into civil cases, in the context of the Justice and Security Act 2013.

18. The Bingham Centre's submission to the New Zealand Law Commission consultation on national security information in proceedings (June 2015) largely covered these issues, but it may also be helpful to consult some of our other commentary in this area. In particular, our review of the First Report by the Secretary of State after the Act had been in force for one year provides an analysis of the adequacy of the legislative requirements with regard to reports to parliament and of the approach taken to reporting.

Documents

- *Bingham Centre submission to the New Zealand consultation*
  Available at: http://bit.ly/1Nd1wYO

- *Bingham Centre, Closed Material Procedures under the Justice and Security Act 2013: A Review of the First Report by the Secretary of State*
  Available at: http://bit.ly/1kaOwqs

- *Lawrence McNamara, 'The Rise of Closed Material Procedures: The Rise of the Secret Trial One Year On', UK Human Rights Blog, 5 August 2014*
  Available at: http://bit.ly/1ulWbD8

19. As a part of the Justice and Security Act, the ***Norwich Pharmacal* jurisdiction** was considered at Green Paper stage (eg, paras 1.14-1.46 of the Green Paper) and in the early formulation of the Bill. Early proposals suggested a blanket immunity whereas later proposals (including, ultimately, the Act) moved to the use of closed material proceedings.

20. With regard to background, law, principles and evidence relating to these proposals, the Centre's submission to the Cabinet Office Consultation on the Justice and Security Green Paper (cited above in paragraph 9a) may be of interest to the Review. These issues are addressed at paragraphs [65]-[70] and recommendations 12 & 13 (at pages 29-30.

Document:

Bingham Centre Submission to the Cabinet Office Consultation on the Justice and Security Green Paper
Available at: http://bit.ly/1L8oOzz

UK Human Rights Blog

APRIL 3, 2015 BY 1 CROWN OFFICE ROW

CIA Interrogations: what have we learned in the UK?

(https://adam1cor.files.wordpress.com/2015/04/12fb9b780ea5561b0f8a349056f9ac2b_400x400.jpg)When late last year the US Senate Select Committee on Intelligence published parts of its 6,700 page report (http://www.intelligence.senate.gov/study2014/executive-summary.pdf) on the CIA's detention and interrogation programme, it shed light – remarkable light – on how the 'war on terror' had been conducted by the US for some time.

It very rightly prompted questions for this country. The most immediate and top level question was, if that is what the US did, what did Britain do? But one need barely scratch the surface of the matter before encountering some difficult questions about method – how do we find out what Britain did? – and about scrutiny – are there lessons to be learned about oversight and accountability?

We review here some of the expert opinions and highlight five issues that, if the experts are right, are likely to lie at the heart of debate for some time to come.

Early this month the Bingham Centre for the Rule of Law convened a public event that asked an expert panel to consider these issues. Headlining the event was Sir Malcolm Rifkind QC, until recently Chair of the Intelligence and Security Committee of Parliament. He was joined by two lawyers, Sapna Malik from Leigh Day and Clare Algar from Reprieve (both of whom had represented Guantanamo detainees), and John Gearson, former Ministry of Defence adviser and now Professor of Security Studies at King's College London. Sir Daniel Bethlehem QC, former principal Legal Adviser to the Foreign & Commonwealth Office, chaired the event.

The panel was asked to consider three issues: the extent to which the SSCI Report contributes to our own body of knowledge about detention and interrogation programmes, the appropriate response for the UK Government and Parliament to the findings of the Report, and mechanisms for accountability and oversight of UK counter-terrorism law and practice.

While a detailed summary of the presentations and Q&A (http://binghamcentre.biicl.org/documents/527_bingham_centre_event_detention_report_-_final.pdf) is available on the Bingham Centre website, and panellists' views varied in scope and perspective, to our eyes five points stood out among the many matters discussed.

1. Torture affects the tortured and the torturers. The Senate Select Committee's Report (SSCI Report) not only focused on harm to/impact upon detainees as a result of enhanced interrogation, but it also demonstrated that negative effects were felt by the CIA agents who were involved in the torture programmes. In particular, the account of Abu Zubaydah's treatment demonstrated both the effect of torture on Mr Zubaydah and its effect on agents/officers involved in it, and their internal opposition to what was happening.
2. There are substantive questions that remain unanswered in the UK. The panel agreed that several issues in the UK public domain remained to be investigated: the questions raised in Sir Peter Gibson's Detainee Inquiry report (http://www.detaineeinquiry.org.uk/); the extent of UK knowledge of the use of torture techniques; the monitoring and treatment of detainees involved in operations with the US; UK involvement in rendition programmes; and the extent to which UK officials may have been complicit.
3. There was little agreement about the best method for finding answers to those unanswered questions. In particular, there was disagreement about whether a judge-led inquiry or the Intelligence and Security Committee of Parliament (ISC) would be more effective. It was noted that the ISC has been criticised in the past, for example, in relation to the Binyam Mohamed case (http://www.bailii.org/ew/cases/EWHC/Admin/2009/152.html) where the ISC did not discover some relevant evidence and nor was it given that evidence. This led to claims that it had been misled by MI5 (http://www.theguardian.com/world/2010/feb/11/binyam-mohamed-mi5-misled-intelligence-committee). However, under the Justice and Security Act 2013 (http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted) the ISC acquired new powers: intelligence agencies cannot refuse to provide information, the ISC can enter premises at Thames House, GCHQ, Vauxhall, etc., to examine information; and the ISC has oversight of operations in addition to policy, resources, and administration. These changes could arguably remedy the earlier shortcomings, though considerable doubts were still expressed about whether they were sufficient to make the ISC an adequate and appropriate investigatory body. On the other hand, a judge-led inquiry would have the advantage of independence, and the perception of impartiality, plus the ability to compel witnesses. However, there was still no certainty that a judicial vehicle would solve all concerns.
4. Context does not mitigate or excuse lapses in oversight, accountability or legality, but an examination of context is important because it helps us understand policymakers at the time. The context of the situation from a policy perspective was discussed, to better understand the actions and strategies – including the failures and wrongdoings – adopted in responding to terrorism. It was suggested that desperation and lack of knowledge of the intelligence agencies concerning the nature, threat and the appropriate response contributed to the intelligence-gathering policies. Professor Gearson's contribution from a non-legal perspective added value to the legal discussion and highlighted that, although an understanding of context is clearly of great importance, context should not – the point is worth restating – serve as a mitigating factor used to excuse lapses in oversight, accountability or legality.
5. While the ISC or an inquiry should be able to look effectively at what happened in the past, there is not presently an adequate mechanism for operational oversight of current ongoing activity. Oversight and accountability of ongoing activity featured prominently in debate by the panel. Among the issues raised were the role of the media in uncovering information, whether the

investigations themselves are too politicised to be truly independent, and how oversight sits with the "five eyes" intelligence system when allies (Australia, Canada, New Zealand, UK, US) have different moral and legal contexts to their powers.

Prior to an inquiry in the UK, we must first await the conclusion of a number of pending criminal investigations. It remains to be seen whether an inquiry will be judicial in nature or handled by the ISC, or indeed if such an inquiry will be held at all.

But whatever the answers to the substantive questions that remain for the UK, it is very clear that questions about how we will find out about Britain's conduct – past and present – are profoundly important, but there is little agreement about how they should be answered.

The full summary of the Bingham Centre event (http://binghamcentre.biicl.org/documents/527_bingham_centre_event_detention_report_-_final.pdf) is available on the Centre's website.

Justine Stefanelli and Lawrence McNamara are Research Fellows at the Bingham Centre for the Rule of Law. Jack Kenny is an intern at the Bingham Centre.

This entry was posted in In the news. Bookmark the permalink.

6 thoughts on "**CIA Interrogations: what have we learned in the UK?**"

l8in | **April 3, 2015 at 5:20 pm**

Reblogged this on L8in.

0

1

i
Rate This

daveyone1 | **April 4, 2015 at 12:12 am**

Reblogged this on World4Justice : NOW! Lobby Forum..

0

1

i
Rate This

BINGHAM CENTRE FOR THE RULE OF LAW

THE INVESTIGATORY POWERS REVIEW BY THE INDEPENDENT REVIEWER OF TERRORISM LEGISLATION

Submission by the Bingham Centre for the Rule of Law

November 2014

www.binghamcentre.biicl.org

Bingham Centre for the Rule of Law
Submission to the Investigatory Powers Review
November 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Bingham Centre for the Rule of Law welcomes the review of investigatory powers by the Independent Reviewer of Terrorism Legislation under Section 7 of the Data Retention and Investigatory Powers Act 2014 (DRIPA). The Centre's written evidence has been authored by Dr Eric Metcalfe, a Fellow of the Bingham Centre. The response draws on contributions made by experts on investigatory powers during a seminar organised by the Centre on 1 October 2014.

The Bingham Centre acknowledges that the government has a particular responsibility to protect the public from serious crime, including acts of terrorism. It therefore also accepts that in narrowly-defined and exceptional circumstances the police and intelligence services will require the power to intercept private communications, access communications data and other intrusive surveillance. In such circumstances, the need for secrecy will necessarily involve some curtailment of both the right to a fair hearing and the right to an effective remedy of those affected by the surveillance. Nonetheless, the government does not enjoy an unlimited discretion to undertake surveillance. On the contrary, the highly exceptional nature of investigatory powers means that it is all the more important to ensure that the prevailing legal framework in respect of such powers complies with the rule of law. In particular, the law must be accessible and sufficiently certain, provide adequate protection for fundamental rights and comply with the United Kingdom's obligations under international law.

At present, the Bingham Centre has concerns about the extent to which the statutory framework governing investigatory powers falls short of these benchmarks. Accordingly, this response makes a number of recommendations that are all directed towards enhancing adherence to the rule of law and our common law constitution. It makes recommendations about the framework under the Regulation of Investigatory Powers Act 2000 (RIPA), specifically with respect to the interception of communications, the use of intercept evidence, communications data, intrusive surveillance, encryption keys, and oversight. It also makes recommendations with respect to data retention under DRIPA.

Our recommendations are:

(i) A single, comprehensive statutory framework should govern the use of intrusive surveillance powers by public bodies. In particular, no public body should have the power to access communications data save by way of this framework.

(ii) Judicial authorisation should be required before any public body intercepts communications, accesses communications data, uses intrusive surveillance (including a covert human intelligence source), issues an encryption notice or a retention notice. The authorising judge should also have the power to direct the appointment of a special advocate to represent the interests of the subjects of surveillance in appropriate cases.

(iii) The existing power to intercept external communications under section 8(4) RIPA should be repealed. At the very least it should be severely curtailed. All warrants and

authorisations must be founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity.

(iv) The statutory definition of 'intrusive' surveillance should be tightened to include *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy.

(v) The ban on the use of intercept material as evidence in criminal and civil proceedings should be lifted.

(vi) The number of public bodies able to access communications data should be curtailed.

(vii) The oversight functions currently discharged by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner should be combined into a single statutory oversight body. This body's remit should include oversight of the use of all surveillance powers by public bodies.

(viii) Any person who has been the subject of covert surveillance by a public body should be notified of that fact within a reasonable period following the conclusion of the surveillance, unless a judge is satisfied that that individual's right to an effective remedy is outweighed some specific investigative need that would otherwise be prejudiced by the disclosure.

(ix) The Investigatory Powers Tribunal should be granted the power to appoint special advocates to represent the interests of excluded parties, as well as make a declaration of incompatibility under section 4 of the Human Rights Act. Its procedural rules should also be relaxed to allow much greater disclosure to complainants who have been the subject of surveillance, in order that they may bring an effective challenge. This should include sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded. The unsuccessful party should also have the right of appeal to the Court of Appeal on a point of law.

(x) The statutory requirement that candidates for the Intelligence and Security Committee must first be nominated by the Prime Minister in order to be eligible for election should be repealed, as should the power of the Prime Minister to prevent the Committee from publishing material that it considers to be in the public interest to disclose.

INTRODUCTION

1. The Bingham Centre for the Rule of Law welcomes the review of investigatory powers by the Independent Reviewer of Terrorism Legislation under section 7 of the Data Retention and Investigatory Powers Act 2014 (DRIPA). The Centre's response is authored by Dr Eric Metcalfe (Fellow of the Bingham Centre) but also draws upon contributions from experts in a seminar organised by the Centre on 1 October 2014 and has input from senior Bingham Centre staff. The 1 October seminar programme and list of attendees is attached as an appendix.

About the Bingham Centre

2. The Bingham Centre for the Rule of Law was launched in December 2010 and is devoted to the study and promotion of the rule of law worldwide. Its focus is on understanding and promoting the rule of law; considering the challenges it faces; providing an intellectual framework within which it can operate; and fashioning the practical tools to support it. The Centre is named after Lord Bingham of Cornhill KG, the pre-eminent judge of his generation and a passionate advocate of the rule of law. It is part of the British Institute for International and Comparative Law, a registered charity based in London.

3. The Bingham Centre has a particular interest and expertise in the law governing investigatory powers. Indeed, Lord Bingham himself served as the Interception of Communications Commissioner from 1992 to 1993, although under the statutory framework that preceded the Regulation of Investigatory Powers Act 2000 (RIPA). Among the Bingham Centre's current projects is a review of the law governing the use of intercept material as evidence and on 19 September 2014 the First-Tier Tribunal (Information Rights) upheld the Centre's appeal under the Freedom of Information Act 2000 against the Home Office's refusal to disclose legal advice on this issue.[1] The Centre also held an expert seminar on the investigatory powers review on 1 October 2014 in the London offices of Macfarlanes LLP.

INVESTIGATORY POWERS AND THE RULE OF LAW

4. As a starting point, the Bingham Centre acknowledges that the government has a particular responsibility to protect the public from serious crime, including acts of terrorism.[2] Although this submission does not address "current and future threats to the United Kingdom" (s7(2)(a)), it nonetheless proceeds on the assumption that the United Kingdom will continue to face grave threats to its national security and the safety of its public.

5. On the same basis, the Bingham Centre accepts that the police and intelligence services will - in certain, narrowly-defined and exceptional circumstances - continue to require the power to intercept private communications, access communications data, together with other forms of intrusive surveillance such as the use of covert sources and the power to demand encryption

[1] *Bingham Centre for the Rule of Law v Information Commissioner* [2014] UKFTT 2014/0097 (GRC).

[2] See e.g. the judgment of the European Court of Human Rights in *Öneryildiz v Turkey* (2005) 41 EHRR 20 in which the Grand Chamber held that the right to life under Article 2 ECHR requires governments to "put in place a legislative and administrative framework designed to provide effective deterrence against threats to the right to life" (para 89).

keys. As the European Court of Human Rights held in *Klass v Germany,* "the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[3]

6. The Bingham Centre also recognises that the very effectiveness of covert surveillance depends upon it remaining secret while it is being carried out, and that this secrecy necessarily involves some curtailment of both the right to a fair hearing and the right to an effective remedy of those affected by the surveillance.[4] The necessity of this interference, however, does not mean that the government enjoys an "unlimited discretion" to undertake surveillance.[5] On the contrary, the highly exceptional nature of such powers means that it is all the more important to ensure that the legal framework for investigatory powers complies with the rule of law, including in particular that it must be accessible and sufficiently certain, provide adequate protection for fundamental rights and comply with the United Kingdom's obligations under international law.[6] In our view, these are the benchmarks against which the adequacy of the existing law should be assessed.

THE EXISTING LAW GOVERNING INVESTIGATORY POWERS

7. Although s7(1) DRIPA requires the Home Secretary to appoint the Independent Reviewer "to review the operation and regulation of investigatory powers", the term "investigatory powers" is itself nowhere defined, either in DRIPA, RIPA or elsewhere. On its face, it is an extremely broad term, suggesting any statutory power that may be used by a public body for the purposes of investigation. While in practice it is generally understood as synonymous with "surveillance powers", this only begs the question of how "surveillance" is defined. Even taking a narrow definition of "surveillance", e.g. the *covert* use of statutory powers to collect *private* information about an individual, it is apparent that this would include a great many statutory powers outside either RIPA or DRIPA. For instance:

   (a) Section 94(1) of the Telecommunications Act 1984 allows the Secretary of State to give directions to telecommunications service providers "in the interests of national security or relations with the government of a country or territory outside the United Kingdom";

[3] *Klass v Germany* (1980) 2 EHRR 214 at para 48.

[4] See e.g. *Klass* at para 55: "the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge." See also Lord Neuberger's reference in *In re McE* [2009] UKHL 15 to certain "inherent paradoxical problems" involved in surveillance, one of which is that the authorities "cannot warn the parties in advance that interception or listening in will or will not occur, as to do so would defeat the whole point of the exercise" (para 111).

[5] C.f. *Klass* at para 49: the latitude afforded to domestic legislatures "does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

[6] See e.g. Tom Bingham, *The Rule of Law* (Penguin, 2010), Part 2, pp37-129.

(b) Part III of the Police Act 1997 provides a framework for authorising interference by police with private property, including the use of surveillance devices;

(c) A number of statutes grant public bodies power to access communications data in certain circumstances, including the Police and Criminal Evidence Act 1984, the Social Security Fraud Act 2001, the Charities Act 1993, the Criminal Justice Act 1987, the Environmental Protection Act 1990, the Financial Services and Markets Act 2000 and the Health and Safety at Work Act 1974;[7]

(d) Section 1(5)(c) RIPA similarly provides for the power of public bodies to intercept stored communications without a warrant by way of "*any statutory power* that is exercised … for the purpose of obtaining information or of taking possession of any document or other property";

(e) Although the Data Retention (EC Directive) Regulations 2009 (SI 2009/859) have now been superseded by Part 1 of DRIPA, the power of the Secretary of State to provide codes of practice for the retention of communications data continues to be set out in Part 11 of the Anti-Terrorism Crime and Security Act 2001.

8. For practical reasons, this submission has focused primarily on those powers contained in RIPA and DRIPA. In our view, however, it is clear that there is a broader need for a coherent and, ideally, comprehensive statutory framework governing the use of covert surveillance powers in general.[8]

Interception of communications

Authorisation

9. The Bingham Centre does not doubt the diligence and conscientiousness of the Secretaries of State in issuing interception warrants nor does it have cause to dispute the candour and integrity

[7] Section 1(6) DRIPA now provides that a public telecommunications operator who retains relevant data under Part 1 of DRIPA must not disclose it except in accordance with an authorisation under Chapter 2 of Part 1 of RIPA, "a court order or other judicial authorisation or warrant" or as provided by regulations made under s1(3) DRIPA.

[8] See e.g. the Report of the Newton Committee of Privy Counsellors on the Anti-Terrorism Crime and Security Act 2001 (HC100, December 2003) at para 406: "we recognise that the need to retain communications data for terrorism and other serious crimes creates the potential for other use or abuse of that data. The protection provided by the Regulation of Investigatory Powers Act is a step in the right direction where it applies, but a coherent legislative framework governing both retention of, and access to, communications data seems to be the only way of providing a comprehensive solution to this issue"; and Lord MacDonald QC, *Review of Counter-Terrorism and Security Powers* (Cm 8003, January 2011) at p7: "although RIPA is the principle legal framework under which communications data may be acquired, there is a wealth of other statutes under which local authorities may also acquire such data. The Review has found that these were mostly not designed with the acquisition of communications data in mind, so that they contain significantly fewer safeguards. This is a very unsatisfactory situation and it needs to be addressed with real urgency if public confidence is to be maintained".

and of those applying for such warrants.[9] We nonetheless consider that it is constitutionally inappropriate for the Secretary of State to have the final say in issuing interception warrants. In their evidence before the Intelligence and Security Committee, the Home Secretary and the Foreign Secretary both stressed the need for democratic accountability in issuing interception warrants, so that government ministers remained answerable for the warrants they issued and could be removed by way of the ballot box if necessary.[10] Yet it is very difficult to see how this could ever be the case. For a start, s17 RIPA prohibits any evidence being adduced in any court or tribunal that would even "tend ... to suggest" that an interception warrant has been made.[11] Secondly, s19 RIPA provides that it is a criminal offence for any person "holding office under the Crown", any member of staff of an intercepting agency or communications service provider, among others, to disclose the existence of an interception warrant unless authorised to do so for certain limited purposes, none of which appear to entail disclosure to Parliament or the public at large.[12]

10. Indeed, in the nearly thirty years since the power to intercept communications has been put on a statutory footing, we are not aware of a single instance in which it was revealed that a government minister signed a particular interception warrant, still less that any minister has ever appeared before Parliament or any court or tribunal or inquiry to account for having done so. In our view, this is because the same secrecy that rightly attaches to the interception of communications by police and intelligence services also prevents meaningful democratic accountability for the Secretary of State's decision to authorise such interception in particular cases.

---

[9] Having said that, we note that concerns have been raised at times; see the remarks of Lord Neuberger in *R(Binyam Mohamed) v Secretary of State for the Foreign and Commonwealth Affairs* [2010] EWCA Civ 65 at para 168, concerning the preparation of public interest immunity certificates: "as the evidence showed, some Security Services officials appear to have a dubious record relating to actual involvement, and frankness about any such involvement, with the mistreatment of Mr Mohamed when he was held at the behest of US officials. I have in mind in particular witness B, but the evidence in this case suggests that it is likely that there were others. The good faith of the Foreign Secretary is not in question, but he prepared the certificates partly, possibly largely, on the basis of information and advice provided by Security Services personnel. Regrettably, but inevitably, this must raise the question whether any statement in the certificates on an issue concerning the mistreatment of Mr Mohamed can be relied on, especially when the issue is whether contemporaneous communications to the Security Services about such mistreatment should be revealed publicly. Not only is there some reason for distrusting such a statement, given that it is based on Security Services' advice and information, because of previous, albeit general, assurances in 2005, but also the Security Services have an interest in the suppression of such information."

[10] "Theresa May's evidence to the intelligence and security committee", by Andrew Sparrow, *The Guardian,* 16 October 2014; "Ministers should assess UK surveillance warrants, says Philip Hammond" by Julian Borger, *The Guardian*, 23 October 2014: "'Perhaps it is a feature of the times that we live in, but I'm sure I can speak for all my colleagues who sign warrants that we all have, in the back of our minds, that at some point in the future we will – not might be, but will – be appearing before some inquiry or tribunal or court to account for the decisions we've made', Hammond said."

[11] Section 18 RIPA provides for certain exceptions to this, yet it is notable that almost all of these relate to courts and tribunals with the power to hold closed proceedings and which are generally under a duty to prevent the disclosure of information contrary to the public interest.

[12] Although s19(9) grants the Interception of Communications Commissioner the power to authorise disclosure, he reports in the first instance to the Prime Minister (s58(4)) who in turn may exclude material contained in the Commissioner's report from being laid before Parliament if he considers that it would be contrary to the public interest for reasons of national security, et al.

11. Moreover, it is generally the case that the Secretary of State who considers an application for a warrant from an intercepting agency is the same person who is accountable to Parliament for its performance, e.g. the Foreign Secretary in the case of MI6 and GCHQ; the Home Secretary in the case of the National Crime Agency, MI5 and the Metropolitan Police; and so forth.[13] There is, therefore, an inevitable risk that, when considering whether to grant an interception warrant, the Secretary of State may give undue weight to broader political considerations at the expense of the fundamental rights of those affected by the surveillance. This risk is especially serious in cases involving the threat of terrorism, and where the rights in question are those of unpopular minorities.[14] In a 2009 case involving directed surveillance of privileged conversations between lawyers and persons in custody, for instance, Lord Neuberger expressed concern at the possibility "that the Government has been knowingly sanctioning illegal surveillance for more than a year".[15] Despite this adverse comment, however, there is no indication that the government faced any public outcry or parliamentary censure as a result of this failing.

12. Even where democratic accountability of surveillance decisions *is* possible (i.e. because authorisations for directed surveillance, unlike interception warrants, may sometimes be disclosed), as the case of *In re McE* shows, the rights of unpopular minorities may be vulnerable where the decision to authorise surveillance is left to the executive. As the ECtHR held in *Klass*:[16]

> *The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.*

---

[13] Save in the case of Scottish warrants for serious crime, s7 RIPA refers only to the power of the Secretary of State to issue warrants and therefore it is exercisable by any of the Secretaries of State: see Schedule 1 of the Interpretation Act 1978. The practice, however, is as outlined above.

[14] See e.g. the judgment of Lord Dyson in *Walumba Lumba v Secretary of State for the Home Department* [2011] UKSC 12 concerning a secret policy operated by the Home Office between 2006 and 2008 concerning the blanket detention of foreign prisoners: "It is material that there is no suggestion that officials acted for ulterior motives or out of malice towards the appellants. Nevertheless, there was a deliberate decision taken at the highest level to conceal the policy that was being applied and to apply a policy which, to put it at its lowest, the Secretary of State and her senior officials knew was vulnerable to legal challenge. For political reasons, it was convenient to take a risk as to the lawfulness of the policy that was being applied and blame the courts if the policy was declared to be unlawful" (para 166).

[15] *In re McE* [2009] UKHL 15 at para 119. At the time of writing, we note also the revelations regarding surveillance of privileged lawyer-client conversations: see *Belhadj & others v Security Service & others*, Case IPT/13/132-9/H, 'Respondents' revised response to claimants' request for further information' 29 October 2014. Documents available in O Bowcott, 'UK intelligence officers spying on lawyers in sensitive security cases', 7 Nov 2014 http://www.theguardian.com/world/2014/nov/06/intelligence-agencies-lawyer-client-abdel-hakim-belhaj-mi5-mi6-gchq.

[16] Para 55. See also e.g. para 56: "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge". The requirement for judicial authorisation is even more explicit in cases involving the seizure of journalistic material under Article 10 ECHR: see e.g. *Sanoma Uitgebers BV and others v Netherlands* (2010) 51 EHRR 31.

13. The Court in *Klass* did not exclude the possibility that effective control could also be exercised by a non-judicial body, so long as it could be shown that it was "independent of the authorities carrying out the surveillance" - i.e. "enjoying sufficient independence to give an objective ruling" - as well as "vested with sufficient powers and competence to exercise an effective and continuous control".[17] In our view, however, it cannot be said that the Secretaries of State are sufficiently independent of the agencies that apply to them for interception warrants; this is because they are accountable to Parliament for the performance of those same agencies.[18] It is *this* aspect of democratic accountability which, in our view, makes government ministers constitutionally ill-suited to grant interception warrants. It is, of course, true that in *Kennedy v United Kingdom,* the Strasbourg Court considered that the Interception of Communications Commissioner and the Investigatory Powers Tribunal provided sufficient judicial control of interception warrants issued by the Secretary of State.[19] For reasons set out in detail below,[20] however, we consider that neither body can properly be said to "exercise an effective and continuous control" over interceptions, and that the ECtHR in *Kennedy* therefore misapprehended the true position under RIPA.

14. Other arguments against judicial authorisation of interception include that it would undermine operational effectiveness,[21] that it would be more resource-intensive than the current model; that it would prevent or inhibit continuing or "downstream" oversight of how interception material is retained and shared. However, these arguments tend to overlook how RIPA *already* provides for judicial authorisation of certain surveillance powers:

    (a) authorisations for police to use intrusive surveillance under Part II must first be approved under s36 RIPA by a Surveillance Commissioner (a person who holds or has held high judicial office under s91(2) of the Police Act 1997);

---

[17] Ibid, para 56.

[18] See e.g. *Kopps v Switzerland* [1999] 27 EHRR 91 at para 74: "It is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence".

[19] (2011) 52 EHRR 4 at paras 166-167.

[20] Paras 40-53.

[21] See e.g. the evidence of the then-Interception of Communications Commissioner Sir Swinton Thomas to the Joint Committee on Human Rights: "From a practical point of view, which I suppose is what I am more concerned with, I think it is a very bad idea to put [interception decisions] in the hands of a judge. As things are at the moment, if you know that a bomb has been taken on a train in Leeds and is on its way to King's Cross and you need information, in a matter of minutes you can get a warrant to intercept the communications of that suspected terrorist. Likewise with a serious crime, if a very large consignment of class A drugs has arrived at Dover and is on its way up to Manchester, the Secretary of State is always on duty, 24 hours a day. It is very often absolutely vital that you act with as much speed as you possibly can. That is what currently happens. You can get a warrant or a modification, which is equally important, straight away. Going to a judge would not permit that degree of elasticity. If it is done by a judge, the other side must have the right to be heard and you will not be able to acquire a judicial hearing at the sort of speed that papers can be put in front of the Secretary of State" (12 March 2007, Q26). However, as the then-Director of Public Prosecutions Sir Ken Macdonald QC explained in the same evidence session, there is no reason why judicial authorisation for interception should not be done on an *ex parte* basis (see Q27) and, as Lord Lloyd of Berwick pointed out, there would be no difficulty in getting judicial authorisation "almost as quickly" as with the Secretary of State (Q28).

(b) authorisations for local authorities to access to communications data, use directed surveillance, or covert human intelligence sources must first be approved by a magistrate under ss23A-D RIPA (as amended by ss37-38 of the Protection of Freedoms Act 2012); and

(c) permission to make an encryption notice under Part III must be given by a Circuit judge under paragraph 1(1) of Schedule 2 RIPA.[22]

15. Of these, we consider that the work of the Surveillance Commissioners in approving the use of intrusive surveillance by police provides a useful model for judicial authorisation of interception warrants under RIPA for the following reasons:

(i) it is well-known that intrusive surveillance may enable police to access the contents of private communications almost as readily as interception (e.g. recording a telephone conversation by way of a covert listening device or viewing a computer screen by way of a hidden camera);[23]

(ii) the Surveillance Commissioners are already obliged to consider the likelihood that the use of intrusive surveillance may result in the acquisition of legally privileged material (as well as the likelihood of obtaining "confidential information" under the Police Act 1997, including not only privileged material but also confidential journalistic material, personal information, or communications with an MP on constituency matters);[24]

(iii) s36(2) RIPA provides for police to use intrusive surveillance without judicial approval in cases of urgency, subject to subsequent review by a Surveillance Commissioner who has the power to quash or cancel such authorisations under s37(2) or (3). (We note, moreover, that this is consistent with the procedures in most countries which require judicial authorisation for interception, in that they allow for emergency self-authorisation by police subject to judicial confirmation within 24 or 48 hours);[25]

(iv) in addition to approving the use of intrusive surveillance by police, the Surveillance Commissioners also provide "downstream" oversight by way of their role in reviewing the renewal of authorisations as well as by way of the annual report of the Chief

[22] Save where the police or intelligence services have obtained the encrypted material by way of a warrant made by the Secretary of State: see paragraph 2 of Schedule 2 RIPA.

[23] See e.g. *R v Allsop and others* [2005] EWCA Crim 703; *R v E* [2004] EWCA Crim 1243; *R v Smart and another* [2002] EWCA Crim 772.

[24] In her evidence to the Intelligence and Security Committee in October 2014, the Home Secretary suggested that a key difference between judicial authorisation of search warrants and that of interception warrants was that a search takes place in public whereas surveillance involves a different kind of intrusion. In our view, however, the different nature of the intrusion only makes judicial authorisation *more* necessary. More to the point, intrusive surveillance by the police under Part II RIPA also involves considerable secrecy, yet it is not suggested that judicial authorisation in these cases is somehow less appropriate.

[25] See e.g. 18 US Code § 2518(7), enabling interception without a judge's order where there is immediate danger of death or serious physical injury, or "conspiratorial activities" which either threaten national security or are characteristic of organized crime, so long as an application is made to a judge within 48 hours.

Commissioner under s62 RIPA. Again, this is consistent with the procedure of other jurisdictions which require judicial authorisation;[26]

(v) the Surveillance Commissioners have each held high judicial office, which means that they are each former Court of Appeal or High Court judges or their Scottish equivalent.

16. We do not suggest that it is the Surveillance Commissioners themselves who should necessarily assume responsibility for making interception warrants: in our view, the same function could in principle also be carried out by any High Court judge (see e.g. their expertise in cases involving terrorist asset-freezing, TPIMs and deportation on grounds of national security) or even the specialist district court judges who preside over cases involving extradition or terrorism. If judicial supervision is possible in these areas involving highly sensitive matters of national security and close scrutiny of the activities of the intelligence services, then it should also be possible in the case of interception of communications. In any event, the role of the Surveillance Commissioners shows not only how judicial authorisation of surveillance powers *may* work in practice, but also that it *has* worked for nearly fifteen years under Part II of RIPA.[27]

17. For the avoidance of doubt, we do not recommend that the judge's task be confined to deciding whether or not to *approve* an authorisation – rather, the relevant agency should apply for an interception warrant in the same manner as a search warrant, i.e. it is for the judge himself or herself to decide whether the surveillance sought is necessary and proportionate, rather than simply reviewing whether the applicant's assessment of necessity and proportionality was reasonable. We also recommend that the judge should have the power to direct the appointment of a special advocate in appropriate cases (e.g. where the application is particularly complex) in order to test the application in a closed hearing, just as a judge may currently do in cases involving public interest immunity[28] and is routinely the case in applications for surveillance in Queensland, Australia.[29]

Bulk interception of 'external' communications under s8(4)

18. At the time of writing, the legality of warrants for the bulk interception of external communications under s8(4) RIPA is the subject of several legal challenges, before both the

[26] See e.g. 18 US Code § 2518(6), under which an interception order "may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception".

[27] Moreover, if it is correct that the Home Secretary spends a "significant part of her day dealing with intercept and surveillance warrants",(see "Theresa May defends culture of secrecy over mass snooping" by Alan Travis, The Guardian, 16 October 2014) then it is apparent that an additional benefit of judicial authorisation is that it would enable each of the relevant Secretaries of State to devote more time to those duties to which they are constitutionally better-suited to discharge.

[28] See *R v H* [2004] UKHL 3 at para 36.

[29] See the role of the Public Interest Monitor under s326(b) of the Crime and Misconduct Act 2001 (Qld) as set out in JUSTICE, *Secret Evidence* (June 2009) at paras 333-337.

Investigatory Powers Tribunal[30] and the European Court of Human Rights.[31] In outline, the key issues are as follows:

(a) unlike a warrant issued under s8(1), there is no requirement for a warrant under s8(4) to be targeted at the communications of either a particular person or a specific premises. As the Investigatory Powers Tribunal noted in *British Irish Rights Watch and others v Security Service and others*, a warrant under s8(4) may in principle result in "the interception of all communications between the United Kingdom and an identified city or country".[32] The only constraint is what the Secretary of State considers to be necessary in the interests of national security, the detection or prevention of serious crime, safeguarding the economic well-being of the United Kingdom,[33] or for the purposes of giving effect to an international mutual legal assistance agreement (s5(3) RIPA);

(b) although a warrant under s8(4) only authorises the interception of "external" communications (defined by s20 as those either sent or received outside the British Islands), s5(6) RIPA further authorises the interception of any such communications not identified by the warrant as is necessary in order to intercept the external communications in question. As Lord Bassam told Parliament in 2000, "it is just not possible to ensure that only external communications are intercepted" and "there is no way of filtering ... out [internal] communications without intercepting the whole link".[34] In practical terms, therefore, the interception of external communications is liable to involve the interception of an unknown number of internal communications as well;

(c) although Parliament was told in 2000 that email sent and received within the UK would not fall within the definition of "external communications" under s20, even if it was routed outside the UK in transit,[35] it remains unclear how this definition would apply to such activities as an inquiry made of a search engine or a post to a friend's page using social media. It was not until 16 May 2014 that a senior Home Office official revealed in a witness statement that the intelligence services considered that search engine inquiries and posts to social media platforms were "external communications" for the purposes of s8(4) RIPA, so long as the relevant server was outside the British Islands, notwithstanding that the only persons involved in the communication were within the UK at all material times;[36]

---

[30] See *Liberty, the ACLU and others v GCHQ and others* (IPT/13/77H, IPT/13/168-173/H); *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (IPT/13/92/CH); and *Amnesty International v The Security Service and others* (IPT/13/194/CH).

[31] See *Big Brother Watch and others v United Kingdom* (no 58170/13, lodged 4 September 2013).

[32] IPT/01/77, 9 December 2004 at para 9.

[33] This ground has now been narrowed by s3 DRIPA to only those economic interests that are "also relevant to the interests of national security". In addition, s5(5) RIPA has always provided that a warrant cannot be necessary for the purposes of safeguarding economic interests unless the information in question relates "to the acts or intentions of persons outside the British Islands"

[34] Hansard, HL debates, 12 July 2000, col 323.

[35] See the speech of Lord Bassam, ibid and para 5.1 of the Interception of Communications Code of Practice, issued in July 2002 under s71 RIPA.

[36] See witness statement of Charles Farr dated 16 May 2014 at paras 132-138.

(d) the primary safeguard to prevent internal communications collected under s8(4) warrants being "read, looked at or listened to" by the intelligence services is that set out under s16(2), which prohibits officials from selecting material for inspection by reference to a factor which is "referable to an individual who is known to be for the time being in the British Islands", where one of the purposes of the search is to identify "material contained in communications sent by him or intended for him". There is nothing in s16 or elsewhere in RIPA, however, to prevent a person's internal communications being searched by reference to *other* factors which may nonetheless lead to disclosure of his or her sensitive personal information, e.g. religious beliefs, medical status, sexual orientation or political opinions;

(e) on the same basis, there is nothing under s16 or elsewhere in RIPA to prevent the *data* related to internal communications intercepted under s8(4) - e.g. traffic data, subscriber data and service use data - being collected, retained and used by the intelligence services for whatever purpose they consider to be necessary for the purposes of national security, etc under s5(3). To the extent that there is any internal guidance that further restricts how internal communications and related data may be used, the intelligence services have refused to disclose this on the grounds that it would be prejudicial to national security.

19. In the Bingham Centre's view, the current framework governing the bulk interception of communications and related data under s8(4) raises a number of concerns.[37] First, the relevant provisions - especially the definition of "external communication" under s20 - appear to us to lack sufficient clarity and certainty to comply with the fundamental requirements of the rule of law.[38] Secondly, we doubt whether the location from which a particular communication was sent or received (i.e. within or without the British Islands) provides a sufficient basis on which to distinguish between the narrow and targeted requirements of warrants under s8(1) with the virtually unrestrained breadth of warrants under s8(4). Thirdly, the practice of bulk interception - in which potentially millions of internal communications may be intercepted for the sake of obtaining a particular external communication - seems to us to be fundamentally at odds with the very concept of proportionality itself. In our view, all warrants and authorisations must be

[37] For reasons of space, we are unable to address an equally pressing issue which is the extent to which the intelligence services may *receive* communications data and the contents of communications collected by foreign intelligence agencies.

[38] C.f.. *Liberty and others v United Kingdom* (2009) 48 EHRR 1 at para 69, in which the ECtHR held that the relevant provisions of the Interception of Communications Act 1984 breached Article 8 ECHR because, inter alia, they did not "indicate with sufficient clarity ... the scope or manner of the very wide discretion conferred on the State to intercept and examine external communications ... In particular it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material"; see also *Weber and Saravia v Germany* (2008) 46 EHRR SE5 at para 94: the law governing interception must "indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".

founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity (which would, of necessity, include terrorist offences).

20. Nor is the scale of the apparent interference with the right to privacy mitigated by the fact that relatively few of the communications intercepted by the intelligence services under a s8(4) warrant may be "read, looked at or listened to" under s16(2). In this context, we note the recent judgment of the CJEU in *Digital Rights Ireland*, in which the Grand Chamber held that the blanket retention of customers' communications data for up to 2 years under the 2006 Data Retention Directive entailed "an interference with the fundamental rights of practically the entire European population" contrary to the rights to privacy and data protection under Articles 7 and 8 of the EU Charter of Fundamental Rights because it did "not require any relationship between the data whose retention is provided for and a threat to public security".[39]

21. For these reasons, we recommend that the current power to intercept external communications under s8(4) be repealed. At the very least it should be severely curtailed. We note that there is no statutory restriction against using s8(1) warrants in respect of so-called "external" communications. We see no reason, therefore, why targeted warrants should not be used in respect of external communications on the same basis that they are used within the UK.

Intercept as evidence

22. Section 17(1)(a) RIPA prohibits the use of intercept obtained under warrant as evidence in either criminal or civil proceedings.[40] In January 2008, a review committee of Privy Counsellors reported its conclusion that "intercept as evidence should be introduced", subject to certain operational tests that would have to be met.[41] In December 2009, the Home Secretary reported to Parliament that it had been unable to produce a viable model that met the legal requirements identified by the Privy Council.[42] The Home Secretary nonetheless stated that the Home Office's implementation team would continue to work to "identify a way forward".[43] As recently as June 2013, a Home Office minister told Parliament that the government was continuing to review the use of intercept as evidence, "under the guidance of the cross-party group of Privy Counsellors" and that it would "report back to the House in due course".[44] As of yet, there has been no subsequent report.

23. In our view, intercept evidence is one of the most compelling and probative forms of evidence available.[45] It is widely used in other common jurisdictions with similar criminal and civil

[39] *Digital Rights Ireland v Minister for Communications and others* (2014) ECLI:EU:C:2014:238 at paras 56 and 59.
[40] Notably, evidence obtained by way of interception without a warrant under ss3 or 4 RIPA (e.g. interceptions in prisons, etc) *are* admissible.
[41] Cm 7324, at para 204.
[42] Cm 7760 at paras 23-25.
[43] Ibid, para 25.
[44] 6 June 2013, col 1229W.
[45] As Lord Lloyd of Berwick told Parliament during the debates on what became s17: "We have here a valuable source of evidence to convict criminals. It is especially valuable for convicting terrorist offenders

proceedings as our own,[46] including some with more onerous requirements governing the disclosure of relevant unused material.[47] And, as Lord Bingham noted in 2004, there is nothing in the ECHR that prohibits the use of intercept as evidence.[48] On the other hand, the lack of provision for intercept evidence has not only made it more difficult to prosecute terrorism offences, but increased resort to exceptional measures such as TPIMs.[49] We therefore consider it essential that any reform of the legal framework of investigatory powers in the UK must address the issue of intercept evidence.

Communications data

The changing nature of communications data

24. The lower level of protection accorded to communications data under Chapter 2 of Part 1 of RIPA reflects the longstanding view that the content of any given communication is necessarily more sensitive than the data which relates to it. In the 1984 case of *Malone v United Kingdom*,

---

because in cases involving terrorist crime it is very difficult to get any other evidence which can be adduced in court, for reasons with which we are all familiar. We know who the terrorists are, but we exclude the only evidence which has any chance of getting them convicted; and we are the only country in the world to do so" (Hansard, HL Debates 19 June 2000, col 109-110); see also the views of the Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning*, HL 157/HC 394, 16 July 2007 at para 126: "We are satisfied that the evidence of the DPP and the former Attorney General puts the matter beyond doubt: that the ability to use intercept as evidence would be of enormous benefit in bringing prosecutions against terrorists in circumstances where prosecutions cannot currently be brought, and that the current prohibition is the single biggest obstacle to bringing more prosecutions for terrorism. We recommend that this be taken as the premise of the forthcoming review by the Privy Council. The difficult question is not whether the current ban on the evidential use of intercept should be relaxed, but how to overcome the practical obstacles to such a relaxation".

[46] See e.g. *Intercept Evidence: Lifting the Ban* (JUSTICE, October 2007).

[47] See e.g. "The Unique Challenges of Terrorism Prosecutions" (Ch 7) vol 4 at p267), *Air India Flight 192: A Canadian Tragedy* (June 2010): "In general, disclosure obligations in both the United States and the United Kingdom are less broad than in Canada. Both the United States and the United Kingdom attempt to flesh-out disclosure requirements in statutes and other rules while, as discussed above, Canada relies on a case-by-case adjudication under the Charter. Both the decreased breadth and increased certainty of disclosure requirements in the United States and the United Kingdom may make it less necessary for prosecutors to claim national security confidentiality over material that may be relevant to a case, but which does not significantly weaken the prosecution's case or strengthen the accused's case."

[48] *Attorney General's Reference No 5 of* 2002 [2004] UKHL 40 at para 14: "the United Kingdom practice has been to exclude the product of warranted interception from the public domain and thus to preclude its use as evidence. But this has been a policy choice, not a requirement compelled by the Convention, and other countries have made a different policy choice. Article 8(2) of the European Convention permits necessary and proportionate interference with the right guaranteed in Article 8(1) if in accordance with the law and if in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. Save where necessary to preserve the security of warranted interception, there is no reason why it should have been sought to exclude the product of any lawful interception where relevant as evidence in any case whether civil or criminal".

[49] See e.g. Home Office Minister Lord Rooker, Hansard, HL Debates, 27 November 2001, col 146: "If we could prosecute on the basis of the available evidence in open court, we would do so. *There are circumstances in which we simply cannot do that because we do not use intercept evidence in our courts*".

[50] for instance, the British government had argued that the practice of 'metering' (which involved a meter check printer being attached covertly to a telephone line to record "the numbers dialled on a particular telephone and the time and duration of each call")[51] did not entail any interference with the applicant's rights under Article 8 ECHR. Although this argument was rejected by the ECtHR on the basis that the relevant data was "an integral element in the communication", it accepted that the collection of data was nonetheless to be distinguished from the interception of content.[52]

25. It is obvious, however, that there has been a fundamental shift in the nature of communications technology over the past three decades. Not only is there increasing convergence of communications *networks* (e.g. voice and data being carried on the same infrastructure) but also a convergence of *functions*, so that most individuals now carry at least one or more devices which are each capable of communicating in a number of different ways, e.g. a person who uses his or her mobile phone to make calls, send texts and emails, post on social media and browse websites on the Internet.

26. In addition to the fact that most of our private communications are now made via the Internet, it is also apparent that there has been a vast increase in the amount of communications data that is generated by each person, which is then automatically collected and stored by a wide range of communications service providers and accessible to public authorities under RIPA. It is apparent that the analysis of such data – including not only numbers dialled and the time and duration of a call but also geo-location data and the IP addresses of websites visited – can readily disclose details of a person's relationships with others as well as various patterns of behaviour capable of revealing broad range of sensitive information about that individual, including their ethnic origin, their political opinions or religious beliefs, their physical or mental health, and/or their sexual orientation.[53]

27. In our view, it is clear that there is very little meaningful comparison between the quality of information available from the Post Office's metering of a single landline in the early 1980s and that available from an ordinary mobile phone more than three decades later. The idea that

[50] (1984) 7 EHRR 14.
[51] Ibid, para 83.
[52] Para 84.
[53] For example, a study by the Center for Internet and Society at Stanford Law School analysed the communications data gathered from 546 mobile phone users ("MetaPhone: The Sensitivity of Telephone Metadata" by Patrick Mutchler and Jonathan Mayer, 12 March 2014). In the first instance, it noted that, in certain cases, the simple fact that a number was called was itself highly sensitive in nature: "Participants had calls with Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more". The study went on to find "a number of patterns that were highly indicative of sensitive activities or traits", for example: "Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis" and "Participant E had a long, early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after".

intercepting the content of a person's communications is always more intrusive than accessing their communications data is simply no longer sustainable. The interception of the content of any particular telephone call by an individual may reveal very little about that person's religious beliefs, their medical information or their sexual orientation. Access to and analysis of the communications data from the same person's mobile phone may, by contrast, readily disclose a wealth of highly sensitive information about that person, all without a single word of their communications being read, looked at or listened to by anyone else. By the same token, it is equally true that access to communications data may also disclose information subject to legal professional privilege or the identity of a journalist's source. We are concerned, therefore, by recent revelations that the Metropolitan police may have been using authorisations under Chapter 2 to access communications data as a means of avoiding the requirements of the Police and Criminal Evidence Act 1984 in respect of journalistic material.[54]

Authorisation

28. Given the obvious sensitivity of communications data, it is clear that existing procedures for authorising access to such data are inadequate. In the first instance, Chapter 2 of Part 1 of RIPA provides that when a public body seeks access to communications data, the person responsible for authorising the request is, in almost every case, a senior member of the same agency. Even if senior officials scrutinize applications for communications data with great care, it is plain that they are not independent of the agency carrying out the surveillance and are therefore institutionally incapable of the objectivity needed to give an impartial decision on the merits of the application.

29. In this respect, we note that Protection of Freedoms Act 2012 introduced a requirement for prior judicial authorisation of communications data requests by local authorities, together with a power for the Secretary of State to extend this requirement to other public bodies by way of an order. While this might at first glance appear to provide an appropriate way forward, we note that serious concerns have been expressed that many magistrates do not have sufficient training or expertise to provide the necessary degree of supervision.[55] We therefore recommend that authorisation for access to communications data should be placed on the same footing as the interception of communications: i.e. ideally authorised High Court judges or their equivalent. Similarly, in cases of urgency, the police and intelligence services should have the power to self-

[54] See, for example, 'A Travis, 'Police told to reveal the use of surveillance powers to identify journalists' sources', *The Guardian*, 6 Oct 2014, http://www.theguardian.com/uk-news/2014/oct/06/police-ordered-reveal-ripa-powers-identify-journalists-sources. We welcome the government's undertaking to reform the law: P Wintour, 'British police's use of Ripa powers to snoop on journalists to be reined in' *The Observer*, 12 Oct 2014, http://www.theguardian.com/world/2014/oct/12/police-ripa-powers-journalists-surveillance.

[55] See e.g. the 2014 report of the Chief Surveillance Commissioner at para 3.10: "What has become clear is that the knowledge and understanding of RIPA among magistrates and their staff varies widely. Adequate training of magistrates is a matter for others, but I highlight the need. The public is not well served if, through lack of experience or training, magistrates are not equipped effectively to exercise the oversight responsibility which the legislation requires. I am aware, for example, of one magistrate having granted an approval for activity retrospectively, and another having signed a formal notice despite it having been erroneously completed by the applicant with details of a different case altogether."

authorise access to communications data so long as it is subject to judicial confirmation within 48 hours.

30. A separate concern is that, unlike interception warrants under s8(1), there is no requirement that a request for access to communications data be targeted against a particular individual. We therefore recommend that this requirement be introduced to ensure that the power to access communications data is not exercised disproportionately.

31. More generally, we recommend that both the number of statutory powers to access communications data and the number of public bodies able to wield those powers should be severely curtailed. In the latter case, we recommend that the power to access such data should be restricted to the police, the intelligence services and the limited number of other public bodies with a responsibility to investigate serious criminal activity.[56] As regards the former, we note that the current government has already committed itself to ensuring that "RIPA is the only mechanism by which communications data can be acquired"[57] and we further note the requirement in s1(6) DRIPA prohibiting disclosure of communications data retained by a public telecommunications operator pursuant to a retention notice other than by way of Chapter 2 RIPA or "a court order or other judicial authorisation or warrant" or under regulations made by the Secretary of State. Although this is a welcome move, we note that it does not prevent access to communications data held by *other* communications service providers otherwise than pursuant to a retention notice, nor has the Secretary of State published any regulations in draft.

Intrusive surveillance, directed surveillance and covert sources

32. The distinction under Part 2 RIPA between 'intrusive' and 'directed' surveillance is meant in principle to ensure that any surveillance that is likely to involve a serious interference with a person's privacy (i.e. intrusive) requires a much higher level of authorisation than those which do not (i.e. directed). However, as the Code of Practice itself notes, the statutory definition of 'intrusive' "relates to the *location* of the surveillance [i.e. within a person's home or vehicle] and *not* any other consideration of the nature of the information that is expected to be obtained". It is therefore not necessary, the Code continues, "to consider whether or not intrusive surveillance is likely to result in the obtaining of private information".[58] Part 3 of the Police Act 1997, by contrast, requires judicial authorisation whenever property interference is likely to result in "the acquisition of knowledge of matters subject to legal privilege, confidential personal information or confidential journalistic information".[59]

---

[56] C.f. the 2009 recommendation of the House of Lords Constitution Committee that "such powers should only be available for the investigation of serious criminal offences which would attract a custodial sentence of at least two years" (*Surveillance, Citizens and the State*, HL 18, January 2009, para 177). An exception could also be made for the other emergency services who sometimes need to access subscriber data in order to identify persons involved in accidents, etc.

[57] Home Office Review of Counter-Terrorism Powers (Cm 8004, January 2011), p 29.

[58] Para 2.11.

[59] Ibid, para 4.12.

33. The possibility that 'directed' surveillance may prove highly intrusive was highlighted in *In re C*, in which the Divisional Court in Northern Ireland held that the use of surveillance to monitor privileged communications between lawyers and suspects in prison cells and custody suites was unlawful because of the lack of prior judicial authorisation.[60] However, although the subsequent 2010 order[61] introduced the requirement for such authorisation in order to monitor 'legal consultations' in places of detention, it is notable that it still adopted a location-based approach rather than one of substance. In other words, it is still permissible under RIPA to use directed surveillance of a privileged conversation that takes place in a town hall or an MPs office or a park bench, etc.

34. We therefore recommend that the definition of 'intrusive' surveillance be tightened, so that the former includes *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy. 'Directed' surveillance, in contrast, would be any use of covert surveillance that either does not or is not likely to involve a significant interference with a person's privacy.

35. For the same reasons outlined above in respect of interception and communications data, we also recommend that the power of the Secretary of State to authorise intrusive intelligence by the intelligence services under s41 RIPA should be repealed. Instead, *all* use of intrusive surveillance should be authorised by the Surveillance Commissioners or a judge of equivalent level.

36. As regards the use of covert sources, we note an increasing number of revelations in recent years concerning the conduct of undercover officers, including in particular members of the National Public Order Intelligence Unit, the National Domestic Extremism Unit, and the Metropolitan Police's Special Demonstration Squad. These have resulted not only in a series of investigations by HM Inspector of Constabulary, the National Crime Agency and the Independent Police Complaints Commission among others, but also several miscarriages of justice[62] and, in the most recent case, a settlement of £425,000 to a woman whose child was fathered by an undercover police officer.[63]

37. In our view, these cases further highlight the inadequacy of the internal self-authorisation model that underpins much of RIPA. We note, moreover, the 2011 recommendation of the then-President of the Association of Chief Police Officers, Sir Hugh Orde, that judicial authorisation

[60] [2007] NIQB 101, subsequently upheld by the House of Lords in *In re McE* [2009] UKHL 15.
[61] The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 (SI 2010/461).
[62] *David Robert Barkshire and others v The Queen* (Court of Appeal Criminal Division, unreported, 20 July 2011).
[63] See e.g. BBC News, "Met pays £425,000 to mother of undercover policeman's child", 24 October 2014.

of undercover officers should be required in complex cases.[64] The Chief Surveillance Commissioner has also indicated that he was "also agreeable in principle to Commissioners giving prior approval to certain kinds of such activity by a [covert human intelligence source], provided that the OSC is given the appropriate resources to deal with the number of cases which arise and subject to any necessary legislation conferring the power".[65] We therefore recommend that the use of undercover officers should be authorised by a judge in any case where their conduct is likely to involve a significant interference with another person's privacy.

Encryption keys

38. The threat of terrorism has since the 1990s been cited by government officials as justifying the need for a statutory power to obtain encryption keys,[66] though the powers under Part 3 of RIPA were not brought into force until October 2007. Since then, it does not appear to have been widely used by either the police or the intelligence services and, when it has been used, it has mostly been used for non-terrorist offences such as child sex abuse.[67]

39. Although we consider that the power to obtain encryption keys is, in certain circumstances, a necessary one, there are a number of ways that the existing framework could be improved. First, Part 3 of RIPA is poorly-drafted. As we noted above, accessibility and certainty are both core requirements of the rule of law and the ECtHR has repeatedly made clear the need for "clear, detailed rules" and "accessibility and clarity" not only in the case of interception but also to "more general programmes of surveillance".[68] Secondly, permission to make a notice can only be made by a Circuit Judge, save where the encrypted material has been obtained under a warrant from or with the authorisation of the Secretary of State.[69] As with interception, communications data, and intrusive surveillance, we recommend that the Secretary of State should play no role in authorising surveillance. Instead, an encryption notice should only be authorised by a judge.[70] Thirdly, although there has already been some judicial consideration of the privilege against self-incrimination,[71] neither RIPA nor the Code of Practice make any allowance for journalistic material or material covered by legal professional privilege corresponding with the safeguards contained in PACE.

---

[64] Sir Hugh Orde, "Undercover Policing and Public Trust", 7 February 2011.
[65] 2011-2012 report, para 5.1.
[66] See e.g. Department of Trade and Industry, Paper of Regulatory Intent concerning Use of Encryption on Public Networks (June 1996).
[67] See e.g. the report of the Chief Surveillance Commissioner for 2009-2010 at para 4.11: "[The offence of] the possession of indecent images of children … is the main reason why section 49 notices are served. Other offences include: insider dealing, illegal broadcasting, theft, evasion of excise duty and aggravated burglary. It is of note that only one notice was served in relation to terrorism offences". See more generally JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011), paras 327-333.
[68] *Liberty and others v United Kingdom* (2009) 48 EHRR 1 at para 63.
[69] Paragraph 2 of Schedule 1 of RIPA.
[70] In cases involving the intelligence services and other sensitive cases, it may be more appropriate for the application to be made to a security-cleared High Court or Crown Court judge rather than a Circuit Court judge.
[71] See *R v S and A* [2008] EWCA Crim 2177 and *Greater Manchester Police v Andrews* [2011] EWHC 1966 (Admin).

Oversight

The Commissioners

40. In *Kennedy*, the ECtHR described the Interception of Communication's review of "a random selection of specific cases in which interception has been authorised" as "an important control of the activities of the intercepting agencies and of the Secretary of State himself".[72] The Bingham Centre agrees that the oversight provided by the Interception Commissioner - together with that provided by the Intelligence Services Commissioner and the Chief Surveillance Commissioner – constitutes an extremely important safeguard against the unnecessary or disproportionate use of surveillance powers. As valuable as this independent safeguard is, however, we consider that the oversight regime provided by the Commissioners suffers from a number of significant deficiencies.

41. First, it is clear that the remit of each Commissioner, taken together, does not provide comprehensive oversight of the exercise of surveillance powers under RIPA. The Interception of Communications, for instance, has no statutory remit in respect of interceptions under section 3 and has only agreed to provide oversight of interceptions in prisons on a "non-statutory" basis.[73] This does not, however, include other places of detention such as private prisons or secure mental health facilities, nor does it extend to the very broad power of communications service providers and operators of private communications networks to intercept communications for "the purposes connected with the provision or operation of a [telecommunications] service" under ss 3(1) and 3(3) respectively.

42. Secondly, the current framework defines the remit of each oversight Commissioner according to function in some cases and by agency in other cases. In practical terms, this means that surveillance of a privileged communication between a suspected terrorist and his lawyer may be subject to oversight by three different Commissioners, depending entirely on how it was authorised and according to which agency carried out the surveillance, i.e.:

    a. If the phone conversation was intercepted under Part 1 RIPA then the Secretary of State's warrant would be subject to review by the Interception of Communications Commissioner;

    b. If the phone conversation was monitored by way of a hidden microphone planted in the suspect's home by one of the intelligence services, then the Secretary of State's authorisation for intrusive surveillance under Part 2 RIPA would be subject to review by the Intelligence Services Commissioner; or

[72] *Kennedy*, para 166.

[73] See the 2002 report of Sir Swinton Thomas at para 59: 'I have been asked by the Home Office, and have agreed in principle, to oversee the interception of communications in prisons'.

c. If the phone conversation was monitored by way of a hidden microphone planted in the suspect's home by the police, then review of the authorisation for intrusive surveillance under Part 2 RIPA would be subject to review by the Chief Surveillance Commissioner.

The potential for this piecemeal oversight also arises in other parts of RIPA: e.g. the use of encryption notices under Part 3 which has been reported on by all three commissioners. In our view, it is highly undesirable that the same intrusion could be subject to oversight by three different bodies, each with their own distinct procedure and approach, depending on the choice of methods and the agency involved.

43. Thirdly, it is apparent that both the Interception of Communications Commissioner and the Intelligence Services Commissioner are part-time posts, and inspect only a small sample of the warrants and authorisations made annually under Part 1 RIPA by the various Secretaries of State.[74] In his most recent report, for instance, the Interception of Communications Commissioner stated that he inspected approximately 600 applications for warrants made in 2013,[75] amounting to little more than 20% of the 2760 warrants issued that year. Although the Commissioner has defended this as a "sufficient representative sample of the individual warrants",[76] we note that each warrant embodies a decision by a member of the executive to invade the privacy of one or more persons (and in the case of a warrant under s8(4), potentially millions of people). It is therefore not acceptable, in our view, that approximately 4 in every 5 warrants, and more than 90% of authorisations to access communications data, are never looked at by a judge, even after the fact.

44. Fourthly, even when warrants and authorisations are scrutinized, it remains unclear what standard is applied by the reviewing Commissioner in each case, e.g. does he satisfy himself whether the interference with Article 8(2) was necessary and proportionate[77] or does he simply consider whether the Secretary of State's assessment of those factors was *Wednesbury* reasonable?

45. Fifthly, even in the unlikely event that the Interception of Communications Commissioner discovered that the Secretary of State had made a warrant that he considered to be unlawful, RIPA does not provide him with any power to quash the warrant. He may, of course, report the matter to the Prime Minister under s58(2) but the Prime Minister has the discretion to redact such information from the report laid before Parliament. Nor does the Interception of

[74] House of Commons Home Affairs Committee, *Counter-terrorism* (HC 231, April 2014) at para 163: "The information given to us by the Commissioners indicate that they examine a small number of warrants under the current oversight system. The Intelligence Services Commissioner told us that in 2012 he had examined 8.5% of warrants. The Interception of Communications Commissioner told us that he had examined between 5% and 10% of the applications. He was not able to be more specific as he did not know how many applications there were."
[75] Para 3.36.
[76] Para 3.37.
[77] c.f. *Huang v Secretary of State for the Home Department* [2007] UKHL 11 at para 20.

Communications Commissioner have the power to refer a possible breach of Article 8 ECHR to the Investigatory Powers Tribunal.

46. For the above reasons, the Bingham Centre does not consider that the Commissioners overall provide "effective control" of surveillance powers under RIPA, save in the limited circumstances where those powers have already been subject to prior judicial authorisation (e.g. the use of intrusive surveillance where approved by the Surveillance Commissioners, or the use of directed surveillance by local authorities). In our view, extending judicial authorisation across the board would go a long way to reducing the administrative burden on the commissioners. While the burden will, of course, shift rather than disappear, the shift is worthwhile as it is of vital importance for control to be effective. Even so, it is apparent that the different oversight schemes are in need of rationalisation and we therefore recommend that the current functions be combined within a single, properly-staffed and funded body providing more coherent and effective oversight. We also recommend that this body have a broader remit to oversee the use of *all* surveillance powers by public bodies, rather than the current fragmented statutory regime. Although concerns have been expressed that putting oversight on a more permanent footing may result in less independent-minded candidates being available, we consider that it should be possible to devise a model that strikes an appropriate balance between independence and effectiveness. We note, for instance, that the Law Commission is chaired by a High Court or Appeal Court judge, serving for up to three years. We see no reason why appointment to chair the statutory oversight regime for surveillance powers should not be on a similar footing.

Investigatory Powers Tribunal

47. Just as the ECtHR in *Kennedy* praised the role of the oversight Commissioners, so too it commended the Investigatory Powers Tribunal as an "independent and impartial body, with its own rules of procedure" that constituted a "general safeguard" against the abuse of surveillance powers.[78] In addition, the ECtHR found that the procedures of the Tribunal did not "impair the very essence of the applicant's Article 6 rights", notwithstanding that the Tribunal considered his specific complaints in private without him being present, did not provide the applicant with any disclosure, did not afford him the opportunity to cross-examine any witnesses on the other side, and did not appoint a special advocate to represent his interests in any of the hearings from which he had been excluded.[79]

48. In our view, however, the decision of the ECtHR in *Kennedy* is not consistent with its own established jurisprudence on the justiciability of surveillance decisions under Article 6.[80] More

[78] See *Kennedy*, paras 167 and 169.
[79] Ibid, para 184-190.
[80] See e.g. *Klass* at para 75: "the question whether the decisions authorising such surveillance under the [German statute] are covered by the judicial guarantee set forth in Article 6…must be examined by drawing a distinction between two stages: that before, and that after, notification of the termination of surveillance. As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6 … as a consequence, it of necessity escapes the requirements of that Article"; see also the dissent of Lord Kerr in

generally, while we accept that the Tribunal constitutes an essential safeguard against unlawful and disproportionate surveillance,[81] we are concerned that it is also severely flawed in a number of respects.

49. First, the proportion of applicants who are successful in their complaints before the Tribunal is extremely low – some 0.5% in the first decade of its operation.[82] In contrast, the annual success rate for complainants before other tribunals varies between 13% (mental health) and 41% (immigration and asylum).[83] In our view, the very poor success rate of complaints before the IPT does not necessarily reflect the quality of decision-making in the field of surveillance powers but rather almost certainly reflects the difficulty of bringing an effective challenge against the use of covert powers in a Tribunal in the absence of (i) proper notification requirements and (ii) any right to disclosure.

50. In *Klass*, the ECtHR conceded that the lack of any requirement on a public body to notify a person that they had been subject to surveillance following its conclusion meant that there was "in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality".[84] Despite this, the Strasbourg Court held that, although desirable, the absence of notification of surveillance did not breach the right to an effective remedy under Article 13 ECHR.[85] Although more recent cases have stressed the importance of notification requirements as safeguards against abuse of surveillance powers,[86] the ECtHR has yet to hold that notification is a *necessary* safeguard in such cases.[87] We note, however, that notification requirements are now a commonplace feature of surveillance laws in a great many jurisdictions including

---

Tariq v Home Office [2011] UKSC 11 at para 128: "The entire point of surveillance is that the person who is subject to it should not be aware of that fact. It is therefore impossible to apply article 6 to any challenge to the decision to place someone under surveillance, at least until notice of termination of the surveillance has been given … It is precisely because the fact of surveillance must remain secret in order to be efficacious that article 6 cannot be engaged. It appears to me, therefore, that the decision in Kennedy ought to have been made on the basis that article 6 was not engaged because the issues that the case raised were simply not justiciable."

[81] See e.g. *Paton v Poole Borough Council* (IPT/09/01/C, 29 July 2010).

[82] See JUSTICE, *Freedom from Suspicion*, at paras 358-364.

[83] Ibid, para 359.

[84] *Klass* at para 57.

[85] Ibid, para 69.

[86] See esp. *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* [2007] ECHR 533 at para 57: "[U]nless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them."

[87] The issue is currently before the Court in the case of *Lüütsepp v Estonia* (46049/13).

Belgium,[88] Bulgaria,[89] Canada,[90] Germany,[91] Ireland,[92] the Netherlands,[93] New Zealand,[94] Sweden[95] and the United States.[96] In his 2013 report to the General Assembly on communications surveillance, moreover, the UN Special Rapporteur on Freedom of Expression stated:[97]

> *Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.*

51. We further note that the Codes of Practice on communications data and encryption keys under RIPA both make provision for notification where a Commissioner establishes that an individual has been "adversely affected" by any "wilful or reckless failure" by a public body.[98] In such cases, the Commissioner is required, "subject to safeguarding national security" to "inform the affected individual of the existence of the Tribunal and its role" as well as to "disclose sufficient information to the affected individual to enable him to effectively engage the Tribunal". It is unclear, however, why these notification requirements should be limited to only cases involving communications data and encryption keys, as well as why the threshold should be restricted to "wilful or reckless" failures. Rather than have the Commissioner make a determination of whether to notify in each case, we consider that the better approach would be to require mandatory notification in each case within a reasonable period (e.g. 6 months following the warrant or authorisation expiring), subject to a judge's decision that notification should be delayed on the basis that that individual's right to an effective remedy is outweighed by some specific investigative need that would otherwise be prejudiced by the disclosure. As with the

---

[88] See Belgian Constitutional Court, *case no. 145/2011*. 22 September 2011 at paras B.82-B92, in which the court held the lack of notification breached the right to privacy under Art 22 of the Belgian Constitution.
[89] See *Lenev v Bulgaria* (41452/07, 4 December 2012) noting that section 34h of the Special Surveillance Means Act 1997 has been amended such that the supervising commission "must inform of its own motion persons who have been unlawfully subjected to secret surveillance, unless notification might jeopardise the purpose of the surveillance, allow the divulgation of operational methods or technical devices, or put the life or health of an undercover agent or his or her relatives or friends in jeopardy" (para 82).
[90] Section 196 of the Criminal Code provides for notification within 90 days of authorisation unless the judge is satisfied that investigations are ongoing or a subsequent investigation would be impeded. Notification cannot be delayed for more than 3 years.
[91] See e.g. *Klass* at para 19 and *Weber and Saravia v Germany* (54934/00, 29 June 2006) at para 136.
[92] Section 10(3) of the Criminal Justice (Surveillance) Act 2009.
[93] Article 34(1) of the Intelligence and Security Services Act 2002 requires notification after 5 years unless certain grounds are met.
[94] Sections 61 and 62 of the Search and Surveillance Act 2012.
[95] Section 11(a) of the 2008 law on Signals Intelligence (SFS 2008:717).
[96] 18 US Code § 2518(8)(d).
[97] UN Special Rapporteur on Free Expression A/HRC/23/40, 17 April 2013, at para 82. See also e.g. the International Principles on the Application of Human Rights to Communications Surveillance, May 2014.
[98] Communications Data Code of Practice at para 8.3. See also the similar provision in the Code of Practice for the Investigation of Protected Electronic Information at para 11.4.

Canadian Criminal Code, however, we recommend that there should be a maximum limit to the period of time for which notification can be delayed, e.g. 5 or 7 years.

52. As regards disclosure and the fairness of the IPT's procedures more generally, we accept that it is appropriate for the Tribunal to respect the agencies' policy of neither confirm nor deny (NCND) in the first instance, and particularly where the subject has not been notified of the surveillance in question. In our view, however, it is important to treat NCND as a starting point only, a defeasible principle that can be set aside where it becomes apparent to the IPT that it is necessary for the complainant to receive disclosure of material in order to effectively present his or her case. As the Vice President of the Court of Appeal held in a recent case, NCND is "not a legal principle" but rather a "departure from procedural norms" that "requires justification" in the same way as public interest immunity.[99] The framework of the IPT's procedures under Part 4 of RIPA, by contrast, do not – in our view – provide the Tribunal with sufficient flexibility to balance national security concerns with those of open justice and natural justice. Among other things, the IPT has no power even to make a declaration of incompatibility, has no formal power to appoint a special advocate to represent the interests of an excluded party, and indeed cannot even notify a party that a closed hearing has been held unless the other party consents. In this way, the framework under Part 4 compares unfavourably with the extensive case law that has developed in relation to closed proceedings in other courts and tribunals since 2001.[100]

53. We also consider that the ouster provision contained in s67(8) RIPA to be incompatible with the requirements of our common law constitution: if an appeal on a point of law is possible from other courts and tribunals employing closed procedures, we can see no good reason why the IPT should be immunised in this manner from the supervision of the higher courts. We therefore recommend that the IPT's procedural rules be significantly relaxed in order to enable much greater disclosure to complainants who have been subject to surveillance in order that they may bring an effective challenge, including sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded.

The Intelligence and Security Committee

54. Although the Intelligence and Security Committee provides important democratic oversight of surveillance powers and the activities of the intelligence services, we note that the accuracy of ISC reports has been the subject of judicial criticism in recent years, first in *R(Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs*[101] and subsequently in the report of Hallett LJ sitting as the Deputy Coroner in the inquest following the 7/7 bombings.[102] Following

[99] *Mohamed Ahmed Mohamed and CF v Secretary of State for the Home Department* [2014] EWCA Civ 559 at para 20 per Maurice Kay VP. See also *DIL and others v Commissioner of Police of the Metropolis* [2014] EWHC 2184 (QB) para 42 per Bean J.

[100] See e.g. *AF v Secretary of State for the Home Department (No 3)* [2010] 2 AC 269; *Bank Mellat v HM Treasury (No 1)* [2013] UKSC 38.

[101] [2010] EWCA Civ 65 at para 168 per Lord Neuberger MR.

[102] Report of Deputy Coroner Hallett LJ under Rule 43 of the Coroner's Rules 1984 (6 May 2011), paras 110-116.

these criticisms, the constitution of the ISC was amended by Part 1 of the Justice and Security Act 2013. We note, however, that although the members of the ISC are now appointed by Parliament rather than the Prime Minister, a person cannot be eligible for appointment unless they have been nominated by the Prime Minister (s1(4)(a) of the 2013 Act). In addition, although the Committee reports now to Parliament instead of to the Prime Minister, it must nonetheless be sent first to the Prime Minister who may require the redaction of any material he considers to be prejudicial to the operation of the intelligence services (s3(4)). In our view, these restrictions are an unnecessary constraint on the Committee's oversight and should be removed.

Retention of communications

55. Notwithstanding that the judgment of the Grand Chamber in *Digital Rights Ireland* invalidating the Data Retention Directive was handed down in April 2014,[103] we note that the government's proposals to address this were not published until July and then enacted on an emergency basis in only three days. It is concerning that legislation on such an important issue was handled in such a manner. It remains unclear, moreover, whether the provisions of ss1-2 DRIPA are compatible with the CJEU's judgment. In our view, much will depend on the regulations and the particular retention notices made by the Secretary of State and we understand that this already the subject of legal challenge. At the very least, we recommend that the power to make retention notices should be removed from the Secretary of State. Instead, retention notices should be issued by a judge on application by the relevant public body seeking retention.

SUMMARY OF RECOMMENDATIONS

56. We recommend as follows:

(i) A single, comprehensive statutory framework should govern the use of intrusive surveillance powers by public bodies. In particular, no public body should have the power to access communications data save by way of this framework.

(ii) Judicial authorisation should be required before any public body intercepts communications, accesses communications data, uses intrusive surveillance (including a covert human intelligence source), issues an encryption notice or a retention notice. The authorising judge should also have the power to direct the appointment of a special advocate to represent the interests of the subjects of surveillance in appropriate cases.

(iii) The existing power to intercept external communications under section 8(4) RIPA should be repealed. At the very least it should be severely curtailed. All warrants and authorisations must be founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity.

[103] C-293/12, ECLI:EU:C:2014:238.

(iv) The statutory definition of 'intrusive' surveillance should be tightened to include *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy.

(v) The ban on the use of intercept material as evidence in criminal and civil proceedings should be lifted.

(vi) The number of public bodies able to access communications data should be curtailed.

(vii) The oversight functions currently discharged by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner should be combined into a single statutory oversight body. This body's remit should include oversight of the use of all surveillance powers by public bodies;

(viii) Any person who has been the subject of covert surveillance by a public body should be notified of that fact within a reasonable period following the conclusion of the surveillance, unless a judge is satisfied that that individual's right to an effective remedy is outweighed some specific investigative need that would otherwise be prejudiced by the disclosure;

(ix) The Investigatory Powers Tribunal should be granted the power to appoint special advocates to represent the interests of excluded parties, as well as make a declaration of incompatibility under section 4 of the Human Rights Act. Its procedural rules should also be relaxed to allow much greater disclosure to complainants who have been the subject of surveillance, so that they may bring an effective challenge. This should include sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded. The unsuccessful party should also have a right of appeal to the Court of Appeal on a point of law;

(x) The statutory requirement that candidates for the Intelligence and Security Committee must first be nominated by the Prime Minister in order to be eligible for election should be repealed, as should the power of the Prime Minister to prevent the Committee from publishing material that it considers to be in the public interest to disclose.

APPENDIX: BINGHAM CENTRE EXPERT SEMINAR, 1 OCTOBER 2014

On 1 October 2014, the Bingham Centre for the Rule of Law held an evening conference on the subject of the Investigatory Powers Review led by the Independent Reviewer of Terrorism Legislation, David Anderson QC. Chaired by Eric Metcalfe of Monckton Chambers and the Bingham Centre, the event consisted of three panels: (I) Interception Warrants; (II) Communications Data; and (III) Oversight.

The evening began with an introduction to the Review by David Anderson, and was followed by a discussion of Section 8(1) warrants by Helen Mountfield QC, and Section 8(4) warrants by Matthew Ryder QC, both of Matrix Chambers. Panel II consisted of a discussion of Access to Communications Data under Part 1, Chapter 2 of RIPA by Graham Smith of Bird & Bird, followed by Gillian Phillips, Director of Editorial Legal Services at The Guardian on the subject of RIPA and Professional Privacy. Finally, Panel III concluded with presentations from Tom Hickman of Blackstone Chambers and the Bingham Centre and Eric Metcalfe on the Investigatory Powers Tribunal and the oversight Commissioners and the Intelligence and Security Committee.

The event included lively and and expert debate from the floor and was followed by a reception. The Bingham Centre is grateful to Macfarlanes for hosting the event.

List of Attendees

Name	Organisation
Mr Chris Acton	Macfarlanes
Mr David Anderson QC	Independent Reviewer of Terrorism Legislation
Mr Benjamin Baltzer	Embassy of the Federal Republic of Germany
Mr Martin Bentham	Evening Standard
Dr Jessie Blackbourn	Kingston University
Mr Owen Bowcott	The Guardian
Ms Jennifer Bruce	Ofcom
Mr Tom Bullmore	Treasury Solicitor's Department
Mr Jude Bunting	Doughty Street Chambers
Ms Elinor Buxton	Foreign & Commonwealth Office
Lord Carlile CBE QC	Gray's Inn
Ms Hannah Carter	Ofcom
Mr Rupert Casey	Macfarlanes
Ms Jo Cavan	Interception of Communications Commissioner's Office
Mr Martin Chamberlain QC	Brick Court Chambers
Mr Jan Clements	The Guardian
Mr Martin Coombes	Macfarlanes

Mr Gordon Corera	BBC
Mr Jeremy Courtenay-Stamp	Macfarlanes
Ms Gail Crawford	Lathan & Watkins LLP
Ms Aalia Datoo	Macfarlanes
Dr Andrew Defty	University of Lincoln
Ms Adriana Edmeades	Privacy International
Mr Charlie Edwards	RUSI
Mr Charles Farr OBE	Home Office
Mr Daniel Futter	Metropolitan Police, Directorate of Legal Services
Ms Tessa Gregory	Leigh Day
Mr Stephen Grosz QC (Hon)	Bindmans; Bingham Centre Fellow
Ms Gabrielle Guillemin	ARTICLE 19
Ms Laila Hamzi	Bingham Centre for the Rule of Law
Ms Swee Leng Harris	Bingham Centre for the Rule of Law
Dr Tom Hickman	Blackstone Chambers; Bingham Centre Fellow
Mr Jess Hinings	Ofcom
Ms Sandra Homewood	Bingham Centre for the Rule of Law
Mr Ben Hooper	11 King's Bench Walk
Mr Henry Hughes	187 Fleet Street
Mr Mark Hunting	Ropes & Gray LLP
Mr Ben Jaffey	Blackstone Chambers
Mr Tim Johnston	Brick Court Chambers
Ms Sarah Kavanagh	NUJ
Mr Bernard Keenan	LSE
Mr Eric King	Privacy International
Ms Izza Leghtas	Human Rights Watch
Mr Paul Lomas	Freshfields
Ms Gemma Ludgate	Special Advocates Support Office
Professor Andrew Lynch	University of New South Wales
Mr Daniel Machover	Hickman & Rose
Mr Iain Mackie	Macfarlanes
Ms Jennifer Macleod	Brick Court Chambers
Mr Andy Mather	Macfarlanes
Dr Eric Metcalfe	Monckton Chambers; Bingham Centre Fellow

Ms Helen Mountfield QC	Matrix Chambers
Sir Jon Murphy QPM	Chief Constable, Merseyside Police
Sir David Omand GCB	King's College London
Ms Angela Patrick	JUSTICE
Ms Gillian Phillips	The Guardian
Mr Mark Powell	HM Inspectorate of Constabulary
Ms Charlotte Powell	Furnival Chambers
Dr Tristram Riley-Smith	Centre for Science & Policy, Cambridge University
Mr Matthew Ryder QC	Matrix Chambers
Mr Naz Saleh	Metropolitan Police
Ms Helen Shaw	Inquest
Ms Jessica Simor QC	Matrix Chambers
Mr Graham Smith	Bird & Bird
Ms Justine Stefanelli	Bingham Centre for the Rule of Law
Mr Dominic van der Wal	Special Advocates Support Office
Mr James Welch	Liberty
Ms Harriet Wistrich	Birnberg Peirce & Partners
Mr Julian Wright	Metropolitan Police

BINGHAM CENTRE FOR THE RULE OF LAW

Consultation response to New Zealand Law Commission: National Security Information in Proceedings (Issues Paper 38)

Response by the Bingham Centre for the Rule of Law

Response by the Bingham Centre for the Rule of Law, 30 June 2015

www.binghamcentre.biicl.org

A. Introduction

1. This submission addresses a selection of issues that arise from Issues Paper 38. It covers four main areas:
    - overarching issues about decisions to legislate in the area
    - key protections: sunset clause and periodic review
    - matters relating to open justice, transparency and accountability
    - the expansion of secrecy provisions into criminal proceedings

2. It should be noted that although we pay limited attention to the equality of arms issues, that should not be interpreted as meaning that we see few or no problems with the effects on natural justice or the operation of procedures as they stand in the UK.

3. We begin in section B by addressing the possibility raised by the Commission that New Zealand should not move to legislate to expand secrecy. In the remaining sections we proceed on the basis that New Zealand is likely to enact legislation that will in some form expand secrecy in proceedings.

4. Our recommendations are aimed at putting in place safeguards that aim to combat the most troubling aspects of the laws, trying to provide practical mechanisms that would aid fairness, openness, transparency and accountability. However, in almost all instances, those measures are a second-best alternative. The better alternative is not to depart from core rule of law commitments in the first place.

5. In several instances IP38 raises issues, identifying matters as being very important, but no specific questions are directly stated in relation to those issues. Of note, these occur in relation to:
    - Periodic review (6.96, but no question posed)
    - Open justice (throughout, but especially Ch 2, but only Q 6 posed, which is limited in focus)

    In other instances we raise matters that arise from IP38 and legislation of the type envisioned, but which are not addressed in the paper. In particular:
    - Can closed judgments later be opened when the danger to national security has passed?

The Bingham Centre for the Rule of Law

6. The Bingham Centre for the Rule of Law was launched in December 2010. It is a London-based independent research institute, operating internationally, devoted to the study and promotion of the rule of law worldwide. Its focus is on understanding and promoting the rule of law; considering the challenges it faces; providing an intellectual framework within which it can operate; and fashioning the practical tools to support it. The Centre is named after Lord Bingham of Cornhill KG, the pre-eminent judge of his generation and a passionate advocate of the rule of law. It is part of the British Institute for International and Comparative Law, a registered charity in the UK.

The authors and the background to the submission

7. This submission was prepared by Dr Lawrence McNamara, Senior Research Fellow and Deputy Director of the Bingham Centre for the Rule of Law, and Justine Stefanelli, Maurice Wohl Associate Senior Research Fellow in European Law at the Bingham Centre for the Rule of Law.

8. The submission aims to inform the New Zealand Law Commission's consultation by providing background and analysis of the experience in the UK, where the Justice and Security Green Paper (2011) and the subsequent Justice and Security Bill raised many of the issues that are found in the New Zealand Issues Paper 38 (IP38). The Bingham Centre was involved in

consultations and made submissions in the period leading up to the enactment of the Justice and Security Act 2013, some of which made their way into the legislation.

9. One of the authors of this submission (McNamara) prior to joining the Bingham Centre was separately engaged in consultations and submissions on the Justice and Security Bill while running a major research project at the time, *Law, Terrorism and the Right to Know*, funded by the UK Economic and Social Research Council and based at the University of Reading. He gave evidence to the UK Joint Committee on Human Rights with regard to the effects of laws on media freedom and open justice. Some of the recommendations made their way into the legislation. While at the Bingham Centre, McNamara has continued to research and analyse the operation of the Justice and Security Act 2013 and related matters.

10. The authors hope that this submission largely based on the UK experience will be of assistance to the New Zealand Law Commission in its work, not least with respect to paragraph (f) in the terms of reference about what New Zealand may learn from the experience in foreign jurisdictions. Should it assist the Commission we would be happy to discuss any aspects of the matters we raise.

B. Overarching issues: the need to legislate, sunset clause and periodic review

11. We welcome the New Zealand Law Commission's approach to the issues and, particularly, the view that there should be a cautious approach to the use of closed procedures to minimise the risk that use of such procedures will become normalised.

12. With that in mind, we make three general observations about the need for, and wisdom of, legislation that would enact laws along the lines of those currently operating in the UK and elsewhere.

13. First, while there are increasingly well-established points of comparison on which New Zealand might draw when formulating procedures that will see the expansion of secrecy in civil (and potentially criminal) proceedings – the UK, Canada, Australia among them, and the EU has now adopted rules for closed material proceedings – the Commission is quite right when it states:

> *It is timely for New Zealand to consider how, as a society, we wish to balance these interests of protecting national security and upholding the right to natural justice … This project considers how withholding information on the grounds of national security may affect the fundamental values of natural justice and open justice, and to what degree (<u>if at all</u>) these values should be limited when there is a threat to New Zealand's national security. (Foreword, page iii, emphasis added).*

That is, the Commission appears to have the full suite of options on the table, including whether to legislate at all in the ways that other jurisdictions have done. Although the tenor of IP38 appears to suggest there will be some legislative reform, in our view there is much to be said for seriously exploring the option of maintaining long-established procedures and protections, and not pursuing legislation that would expand secrecy. Put simply, New Zealand should not enact general secrecy provisions based only on the fact that there is currently an international trend toward such legislation.

14. With that in mind, the experience in the UK warrants close attention. In the debates about the Justice and Security Bill there were great concerns about the proposals.

15. A submission by the special advocates (to a consultation process in this country) captures crisply and cleanly the extent to which secrecy in proceedings is a departure from established principles:

> *Our experience as SAs involved in statutory and non-statutory closed material procedures leaves us in no doubt that CMPs are inherently unfair; they do not "work effectively", nor do they deliver real procedural fairness. The fact that such procedures may be operated so as to meet the minimum standards required by Article 6 of the ECHR, with such*

modification as has been required by the courts so as to reduce that inherent unfairness, does not and cannot make them objectively fair.[1]

16. In particular, one special advocate emphasised to the Joint Committee on Human Rights that

> *the public should be left in absolutely no doubt that what is happening... has absolutely nothing to do with the traditions of adversarial justice as we have come to understand them in the British legal system.*[2]

17. The Supreme Court has similarly stated that "unlike the law relating to [public interest immunity], a closed material procedure involves a departure from both the open justice and the natural justice principles."[3]

18. Secondly, as legislation becomes more widespread internationally there is a risk that individual jurisdictions see the question of normalisation not through the lens of enacting legislation, but through the application of the legislation. Such a perception would be both wrong and dangerous. Any moves to legislate to reduce equality of arms, natural justice, openness, accountability are of themselves moves that depart from fidelity to the rule of law and, as the Commission observes, should not be made lightly.

19. Having said that, the application and operation of legislation is of course very important and, in that regard, the UK laws are worrying. There are good reasons to be concerned that there is already 'mission creep' and that the laws are being applied in a wider range of circumstances than might be expected. As a Bingham Centre analysis of the first year of the operation of the Justice and Security Act argued:

> *The Ministry of Justice has stated that [with 5 or 6 applications for CMPs] the powers have been invoked 'sparingly' but that is not an appropriate way to characterise their use. Sparingly is a relative concept. It suggests sparingly in relation to the number of occasions when section 6 declarations could have been sought. But, of course, no evidence is provided in that regard. We do not know whether they have been sought at every turn or only sometimes. All we know is that a declaration has been sought on five occasions in the first year. While it is a small number of cases, the early indications are that CMPs will be deployed in a very, very wide range of circumstances.*
>
> *This is apparent from the kinds of cases where the government has thought a section 6 declaration should be sought. They include claims brought by non-British citizens abroad and by British citizens living in the UK. The claims range from those which relate to the deprivation of liberty to those which concern the imposition of economic sanctions. Some cases are focussed on the past - not least Britain's relationship with the IRA - and others relate to much more contemporary issues such as allegations of recent misconduct by the security services. It seems nothing is off the table and, importantly, we are a long way from the archetypal case that was the impetus for the legislation, which was an action against*

---

[1] Justice and Security Green Paper, 'Response to Consultation from Special Advocates' (16 December 2011), para 15, at <http://webarchive.nationalarchives.gov.uk/20140911100308/http://consultation.cabinetoffice.gov.uk/justiceandsecurity/wp-content/uploads/2012/09_Special%20Advocates.pdf>. The Special Advocates subsequently submitted a response to the Justice and Security Bill in June 2012, which remained critical of CMPs and of the opinion that "the case has not been made for the introduction of closed material procedures in other types of civil litigation" (para 2.1), at <http://www.parliament.uk/documents/joint-committees/human-rights/Special_Advocates_Memorandum_JS_Bill.pdf> (both links accessed 29 June 2015). The use of quotation marks around "work effectively" is a reference to the government's claim in the Justice and Security Green Paper: para 2.3.

[2] Ibid, Response to Green Paper, para 12.

[3] *Al Rawi v The Security Service* [2011] UKSC 34, 14 (Dyson LJ).

the government by returning Guantanamo detainees. In the scope of cases, if not in the number, the use of the powers is anything but 'sparing'.[4]

20. Before moving to legislate at all there are good reasons to wait and see how the effects play out and whether the dangers of normalisation and expansion are realised.

21. Thirdly, New Zealand, like the comparator jurisdictions discussed in IP38, has a strong rule of law culture. It is also, like those comparator jurisdictions, a model for other countries, including those where the rule of law is fragile. If New Zealand joins the jurisdictions that have enacted sweeping secrecy provisions it potentially has an effect that goes beyond its borders.

22. In our view, in spite of the widespread moves to travel these legislative paths, a fundamental question remains: are the laws necessary, justifiable and wise? The fact that other jurisdictions have chosen to enact such laws does not answer that question.

23. A decision to implement legislation of the kind generally envisioned in IP38 would see New Zealand depart from longstanding and fundamental rule of law commitments. Even if the Commission proposes and ultimately secures safeguards that "can help mitigate the impact that non-disclosure … might have on what are fundamental principles of our rule of law system" *(Foreword, iii)*, the enactment of legislation would be profoundly significant.

24. ***Recommendation 1 – not legislating or deferring legislation****: The Law Commission should recommend* ***either*** *that no general secrecy laws be implemented at this point in time or,* ***alternatively****, that the enactment of such provisions be delayed for three to five years, pending a review of the ways the laws unfold in foreign jurisdictions. To do so would be a potentially valuable and influential recommendation.*

C. Key protections: sunset clause and periodic review

25. In the event the Commission takes the view that legislative reform is necessary, it is important to consider that there may come a point in time when either the changes are no longer deemed to be necessary, or when the laws are considered to function poorly. It is therefore important to include provisions in any legislative proposal contemplating these eventualities.

26. Although IP38 commendably marks the need to be cautious in its approach to these issues (6.96), it does not discuss the potential need to include, in any scheme adopted, a legislative provision such that the scheme would have a limited lifespan or be subject to periodic review.

27. ***Recommendation 2 – sunset clause:*** *Any legislative proposal should include a sunset clause which gives the legislation a lifetime of five years.*

28. ***Recommendation 3 – periodic review:*** *The legislative proposal should also include a provision for independent review of the operation of all aspects of the law prior to the expiration of that time period that can be taken into account in the context of any debates on renewal of the legislation.*

29. In the UK the Justice and Security Act includes a provision (section 13) for a five-year review of the operation of sections 6-11 of the Act. While this was a welcome improvement to the Bill during the debates, it still falls some way short of what is desirable and appropriate because it does not require a review of the section 12 reporting requirements or the *Norwich Pharmacal* provisions. As the recommendation above indicates, all aspects of the law should be reviewed.

[4] L McNamara, D Locke and L Hamzi (Bingham Centre for the Rule of Law), 'Closed Material Procedures Under the Justice and Security Act 2013: A Review of the First Report by the Secretary of State' (with Supplement (December 2014) http://binghamcentre.biicl.org/documents/442_cmps_the_first_year_-_bingham_centre_paper_2014-03__supplement.pdf, p 8.

D. Open justice, transparency, accountability: the matters raised in IP38 and the questions asked

30. The Issues Paper (IP38) raises a wide range of important matters. However, the specific questions that are raised do not address all of those matters. Specifically, IP38 points to the importance of open justice and openness, but none of the 23 questions asked relate directly to those concerns. It will be helpful to take these in turn.

31. IP38 includes the following:

- The foreword makes explicit the need to balance national security interests with natural justice principles, including open justice, and that any closed procedures should mitigate the negative impact on rule of law principles.

- Chapter 2 considers a number of interests to be taken into account, and focuses on open justice and the public hearing principle in paragraphs 2.47 to 2.51. In particular, paragraph 2.47 states that "[the principle of open justice] is regarded as an important safeguard against judicial bias, unfairness and incompetence, ensuring judges are accountable in the performance of their judicial duties" and in paragraph 2.48 that open justice must therefore "permeate all political and legal institutions".

32. In some instances, IP38 points out possible solutions (eg, 2.53) However, for the most part the consultation questions do not address open justice and transparency issues. Rather, they direct attention to core themes relating to equality of arms, the respective roles of the Crown and the judiciary in protecting national security and fair trial rights.

33. Only one question (Q 6) raises open justice, and it is framed somewhat narrowly around suppression orders, and only in the criminal context. Some questions leave room indirectly for raising these issues, being framed in terms that could be interpreted as encompassing the open justice issues mentioned above. For instance, question 11 asks what features a single framework should include and what mechanisms might include a fair hearing (though it is fairness to the non-Crown party that seems to be in mind.) Question 23 asks:

> 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? (emphasis added).

The same question is not asked of open justice, but it should be asked whether there are also open justice safeguards that can apply to the legislative regime.[5]

34. The result is that although IP38 pays much more attention to openness than did the UK government's Justice and Security Green Paper, the same criticism may be levelled at IP38 as the Joint Committee on Human Rights made of the UK Green Paper, specifically regarding the significance of open justice and the role of the media:

> It is regrettable that the Green Paper overlooks the very considerable impact of its proposals on the freedom and ability of the media to report on matters of public interest and concern. This is a serious omission. The role of the media in holding the government

[5] The UK Supreme Court made a distinction between open justice and natural justice in *Al Rawi*. Noting that both are "fundamental features of a common law trial", open justice was described as more than a "mere procedural rule", but rather "a fundamental common law principle" and natural justice as a principle upon which the concept of a fair trial is based. Natural justice includes notice and an opportunity to be heard, as well as the ability for parties to call their own witnesses and engage in cross-examination of the other party's witnesses. In doing so, the Court emphasised that "a closed material procedure involves a departure from both open justice and natural justice principles" (as distinguished from the UK framework for public interest immunity, which only strays from the open justice principle) (*Al Rawi*, supra note 3 at 10-15 (Dyson LJ)). Accordingly, the open justice strand warrants attention as a distinct element.

to account and upholding the rule of law is a vital aspect of the principle of open justice, as has been amply demonstrated in the decade since 9/11.[6]

35. Against that background, we now raise several issues that identify problems relating to open justice, transparency and accountability, and make recommendations that may go some way to addressing the shortcomings and difficulties that arise in legislative attempts to implement secrecy in proceedings.

E. Balancing interests: natural justice, open justice, national security

36. IP38 notes at 5.26 that the Justice and Security Act requires judges to balance national security against 'the fair and effective administration of justice in the proceedings'. The background to this factor – the fair and effective administration of justice – warrants attention. It reveals a deep flaw in the Act.

37. In the Green Paper[7] and in the Bill as originally introduced on 29 May 2012 there was no provision for balancing at all.[8]

38. The Joint Committee on Human Rights recommended that 'open justice' be an express criterion for consideration by the courts when engaging in a balancing exercise to determine whether to grant an application for CMPs.[9] Amendments were proposed to give effect to that recommendation, with the balance to be against the 'fair and open administration of justice', thus taking account of both natural justice and open justice. The Bill as amended by the Lords on report included an open justice provision (Cl 6(2)(c)).[10]

39. In the Commons the government successfully moved 'fair and effective adminsitration of justice in the proceedings' as an alternative amendment.[11]

40. 'Effective' is quite plainly not the same as 'open'.

41. Opposition and crossbench amendments were tabled again in the Commons and the Lords to secure 'fair and open' as the balancing criterion. Although the open justice amendments secured support across the political spectrum, the government ultimately prevailed and the 'fair and open' amendment was defeated 174-158 votes in the Lords.

42. The UK legislature therefore very explicitly – and very unsatisfactorily – removed the consideration of open justice as a matter to be taken into account by the courts in any balancing exercise.[12] The explanations of why this is such a problematic shortcoming are explained by parliamentarians of all stripes.

---

[6] Joint Committee on Human Rights, 'The Justice and Security Green Paper', Twenty-fourth Report of Session 2010-2012, HL Paper 286, HC 1777 (4 April 2012) para 217.
[7] HM Government, 'Justice and Security Green Paper' (October 2011) Cm 8194
[8] Justice and Security Bill [HL] as introduced, 29 May 2012 http://www.publications.parliament.uk/pa/bills/lbill/2012-2013/0027/13027.pdf.
[9] Joint Committee on Human Rights, 'The Justice and Security Green Paper', Twenty-fourth Report of Session 2010-2012, HL Paper 286, HC 1777 (4 April 2012) paras 215-16.
[10] Justice and Security Bill [HL] as amended on report (23 November 2012), Cl 6(2)(c) http://www.publications.parliament.uk/pa/bills/lbill/2012-2013/0056/130056.pdf.
[11] Justice and Security Bill [HL] as amended in Public Bill Committee (8 February 2013), Cl 6(6) http://www.publications.parliament.uk/pa/bills/cbill/2012-2013/0134/2013134.pdf
[12] By way of comparison, the Australian Law Reform Commission recommended that open justice be a consideration in national security laws: Keeping Secrets: The Protection of Classified and Security Sensitive Information, ALRC Report 98 (2004), Recommendation 11-19 and generally [7.15]-[7.41]; see also recommendation 7- 1 on non-party access. However, the Australian parliament did not follow that recommendation in enacting the National Security Information (Civil and Criminal Proceedings Act) 2004; the Act (eg, Ss 31, 38L) does not include open justice as a criterion and that is a significant weakness.

43. As Conservative peer Baroness Berridge put it when arguing for the 'fair and open' amendment:

> As this is such an irregular trial procedure to adopt, it should be a competition of interests, a battle even for the Government to show that national security outweighs fair and open justice and that the nature of these proceedings is so unusual and so contrary to our principles of a fair trial that it should be only when nothing else is possible.[13]

44. Labour leader in the House of Lords, Lord Beecham, explained the concerns succinctly:

> Openness is therefore replaced by effectiveness, a very different concept. Effective, one might ask, from whose perspective? Is it that of the party, presumably the Government? Openness now counts for nothing. The phrase "in the proceedings" is added, excluding the wider considerations of the public interest. The concept of balancing the two interests disappears.[14]

45. Former DPP and Liberal-Democrat peer Lord Macdonald of River Glaven said:

> In short, the judge must be empowered and permitted to pay heed to the public interest in open justice when he is faced with a government application to go into closed session. That is because closed justice is, on the face of it, so inimical and contrary to our long traditions of fair process, and openness and transparency in justice, so intrinsic to our way of life and our legal processes, that to close down a court, to expel a claimant, without first balancing the virtues of justice being seen to be done is, or should be, unthinkable. [15]

46. Former Treasury Counsel and Intelligence Services Commissioner Lord Brown of Eaton-under-Heywood said:

> This legislation involves so radical a departure from the cardinal principle of open justice in civil proceedings, so sensitive an aspect of the court's processes, that everything that can possibly help minimise the number of occasions when the power is used should be recognised and should appear in the legislation itself.[16]

47. ***Recommendation 4 – open justice as a criterion in legislation****: Open justice should be a part of any legislative framework that might be adopted. It should expressly be a criterion to be taken into account in balancing.*

48. A formulation used in the Justice and Security Bill [HL], as amended on report was the following: Cl 6(2)(c) where a condition of closed material proceedings was that the "degree of harm to the interests of national security if the material is disclosed would be likely to outweigh the public interest in the fair and open administration of justice." Added to that was Cl 6(2)(d): "a fair determination of the proceedings is not possible by any other means."

F. Open justice and media scrutiny as part of democratic accountability

49. Courts are vitally important avenues for scrutiny and accountability, especially in matters relating to terrorism and security, where the authorities will inevitably be reluctant to disclose information that does not support their case and where individuals and communities will be unlikely to provide information. It can be almost impossible to test the information that is available or which is provided by the authorities. In courts, however, there are rules of evidence and disclosure, and open justice principles, that combat the inevitably incomplete and quite possibly misleading information that journalists can obtain.

50. The following extract from a recent empirical study by one of the authors outlines the significance of the issues in the criminal context, but the same themes apply in civil proceedings of all kinds where the behaviour of the state and of individuals is under scrutiny.

---

[13] Hansard HL Deb, 26 March 2013, Col 1035.
[14] Ibid, Col 1027.
[15] Ibid, Col 1029
[16] Ibid, Col 1032

> Trials are about contested versions of events. The Crown has alleged a person has committed criminal offences and the accused person has pleaded not guilty. However, not every issue is contested. On the contrary, much will be uncontested and a 'much more firm' factual picture will emerge in court, as one journalist explained:
>
> > Agreed statements, admissions, facts that are just completely indisputable . . . You get the amounts of money. [You get] the travel patterns – he went here, he went there. [You get] the emails. All of that stuff comes out and that's gold dust really.
>
> The authorities will almost certainly be pleased that this kind of uncontested information is in the public domain, even if it is many months after the arrests. At trials, journalists will 'get to see sensitive material' 61 and will hear first-hand accounts:
>
> > No matter how many miles you walk and no matter how many people you speak [to at the end of the day] the best stuff always comes out. [Y]ou've got the defendant speaking for themselves, or the defendant's mother speaking. You've got the cops speaking. You've got a cop saying, 'Well, I broke down the door and this is what I saw.'
>
> This, for reporters, is a part of democratic public scrutiny: 'That stuff only ever comes out in court and court reporting is so important it is fundamental to our democracy.' … In court,
>
> > 'Instead of getting the embellished stuff and the spin and the bullshit you get . . . what they have to tell the jury. That's limited to an extent but you do get more facts and I think more reliable information.'[17]

51. Even if imperfect, the courts are absolutely crucial avenues for obtaining information of great public interest. In terrorism and security matters, where information will be closely guarded by the state, the ability to adequately report court cases is essential if scrutiny of government is to be effective, if the threat of terrorism is to be understood, and if the public is to have confidence in the way that such threats are addressed.

52. There will inevitably be questions raised as to whether whether arguments that raise open justice issues are in some ways suggesting that open justice should trump all other factors. The answer is no, it should not trump all other factors. However it should be the starting point that openness is preferable, is the default position, and that what can be made public should be made public.

53. In a not dissimilar vein there will also be questions raised about whether journalists are responsible and trustworthy. From the same study, it is clear that any such suggestions are misguided:

> Are journalists reckless about managing information relating to terrorism and security? The answer is, resoundingly, 'no'. Do journalists view their roles uncritically? Again, clearly, 'no'. An accountable and responsible state should not fear the media where national security or natural justice are at issue. In the practice of journalism, as it emerged in the research interviews, the public interest in openness and the application of open justice principles are of vital importance, but they are ultimately secondary and will yield to primary priorities of natural justice and the public interest in national security. However, state controls over information currently make the gulf between these primary and secondary commitments unacceptably and unhealthily wide. There is still considerable scope to maintain and improve access to information before either natural justice or national security is threatened.[18]

[17] L McNamara, 'Secrecy, the media and the state: controlling information about terrorism and security' in G Martin, R Scott-Bray and M Kumar, *Secrecy, Law and Society*, Routledge, 2015, ch 8 (pp 139-157) at 148-149. See also on the Australian experience, L McNamara, 'Closure, caution and the question of chilling: how have Australian counter-terrorism laws affected the media?' (2009) 14 Media and Arts Law Review 1-30.

[18] L McNamara, 'Secrecy, the media and the state: controlling information about terrorism and security' in G Martin, R Scott-Bray and M Kumar, *Secrecy, Law and Society*, Routledge, 2015, ch 8 (pp 139-157) at 153-154.

G. Recognising media interests to give effect to open justice principles

54. IP38 references media issues peripherally in connection with discussion of specific statutes, such as that on suppression orders in criminal law matters (3.34), a discussion of the UK experience in the *Incedal* case (5.35) (though refers to that case as being related to CMPs, whereas it was quite different) and with regard to existing types of protection orders that may result in exclusion of the media from the court room (6.50). It also acknowledges in paragraph 2.52 that despite the value of public proceedings, it may be necessary in light of national security interests to exclude the media (and others) from all or part of the proceedings.

55. The ability of the press to access and report information is an integral part of the public's right to know. The right to know extends to both the accountability of the state and the activities of those who have been subject to the coercive powers of the state.

56. As mentioned above in paragraph 34, the UK Justice and Security Green Paper was criticised by the Joint Committee on Human Rights for failing to take into account "the very considerable impact of its proposals on the freedom and ability of the media to report on matters of public interest and concern", and was considered "a serious omission".[19]

57. Given that the media is effectively the eyes and ears of the public in courts, any proposal for closed procedures should therefore take into account:

- the ability of the press and public to know about important matters of public interest;
- the public confidence in the judiciary that flows from transparency; and
- the ability of the parties, the public, the press and researchers to see and analyse material even after secrecy is no longer needed.

Notice and opportunity to make submissions (non-parties)

58. IP38 does not contemplate the possibility for non-parties to receive notice of applications for closed proceedings and to make submissions on such applications. The role of non-parties in this regard is vital especially in cases where the parties may have agreed that closed procedures are appropriate, whether or not disclosure would be damaging to national security. This may be especially so if gisting (or similar) is used.

59. ***Recommendation 5 – notice to media and a right to be heard****: For open justice to be meaningful in these circumstances, any legislative proposal should ensure that the media receive notice of applications to use closed material proceedings (or the like) and that media interests or others with open justice interests (eg, professional associations, NGOs) have a right to be heard at each stage.*

60. For the above recommendation we suggest a notice period of 7 days may be appropriate. We base that figure on the period prescribed under the UK Criminal Procedure Rules, Rule 16.10 where court closures are sought on national security grounds. A subscription-based email alert would be one possible method.

61. By way of illustration, in the UK an amendment was tabled by Crossbench, Conservative and Liberal-Democrat peers which would give effect to this:

> "( ) Rules of court relating to section 6 proceedings must make provision—

[19] Joint Committee on Human Rights, 'The Justice and Security Green Paper', Twenty-fourth Report of Session 2010-2012, HL Paper 286, HC 1777 (4 April 2012) para 217.

(a) requiring the court concerned to notify relevant representatives of the media of proceedings in which an application for a declaration under section 6 has been made,

(b) providing for any person notified under paragraph (a) to be permitted to intervene in the proceedings,

(c) providing for a stay or sist of relevant civil proceedings to enable anyone notified under paragraph (a) to consider whether to intervene in the proceedings,

(d) enabling any party to the proceedings or any intervener to apply to the court concerned for a determination of whether there continues to be justification for not giving full particulars of the reasons for decisions in the proceedings, and

(e) requiring the court concerned, on an application under paragraph (d), to publish such of the reasons for decision as the court determines can no longer be justifiably withheld."[20]

H. Open statements for closed judgments

62. It is important to systematically record the scale of the use of secret evidence as a matter of democratic accountability. Such information should be recorded in a manner that is sufficient so as to enable a lawyer, researcher or journalist to ascertain from publicly available information the types of situations in which closed procedures are sought and to make a judgment about whether the report is accurate and comprehensive.

63. ***Recommendation 6 – open statements to accompany closed judgments:*** *Any legislative proposal should include a provision that requires closed judgments to be accompanied by a clear and perhaps template-form statement that requires a court to record as an open statement:*

- *the duration of open hearings and closed hearings;*
- *the number of witnesses heard in closed proceedings and the nature of those witnesses;*
- *the length of a closed judgment;*
- *whether national security was an issue in the proceedings;*
- *whether submissions were received from media or other non-party interests.*

64. By way of illustration in the UK, in the UK an amendment was tabled by Opposition peers which would give effect to this

"Open statements for closed judgments

Closed judgments must be accompanied by an open statement from the court, which shall include—

(a) the reasons for the closed material procedure;

(b) any factors which would be particularly relevant in determining whether all or part of the closed judgment could be made open at a later date;

(c) the duration of open hearings and closed hearings;

(d) the number of witnesses heard in closed proceedings, and the nature of those witnesses;

(e) the length of a closed judgment;

[20] Amendment 69ZA, Baroness Berridge, Lord Pannick, Lord Lester of Herne Hill, Fourth marshalled list of amendments to be moved in Committee of the whole House, 27 June 2012, http://www.publications.parliament.uk/pa/bills/lbill/2012-2013/0027/amend/ml027-iv.htm

(f) whether national security was an issue in the proceedings; and

(g) the date at which the closed status of the judgment should be reviewed, which must be no later than five years from the date of the judgment."[21]

65. The final provision in the above amendment relates also to the further recommendation below on Opening Up Closed Judgments. All provisions in the above would provide material which could be consolidated in annual reports.

I. Reporting to parliament

66. IP38 raises briefly the issues of reporting, noting at 6.96 that the legislative framework 'could probably contain provisions requiring periodic reports on the use of those procedures.' Such reporting should be essential and the legislation should be prescriptive.

67. Such a requirement did not feature in the Green Paper or the Justice and Security Bill as introduced, and this shortcoming was criticised during debate on the Bill.[22] Ultimately, the Justice and Security Act included in section 12 a requirement of the Secretary of State to make an annual report stating how often in the preceding 12 months applications for closed material procedures were made, grated and revoked, and how many of the associated final judgments are closed or not closed.[23] However, experience has revealed problems with the reporting regime.

68. As the Bingham Centre argued in its analysis of the first report by the Secretary of State after one year of operation of the Act:
- The information reported was not sufficient to enable to a meaningful understanding of how closed proceedings had been used.
- More information could have been provided under section 12(3) but was not provided, even though information was in the public domain and would clearly not have damaged national security.
- The information reported was not accurate, with the Secretary of State reporting only five of the six occasions on which a CMP declaration was sought. [24]

69. ***Recommendation 7 – reporting to Parliament****: Subject only to any secrecy requirements imposed by the courts or unless the fact of identifying the cases would imperil national security, Parliament should require that the relevant Minister report annually on the use of closed proceedings and that reports should at least state:*
- *the cases in which closed material proceedings (or the relevant type of provision for New Zealand) were sought*25

[21] Amendment 67C, Lord Beecham, Baroness Smith of Basildon, Third marshalled list of amendments to be moved in Committee of the whole House, 27 June 2012, http://www.publications.parliament.uk/pa/bills/lbill/2012-2013/0027/amend/ml027-iii.htm

[22] HL Hansard, 19 June 2012, Col 1712 (Lord Hodgson).

[23] A closed judgment is defined in section 12(5) as "a judgment that is not made available, or fully available, to the public".

[24] L McNamara, D Locke and L Hamzi (Bingham Centre for the Rule of Law), 'Closed Material Procedures Under the Justice and Security Act 2013: A Review of the First Report by the Secretary of State' (with Supplement (December 2014) http://binghamcentre.biicl.org/documents/442_cmps_the_first_year_-_bingham_centre_paper_2014-03__supplement.pdf. We note also in this context that where IP38 (at 5.34) cites the Bingham Centre analysis of the first report, IP38 states that there were five applications of which three were successful. That summary does not capture the full picture. There were six applications, and the government failed on none. It succeeded on four (*CF & Mohamed*, *McGartland*, *Sarkandi*, *Al Ghabra*), a fifth did not need to be decided (Youssef), and a sixth had not been decided at the time of our analysis (*McCafferty*): pp 4-6, 10.

[25] This is in parallel to section 47(b) of the Australian National Security Information Act 2004, which requires identification of the "criminal proceedings and civil proceedings to which the certificates relate".

- *the dates on which applications were made*
- *whether any media or non-party submissions were made*
- *the outcomes of the applications*
- *the citations of the judgments that determined proceedings*
- *where there are reasons why this information cannot be included in the report, the Minister should be required to state those reasons in the report.*

J. Opening up closed judgments

70. IP38 does not consider the possibility that closed judgments might later be opened. Without such a provision, there is a real risk that the material in closed judgments may remain secret long after secrecy is no longer necessary.

71. ***Recommendation 8 – statements to assist review and maximum date before review:*** *Any legislative proposal should include a provision requiring that closed judgments are accompanied by a statement from the court (open where possible, closed where necessary) that includes:*
    - *the reasons for closure of the judgment;*
    - *any factors that would be particularly relevant in determining whether all or part of the closed judgment could be made open at a later date;*
    - *the date at which the closed status of the judgment should be reviewed, with 5 years being the maximum period before review.*

72. ***Recommendation 9 - reviewers****: We recommend that the legislative proposal should ensure that the person who reviews closed judgments is clearly independent from the Executive and is clearly identified. This person may be the original judge in the case, but a retired judge may be a suitable alternative.*

73. By way of illustration, in the UK, the House of Lords considered an amendment (67C) which included a proposal that would allow for closed judgments to be reviewed at a later date.[26] Although the Government accepted there was an issue at stake, acknowledging 'the force of what has been said',[27] the Act as passed did not include any such provision, as the general tenor of the debate was that constructing a system of review would be too difficult.[28]

74. Following the entry into force of the Justice and Security Act, an attempt was made before the High Court to establish general guidance regarding the opening of closed judgments.[29] The Court refused, stating that Parliament had had the opportunity to legislate accordingly and had declined to do so, and therefore that fact should be taken as a signal that the courts should not be offering judicial guidance.[30] The corollary is that it is an important issue for a Parliament to consider.

[26] HL Hansard, 17 July 2012, Col 206.
[27] Ibid Col 209: "I want to revisit this matter and discuss it with officials because I recognise the point that has been made. I am not going to pretend that there may be an easy answer to it, but if there is no longer a national security consideration, I see the force of what has been said."
[28] Ibid Col 210: "The second point is very much one of detail. Who would determine whether there was, in fact, no longer a national security consideration? Where would the responsibility lie? That is the very issue that I want to consider, because how that would be addressed does not readily present itself to me. I sought to indicate that there is an issue here. I am not pretending for a moment that there is an easy answer, but the issue is important to consider."
[29] *R (Evans) v Secretary of State for Defence* [2013] EWHC 3068 (Admin).
[30] Ibid 41.

K. Criminal proceedings

75. IP38 rightly acknowledges (at 5.35) the recent experience in the UK terrorism-related prosecution in the *Incedal* case.[31] The discussion in that paragraph somewhat conflates the secrecy measures taken in that criminal case with those associated with CMPs (which are used in civil proceedings under the Justice and Security Act 2013). Having said that, *Incedal* is not unrelated to broader concerns about CMPs. But for a trend which has seen secrecy normalised with the enactment of the Justice and Security Act, it is difficult to imagine the prosecution seeking to have an entire case heard in secret, or a first instance Court permitting it, or even the Court of Appeal permitting such extensive secrecy.

76. The measures imposed by the Court of Appeal (which included requiring journalists' notes to be locked away in a safe in the court following each day's proceedings, and then later in secure storage at MI5) were criticised by many commentators. Reporters were prevented from informing the public as to the proceedings and faced prosecution for contempt of court and possibly also imprisonment if they disobeyed the suppression order.

77. This case, which has been labelled 'unprecedented' in terms of secrecy[32] serves as an example of the potential for secrecy to become the default.

78. One of the authors of this submission has written three short pieces on the *Incedal* case and the following recommendation draws on the points made in those pieces.[33] In sum, the *Incedal* trial sets a bad precedent and is a major and unjustifiable departure from rule of law standards.

79. Among the many difficulties that arise, one of particular note is that while the media are considered (and this is important), there are no other safeguards considered. Of at least equal importance – and perhaps of far more importance – there was no consideration of seeking or allowing attendance by organisations who may be able to offer valuable insights into the extent to which the proposed process protects and is consistent with the rule of law. The court notes that, "The Rule of law is a priceless asset of our country and a foundation of our Constitution. One aspect of the Rule of Law – both a hallmark and a safeguard – is open justice." This would be enhanced if professional bodies such as the Law Society or the Bar Council were invited to have an independent observer attend the trial. Similarly, NGOs working in the areas of open justice and human rights might be invited to have observers attend. They would of course be subject to any undertakings of confidentiality that apply to others.[34]

80. ***Recommendation 10 – criminal cases:*** *New Zealand's current system of handling national security information in criminal proceedings should be retained, rather than moving to procedures that allow for Incedal-style trials.*

---

[31] *Guardian News and Media Ltd v Incedal* [2014] EWCA Crim 1861.
[32] Ian Cobain, 'Erol Incedal trial: media groups dispute refusal to lift reporting restrictions' *The Guardian* (16 April 2015).
[33] L McNamara, 'Secret Trials: Secrecy at the Expense of Justice' *Inforrm*, 7 June 2014, https://inforrm.wordpress.com/2014/06/07/secret-trials-secrecy-at-the-expense-of-justice-lawrence-mcnamara/; L McNamara, Secret Trials: A Little Transparency, A Lot to Worry About' *UK Human Rights Blog*, 12 June 2014 http://ukhumanrightsblog.com/2014/06/12/secret-trials-a-little-transparency-a-lot-to-worry-about-lawrence-mcnamara/; L McNamara, 'How open will this newly opened justice be?' *Inforrm*, 14 June 2014, http://inforrm.wordpress.com/2014/06/14/how-open-will-this-newly-opened-justice-be-lawrence-mcnamara/
[34] L McNamara, Secret Trials: A Little Transparency, A Lot to Worry About' *UK Human Rights Blog*, 12 June 2014 http://ukhumanrightsblog.com/2014/06/12/secret-trials-a-little-transparency-a-lot-to-worry-about-lawrence-mcnamara/

L. Summary of Recommendations

81. We recommend as follows:

1. The Law Commission should recommend **either** that no general secrecy laws be implemented at this point in time or, **alternatively**, that the enactment of such provisions be delayed for three to five years, pending a review of the ways the laws unfold in foreign jurisdictions. To do so would be a potentially valuable and influential recommendation.

2. Any legislative proposal should include a sunset clause which gives the legislation a lifetime of five years.

3. The legislative proposal should also include a provision for independent review of the operation of all aspects of the law prior to the expiration of that time period that can be taken into account in the context of any debates on renewal of the legislation.

4. Open justice should be a part of any legislative framework that might be adopted. It should expressly be a criterion to be taken into account in balancing.

5. For open justice to be meaningful in these circumstances, any legislative proposal should ensure that the media receive notice of applications to use closed material proceedings (or the like) and that media interests or others with open justice interests (eg, professional associations, NGOs) have a right to be heard at each stage.

6. Any legislative proposal should include a provision that requires closed judgments to be accompanied by a clear and perhaps template-form statement that requires a court to record as an open statement:
    a. the duration of open hearings and closed hearings;
    b. the number of witnesses heard in closed proceedings and the nature of those witnesses;
    c. the length of a closed judgment;
    d. whether national security was an issue in the proceedings;
    e. whether submissions were received from media or other non-party interests.

7. Subject only to any secrecy requirements imposed by the courts or unless the fact of identifying the cases would imperil national security, Parliament should require that the relevant Minister report annually on the use of closed proceedings and that reports should at least state:
    a. the cases in which closed material proceedings (or the relevant type of provision for New Zealand) were sought
    b. the dates on which applications were made
    c. whether any media or non-party submissions were made
    d. the outcomes of the applications
    e. the citations of the judgments that determined proceedings
    f. where there are reasons why this information cannot be included in the report, the Minister should be required to state those reasons in the report.

8. Any legislative proposal should include a provision requiring that closed judgments are accompanied by a statement from the court (open where possible, closed where necessary) that includes:
    a. the reasons for closure of the judgment;
    b. any factors that would be particularly relevant in determining whether all or part of the closed judgment could be made open at a later date;
    c. the date at which the closed status of the judgment should be reviewed, with 5 years being the maximum period before review.

9. We recommend that the legislative proposal should ensure that the person who reviews closed judgments is clearly independent from the Executive and is clearly identified. This person may be the original judge in the case, but a retired judge may be a suitable alternative.

10. New Zealand's current system of handling national security information in criminal proceedings should be retained, rather than moving to procedures that allow for Incedal-style trials.