Name: Darren Ackermann Brookbanks
Student number: BRKDAR003
Qualification: MPhil Public International Law
Title: 'International Regulation of Foreign Intelligence Liaison'
Supervisor: Cathleen Powell
Word count: 19 186

A research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the degree of MPhil Public International Law in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of MPhil Public International Law dissertations, including those relating to length and plagiarism, as contained in the rules of this university, and that this dissertation/research paper conforms to those regulations.

DECLARATION:

1. I know that plagiarism is wrong. Plagiarism is to use another's work and to pretend that it is one's own.
2. I have used the footnote convention for citation and referencing. Each contribution to, and quotation in, this essay/report/project/ … minor dissertation… from the work(s) of other people has been attributed, and has been cited and referenced.
3. This essay/report/project/ … minor dissertation … is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.
5. I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is my own work.

Signature: …… Date: 11/09/15

Table of Contents

ABBREVIATIONS

African Commission	African Commission on Human and Peoples Rights
African Court	African Court on Justice and Human Rights
AIVD	State Secret Service
Banjul Charter	African Charter on Human and Peoples Rights
BRICS	Brazil-Russia-India-China-South Africa
CIA	Central Intelligence Agency
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
GCHQ	Government Communications Headquarters
GILAB	General Intelligence Laws Amendment Bill
HUMINT	Human intelligence
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the Former Yugoslavia
IMF	International Monetary Fund
IPT	Investigatory Powers Tribunal
ISA	Intelligence Services Act
MI5	Military Intelligence 5
MI6	Military Intelligence 6
NATO	North Atlantic Treaty Organisation
NCC	National Communications Centre
NCC Bill	National Strategic Intelligence Amendment Bill
NGO	Non Governmental Organisation
NIA	National Intelligence Agency
NIA Policy	NIA Directive on Communications Monitoring and Interception
NSA	National Security Agency
NSIA	National Strategic Intelligence Act
NZ	New Zealand
Protocol	Protocol on the Statute of the African Court of Justice and Human Rights
RICA	Regulation of Interception of Communications and Provision of Communications-related Information Act
RIPA	Regulation of Investigatory Powers Act
SASS	South African Secret Service
SASS Policy	SASS Policy on Interception of Communications
SIGINT	Signals intelligence
SSA	State Security Agency
TDIP	Transport and Illegal Retention of Prisoners
The BILL	General Intelligence Laws Amendment Bill
UK	United Kingdom
UN	United Nations
UNSC	United Nations Security Council
UNIIIC	United Nations International Independent Inquiry Commission

US	United States
WB	World Bank

INTRODUCTION

Edward Snowden is a hero. In 2013, he leaked what can arguably be considered as the greatest quantity of classified and top-secret foreign intelligence in history. The leak revealed the extent of pervasive global government surveillance that has been and continues to be conducted by foreign intelligence agencies such as the National Security Agency (NSA) in the United States and the Government Communications Headquarters (GCHQ) in the United Kingdom. His actions have led to international security sector reform of the international regulation of foreign intelligence liaison.

Citizen Four, the 2015 Oscar award-winning documentary, is the story of Snowden. When asked by Glen Greenwald and Laura Poitras, the journalist and documentarian who covered his journey, why he did what he did, Snowden's response was that:

> '[I]t all comes down to state power against the people's ability to meaningfully oppose that power ... if the policy switches that are the only thing that restrain these states were changed, you couldn't meaningfully oppose these … that hardened me into action.'[1]

When closing a TED talk on how we take back the internet, Snowden's idea worth sharing was that:

> '… [D]emocracy may die behind closed doors but we as individuals are born behind those same closed doors … We don't have to give up our privacy to have good government … We don't have to give up our liberty to have security … By working together, we can have both open government and private lives ….'[2]

The relationship between state power and people's opposition, the individual and democracy, privacy and good government, liberty and security are themes that run throughout this dissertation. They are thematic relationships that underlie the importance of the international regulation of foreign intelligence liaison. The international regulation of foreign intelligence liaison will continue to be shaped by these relationships.

Chapter I picks up on these themes by reviewing the international regulation of foreign intelligence liaison as a phenomenon. Part II defines foreign intelligence,

---

[1] L Poitras. *Citizen Four, Documentary* (2014 Radius TWC).

[2] E Snowden. 'Edward Snowden: Here's how we take back the Internet' *Ted Talk* 2014, available athttp://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet?language=en#t-2034380 (accessed on 25 August 2015).

part III sets up the objectives of a regime for international law in liberal democracies, part IV recognises the challenges to effective oversight of foreign intelligence agencies and part V maps out different reasons for and uses and forms of foreign intelligence liaison. A core argument is that the inevitable abuse and misuse of foreign intelligence liaison should be regulated through a horizontal accountability mechanism as an international best practice.

Chapter II focuses on the international regulation of foreign intelligence liaison through a legal analysis. It draws on the themes by summarising (part II) and critiquing (part III) two landmark judgments having the potential to set an international best-practice precedent that contributes to the international regulation of foreign intelligence liaison. The core argument is that communications interception warrants should be regulated by judicial pre-authorisation. This is a practical application of Chapter I's core theoretical argument mentioned above.

Chapter III develops these themes by analysing the international regulation of foreign intelligence liaison through recommendations. Part II explores the regulation of signals intelligence (SIGINT) in South Africa. Part III sets out the national and regional applications of art 17 of the ICCPR with regard to private communications. Finally, by summarising and applying the core arguments of Chapters I and II to Chapter III, part IV recommends legal reform through a General Intelligence Laws Amendment Bill 2015 (the Bill).

CHAPTER I: INTERNATIONAL REGULATION OF FOREIGN INTELLIGENCE LIAISON: THE PHENOMENON

I INTRODUCTION

This chapter reviews the international regulation of foreign intelligence liaison. It initially maps out a suggested definition of foreign intelligence liaison, sets out the objectives of a regime for international law in liberal democracies and recognises the challenges to effective oversight of foreign intelligence agencies. International co-operation of foreign intelligence agencies, the globalisation of foreign intelligence liaison and intra-alliance foreign intelligence liaison are then explored. An analysis is subsequently advanced of the utility of international intelligence co-operation; this includes a comparison of different forms of foreign intelligence liaison and methods of managing bilateral intelligence liaison. The analysis is rounded off with an example of foreign intelligence liaison via rendition.

Finally, the costs and benefits of foreign intelligence liaison are assessed and recommendations are made as to how mistrust over foreign intelligence liaison can be overcome.

II DEFINING FOREIGN INTELLIGENCE

Intelligence is

> 'a specialised subset of information that meets the stated or understood needs of policy makers and has been collected, analysed and disseminated to support a state's decision and policy makers.'[3]

In the context of foreign intelligence reform, intelligence is 'the production of unbiased information about (external) threats to the national vision'.[4] Foreign intelligence is required by states as some states or international actors hide information harmful to another state's national security from other states or international actors. States attempt to gather this information either secretly or covertly.

---

[3] G Hannah, KA O'Brien & A Rathmell. 'Intelligence and Security Legislation for Security Sector Reform' *Technical Report for the United Kingdom's Security Sector Development Advisory Team* (2005, Rand Corporation, Cambridge) 1.

[4] Ibid.

Whether as a process, an organisation or a product, intelligence can take on the form of:

- national
- strategic
- tactical
- foreign and security intelligence
- counterintelligence
- counterespionage
- assessment, or
- covert action intelligence.

The immediate or long-term foreign intelligence product delivered to customers to support decisions on foreign targets and external threats is driven by the need to know the intentions, capabilities and activities of other states. Foreign intelligence organisations, functionally structured to undertake the intelligence process of collecting, processing, analysing and disseminating intelligence relevant to external security, need to forecast threats, risks, events and outcomes. An analysis of foreign intelligence is primarily focused on the human intelligence (HUMINT) and signals intelligence (SIGINT) means of collection. This dissertation focuses primarily on the international regulation of foreign SIGINT liaison.

The South African National Communications Centre (NCC) Bill defined foreign SIGINT as:

> '… intelligence derived from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals, and includes any communication that emanates from outside the borders of the Republic, or passes through or ends in the Republic.'[5]

The pre-emption and prevention of forecast attacks by terrorist cells and rogue states would not be possible without improving effective HUMINT and SIGINT intelligence collection.[6]

In liberal democracies, foreign intelligence requires a clear mandate, central co-ordination, oversight and accountability, and independent judicial and

[5] National Strategic Intelligence Amendment Bill [B 38-2008].
[6] Hannah et al (note 3) 1–2, 5–6.

parliamentary oversight and accountability. This is because – notably in the United Kingdom and the United States – the separation of powers principle is a founding principle of such liberal democracies. While control 'set(s) out the constraints under which a (foreign) intelligence agencies operate',[7] accountability 'is an information process whereby (foreign) agencies are under a legal obligation to answer truly and completely the questions put to it by an authority to which it is accountable'.[8] However, only some states have written legislation that regulates their foreign intelligence agencies. Though central co-ordination and independent parliamentary oversight and accountability are more applicable to security intelligence agency reform, foreign intelligence agencies can be pressured to be regulated by legislative oversight through international courts such as the European Court of Human Rights, or have reform pressure exerted on them by donor organisations such as the International Monetary Fund (IMF) or the World Bank (WB).[9]

III OBJECTIVES OF A REGIME FOR INTERNATIONAL LAW IN LIBERAL DEMOCRACIES

Foreign intelligence agencies are crucial to the safeguarding of the state, its people and its institutions. However, the nature of their work can infringe the founding values of liberal democracies. An example of a founding value would be the rule of law. While a delicate balance exists between neither compromising national security nor undermining democratic principles, states should theoretically create a 'democratic control, oversight and review'[10] regime of the work of foreign intelligence agencies.

Though the primary purpose of this regime should be to enhance the legitimacy of the activities of a state's foreign intelligence agency, the objectives of this regime should be to inspire public confidence by guaranteeing that a foreign intelligence agency works with 'propriety, effectiveness, transparency and government accountability'.[11] The essential elements of this regime are statutory,

[7] Hannah et al (note 3) 12.
[8] Ibid.
[9] Hannah et al (note 3) 39.
[10] A Wright. 'Casting a Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight, and Review.' In N LaViolette & C Forcese (eds) *The Human Rights of Anti-terrorism* (2008, Irwin Law, Toronto) 328–329.
[11] Wright (note 10) 333–334.

judicial and supplementary controls such as international instruments, executive accountability and independent and legislative review bodies. These principles are set out in the Ottawa Principles on Anti-terrorism and Human Rights.[12] However, although these principles were adopted at a conference as a model for best practice, they have not yet been recognised as an international standard.

There are divergent views surrounding the independence of intelligence from policy bias. A three-pronged framework for identifying accountability solutions to this challenge has been offered: horizontal, vertical and third-dimensional:[13]

> 'Horizontal accountability refers to the restraint of state institutions by other state institutions, public agencies and the three branches of government (executive, legislative and judiciary) … vertical accountability concerns the hierarchical relationship between senior officials (principals) and their subordinates (agents) within a state institution … (and) third dimension refers to the role of international actors in holding a state institutional actor to account.'[14]

It is the horizontal and third-dimensional accountability solution that become relevant as a guide for international law to be used by international actors in order to hold foreign intelligence agencies accountable.

In international law, although there are statutory controls such as treaties, custom, principles and case law, and judicial controls like that of the International Court of Justice (ICJ), ad hoc tribunals and international courts such as the International Criminal Court (ICC), no accountable executive nor legislative review body exists. The absence of an external separation of powers and, as such, this missing accountability and review mechanism, undermines two elements essential to regulating democratic regimes. When a public authority or a private firm which is not traditionally governed by the controls relevant to foreign intelligence agencies owns personal information, international instruments govern how this information is handled.[15]

---

[12] C Forcese & N LaViolette. 'Ottawa Principles on Anti-terrorism and Human Rights.' *The Human Rights of Anti-terrorism: A Colloquium* (2007, Human Rights Research and Education Centre, Ottawa).
[13] M Caparini. 'Controlling and Overseeing Intelligence Services in Democratic States.' In H Born & M Caparini (eds) *Democratic Control of Intelligence Services: Containing Rogue Elephants* (2007, Ashgate Publishing, Hampshire) 7, 10.
[14] Caparini (note 13) 10.
[15] Wright (note 10) 365.

IV THE CHALLENGES TO EFFECTIVE OVERSIGHT OF FOREIGN INTELLIGENCE AGENCIES

It has been debated whether the protection of state security should trump any objectives and values by which society attempts to constrain this power. An argument has been that it is the unique requirements and characteristics of foreign intelligence agencies that make effective oversight considerably challenging.[16] This challenge becomes apparent when analysing the relationship between intelligence and policy, on the one hand, and accountability mechanisms, on the other. Whereas parliamentary oversight can cause problems such as an ongoing operation or source being compromised by information disclosed by a member or committee, parliamentarians' insufficient security vetting and the politicisation of foreign intelligence agencies, independent judicial oversight brings with it the problems of sensitive information being shared outside of foreign intelligence circles.[17]

Civil wars and their spillover, terrorist attacks and asymmetrical threats have characterised the post-Cold War era and necessitated what Rumsfeld called 'exquisite intelligence'.[18] An asymmetrical threat is a threat disproportionate to the power of the state being threatened. Since September 2001, the multilateral counter-terrorism co-operation of foreign intelligence has put operational transparency at risk and, in so doing, has further challenged the effective oversight of foreign intelligence liaison. Moreover, foreign intelligence services' breaches of international law and human rights abuses overseas may trigger retaliation and risk the international standing of a state. Ultimately, the relations with states in which operations are being conducted or targeted by foreign intelligence agencies can be strained by the public disclosure of clandestine or covert operational information.[19]

A suggested resolution to the challenge of effective oversight has been that fundamental political values be treated as a more important formal power and constraint over foreign intelligence services than international law. Specifically,

---

[16] Caparini (note 13) 4.
[17] Caparini (note 13) 13.
[18] H Born. 'Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices.' (2004) 3(4) *Connections: The Quarterly Journal* 2.
[19] H Born & I Leigh. 'Democratic Accountability of Intelligence Services.' (2007, Geneva Centre for the Democratic Control of Armed Forces (DCAF) Policy Paper No 19) 5.

> '(r)ather than legislation, it is the internalisation of these political values and ideas within the political culture, especially among the political elite, that provides the most essential indicator of democratic governance of the (internal) security sphere.'[20]

It should be noted that this is not another way of saying that oversight is not necessary because the Executive will behave itself anyway. The internalisation of political values may therefore offer inroads towards international regulation of security intelligence agencies in liberal democracies, but less so towards international regulation of foreign intelligence agencies in those same liberal democracies.

V FOREIGN INTELLIGENCE LIAISON

The evolving nature of cross-border threats such as terrorist networks has necessitated that foreign intelligence agencies respond with cross-border co-operation. The international co-operation of foreign intelligence agencies, or foreign intelligence liaison, has taken on the form of 'pooling resources, trading information, drawing up common threat assessments and even circumvent(ing) domestic law'.[21] In particular, the problems associated with trading information and circumventing domestic law have highlighted the need for more effective oversight of national executives.

An initial problem with trading information is that foreign intelligence agencies can be less compliant with the international law governing the pursuit of critical information – for instance, using torture to seek information – than other foreign intelligence agency partners.[22] Additional concerns surrounding the circumvention of legal safeguards, controls and domestic law by foreign intelligence agency co-operation arise through the transfer of the personal data of nationals.[23] Not only may the reckless use of the shared intelligence damage the sharer's foreign intelligence operations but it may also support policies contrary to the moral compass, aims and interests of the sharer.

Therefore, it has been agreed that the international co-operation of foreign intelligence agencies has to be founded on the ministerial approval of minimum safeguards through formal agreements and international legal obligations and

---

[20] Born & Leigh (note 19) 17.
[21] Born (note 18) 7.
[22] UNGA Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 1984.
[23] Born (note 18) 8.

frameworks.[24] The 9/11 Commission in the United States[25] and the Hutton Inquiry[26] and the Butler Commission[27] in the United Kingdom are examples of potential legal foundations that could be used by the Executive to regulate the international co-operation of foreign intelligence agencies effectively.[28] Specifically, these inquiries have handled vital questions as to whether:

- terrorists' threats render increased legal resources and powers necessary for foreign intelligence agencies;
- foreign intelligence is politicised by political leaders, and
- the rule of law effectively governs the work of foreign intelligence officials.[29]

(*a*) The globalisation of foreign intelligence liaison

An argument has been posited that the fluid expansion of terrorist networks and cells is not merely a symptom of globalisation but that the origin of this instability and disruption is globalisation itself.[30] While the fundamental connection between globalisation and terrorism was overshadowed by the events of September 2001, the challenges facing international regulation of foreign intelligence agencies has deepened as accountability mechanisms have not been able to keep up with the global expansion of foreign intelligence operations. The emergence of foreign intelligence liaison, particularly with regard to activities such as rendition, has seen extreme liaison secrecy, a dependence on foreign intelligence partnerships, the diffusion of foreign intelligence co-operation, multilateral co-operation in field operations and training, national infrastructural corporate providers and private security firms challenge the ability of international law to effectively monitor and oversee foreign intelligence agencies.[31]

---

[24] Born (note 18) 8.
[25] 9/11 Commission. *The 9/11 Commission Report* 2004 1–567.
[26] B Hutton. *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly CMG*. (2004, The Stationery Office, London) 1–328.
[27] R Butler. 'Review of Intelligence on Weapons of Mass Destruction.' *Report of a Committee of Privy Counsellors* (2004, The Stationery Office, London) 1–196.
[28] Born (note 18) 3.
[29] Born (note 18) 1.
[30] RJ Aldrich. 'Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem.' (2009) 24(1) *Intelligence and National Security* 8.
[31] Aldrich (note 30) 1–3, 9–10.

This international regulatory challenge posed by the globalisation of liaison has forced the development of accountability mechanisms at a national, regional and international level. Nationally, bi-annual International Intelligence Review Agencies Conferences' and bilateral 'accountability tourism' have succeeded in establishing national best-practice standards but have not addressed the liaison itself.[32] However, since September 2001, liaison has been approached nationally through standing committees such as that for the 'Yellow Cake' saga,[33] special commissions of inquiry and judicial co-operation concerning Abu Omar's rendition.[34] The 'Yellow Cake' saga involved a standing committee that tampered with evidence about the existence of weapons of mass destruction in Niger and Iraq. While liaison may arguably be politically more effectively approached by a free media and press as opposed to standing committees or special commissions of inquiry, judicial co-operation over liaison is a form of legal accountability mechanism that is a more effective national accountability mechanism than political accountability equivalents.[35]

Similarly, regional inquiries have functioned as a more effective tool for oversight over rendition than national mechanisms. This increased focus on a regional accountability mechanism has received notable attention in Europe through two connected inquiries carried out by the European Parliament and the Council of Europe. By pressurising national governments through published reports, reviewing Human Rights Law with the Venice Commission and researching European renditions, these institutions have been able to focus on the legal as opposed to the political structures governing foreign intelligence agencies.[36] Inquiries by former Secretary-General, Terry Davis,[37] and rapporteur Dick Marty[38] via the Parliamentary

---

[32] Aldrich (note 30) 11–12.
[33] J Wilson. 'What I Didn't Find in Africa' *The New York Times* 2003, available at http://www.nytimes.com/2003/07/06/opinion/what-i-didn-t-find-in-africa.html?src=pm&pagewanted=1 (accessed on 25 November 2014); CW Ford 'Niger/Iraq Uranium Story and Joe Wilson (S/NF)' *Unclassified Memorandum* (2003) 1–3; National Intelligence Council 'Iraq's Weapons of Mass Destruction Programs' *NIC Draft Report* (2002) 1–24; Director of Central Intelligence 'Iraq's Weapons of Mass Destruction Programs' CIA White Paper (2002) 1–25; British Government 'British Government Briefing Papers on Iraq' Declassified Draft of British Government's White Paper (2002) 1–44; British Government 'Iraq's Weapons of Mass Destruction: The Assessment of the British Government' Final Version of British Government's White Paper (2002) 1–51.
[34] Aldrich (note 30) 12; *General Prosecutor at the Court of Appeals of Milan v Adler and Ors* 46340/2012 ILDC 1960 (IT 2012).
[35] *Adler and Ors* (note 34).
[36] Aldrich (note 30) 20.
[37] T Davis. 'Secretary-General's Report under Article 52 ECHR on the Question of Secret Detention and Transport of Detainees Suspected of Terrorist Acts, notably by or at the Instigation of Foreign

Assembly of the Council of Europe (PACE) addressed liaison by drafting conventions. This was achieved through legal standards set in international treaties by member states such as the European Convention on Human Rights (ECHR),[39] the European Convention for the Prevention of Torture[40] and its first judgment on rendition in the *El Masri* case.[41] This sparked an inquiry by the European Parliament to develop a Temporary Committee on the alleged use of European countries by the Central Intelligence Agency (CIA) for the transport and illegal detention of prisoners (TDIP). Indeed, the inquiry's rapporteur, Giovanni Claudio Fava,[42] expressly addressed the matters of rendition and liaison between foreign intelligence agencies in Europe.

Foreign intelligence co-operation has also been approached at the international level, particularly by the United Nations. The Office of Investigation of the International Criminal Tribunal for the Former Yugoslavia (ICTY) and the United Nations monitoring mission in Iraq in the 1990s set the precedent for the UN's international intelligence inquiry into the assassination of the Prime Minster of Lebanon, Rafik Hariri, in 2005.[43] This resulted in UN Security Council Resolution 1595's[44] creation of the UN International Independent Inquiry Commission (UNIIIC).[45] This international inquiry signifies the UN's evolving perception of the pertinence of intelligence and of reviewing foreign intelligence activity, the potential

---

Agencies' *Council of Europe Information Documents* SG/Inf (2006) 5 1–50; T Davis 'Secretary-General's Supplementary Report under Article 52 ECHR on the Question of Secret Detention and Transport of Detainees Suspected of Terrorist Acts, notably by or at the Instigation of Foreign Agencies'' *Council of Europe Information Documents* SG/Inf (2006)13 1–35.

[38] D Marty 'Alleged Secret Detentions and Unlawful Inter-state Transfers of Detainees involving Council of Europe Member States' *Committee on Legal Affairs and Human Rights Report* (2006) Doc. 10957 1–76; D Marty 'Alleged Secret Detentions and Unlawful Inter-state Transfers of Detainees involving Council of Europe Member States' *Committee on Legal Affairs and Human Rights Explanatory Memorandum* (2007) AS/Jur 2007 36 1–72; D Marty 'Abuse of State Secrecy and National Security: Obstacles to Parliamentary and Judicial Scrutiny of Human Rights Violations' *Committee on Legal Affairs and Human Rights Report* (2011) Doc. 12714 1–23.

[39] ECtHR 'European Convention on Human Rights' *Council of Europe* (2002) 3–55.

[40] Aldrich (note 30) 21; ECtHR 'European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment' *Council of Europe* (2002) 3–33.

[41] *El-Masri v the Former Yugoslav Republic of Macedonia* 39630/09.

[42] GC Fava 'Report on the Alleged Use of European Countries by the CIA for the Transportation and Illegal Detention of Prisoners (2006/2200(INI))' *Temporary Committee on the Alleged Use of European Countries by the CIA for the Transportation and Illegal Detention of Prisoners Final Session Document* (2007) A6-0020/2007 1–77.

[43] Aldrich (note 30) 25–27.

[44] UNSC 'Res 1595' *Security Council Resolutions* (2005) S/RES/1595 1–3.

[45] Aldrich (note 30) 28; M Detlev 'Report of the International Independent Commission Established pursuant to Security Council Resolution 1595' *United Nations International Independent Commission (UNIIIC) Reports* (2005) UNIIIC 7–61.

use of foreign intelligence agencies' neutrality and recognition of the role of foreign intelligence agencies in good governance.[46]

The effectiveness of national committees appears limited to national contexts; free press, think tank, lobby group and non-governmental organisation (NGO) accountability is constrained by the absence of a democratic mandate and a lack of concern for such groupings' effectiveness. This national level of activity appears to be where international legal best practice is likely to emerge and possibly regulate foreign intelligence liaison over time. In this regard, Inspector-Generals with enhanced operational authority in many countries are a recommended international legal alternative worth exploring with a regional bloc such as the North Atlantic Treaty Oganisation (NATO) or Brazil-Russia-India-China-South Africa (BRICS) or foreign intelligence partners such as the United States and the United Kingdom.[47] This even though their remit might be limited to holding internal inquiries and drafting investigative guidelines.

(*b*) Intra-alliance foreign intelligence liaison

Sun Zhu taught us that 'it is as important to know yourself – and by extension your allies – as it is to know your enemies'.[48] This lesson would suggest that foreign intelligence agencies' collection, processing, analysis and dissemination of foreign intelligence about their own , their allies' and their enemies' foreign intelligence agencies is of paramount importance.[49]

A strongly established and mutually trusting foreign intelligence liaison relationship is usually too valuable to risk breaching as a result of illegal or invasive activity in a host or allied state. Yet, the chapter on liaison was the sole chapter to be completely deleted from an official, recently declassified, internal history of the CIA in the 1950s.[50] Therefore, it has been suggested that there is a close relationship between foreign intelligence agencies' liaison partnerships and their secret intelligence activities. The challenge therefore to internationally regulating foreign

[46] Detlev (note 45) 29.
[47] Detlev (note 45) 31–3.
[48] MS Alexander 'Introduction: Knowing your Friends, assessing your Allies – Perspectives on Intra-alliance Intelligence' *Intelligence and National Security* (2008) 7.
[49] Alexander (note 48) 5.
[50] LL Montague *General Walter Bedell Smith as Director of Central Intelligence, October 1950-February 1953* (1992).

intelligence agencies would appear to be most apparent within foreign intelligence liaison, particularly with respect to rendition.

(*c*) The utility of foreign intelligence liaison

A Former Director-General of the UK's Security Service (MI5), Sir Stephen Lander, has described the new phenomenon of 'intelligence diplomacy' as 'the recognition by governments that there are relationships and understanding in their intelligence communities which can be used diplomatically'.[51] The value that intelligence diplomacy has added to diplomatic relationships has rendered international intelligence collaboration all the more essential. It has therefore been argued that the essential determinant of international intelligence collaboration is the utility that sustains collaboration.[52]

The distinct aspects behind international intelligence co-operation are the dissemination of intelligence-based assessments, the collaboration on operations and – most importantly – quality reporting disseminated from a single source whose primary information has been assessed. The reasons for the stamina behind international intelligence co-operation include the broader political relationships behind the intelligence relationship, long-term institutional partnerships and competent foreign intelligence allies. The routine use of intelligence as a collective asset in government, the operational history of institutional relationships and the mutual perception of the necessity of international intelligence co-operation also sustains foreign intelligence liaison.[53]

However, barring certain specified organisations, domestic legislation does not often allow for the dissemination of the products of intelligence gathering beyond national borders.[54] Therefore, Lander has argued that his utility test would be satisfied because 'the risks and costs of sharing (one's) own national material would be more than outweighed by the benefits of access to others'.[55] Accordingly, a cost–benefit analysis of the utility behind international intelligence co-operation appears

[51] S Lander. 'International Intelligence Co-operation: An Inside Perspective.' (2004) 17(3) *Cambridge Review of International Affairs* 482.
[52] Lander (note 51) 484.
[53] Lander (note 51) 486–488, 492.
[54] Ibid.
[55] Lander (note 51) 493.

to offer a rationale as to why these international legal restrictions may be overlooked in practice.

(*d*) Forms of foreign intelligence liaison

Foreign intelligence agencies act mainly in support of their self-interest and their state's foreign policy.[56] When the costs, risks and benefits are understood as being inevitable, liaison ensues. These benefits include influencing the policies or conflict trajectory of other states, establishing diplomatic ties, lowering the costs of operations and sealing visible gaps. However, liaison may be restrained by:

- the consequences of judicial practices;
- legal issues;
- dificulties with communication systems;
- multi-levelled vetting;
- a liaison ally's poor history of human rights;
- an unequal distribution of power, and
- differences in foreign policy objectives and perceptions of threat.[57]

Multilateral liaison is based on intelligence product sharing, targeting and coverage, the division of labour, sharing intelligence asset access and technology and burden sharing. Though the scope of multilateral liaison may be dependent on shared interests and common threat perceptions, differences in the culture , geography, experience and values such as trust and respect of the foreign intelligence agencies can render this reliance insufficient for establishing foreign intelligence liaison. In principle, information has a larger probability of being disclosed without authority the more broadly that information is shared. Moreover, the more parties that are involved, the more the comparative advantage of this information has resulted in rising costs and decreasing benefits, often because of unknown beneficiaries. Multilateral liaison rarely occurs in full confidence, therefore, because the methods of foreign intelligence gathering and the sources of intelligence cannot be guaranteed

[56] S Lefebvre. 'The Difficulties and Dilemmas of International Intelligence Co-operation.' (2011) 16(4) *International Journal of Intelligence and Counterintelligence* 534.
[57] Lefebvre (note 56).

complete protection: there are counterterrorism concerns, intelligence can be compromised, the fear of being penetrated is ever present.[58]

Plurilateral liaison sees foreign intelligence exchanged at a more informal level through loosely structured informal clubs, groups and networks. With particular attention to shared problems and specific threats, information is shared among these groups less systematically and with more discretion.[59] This form of liaison is generally based on governments' sovereign discretion to share information. Although these plurilateral structures mutually enhance counterterrorism efforts through non-reciprocal intelligence sharing, they are vulnerable to statutory obligations, policy prescriptions and laws.[60]

Bilateral liaison is bound by the third-party rule which states that 'intelligence supplied by a party to another cannot be shared with a third one without the originator's consent'.[61] Therefore, foreign intelligence co-operation occurs preferably via bilateral liaison. This form of liaison commonly includes joint operations and shared training facilities, raw product, assessments, synchronised intelligence systems, standardised vetting procedures, classification criteria and frequent meetings. While bilateral liaison can be set up either informally or formally, its focus on protecting foreign intelligence agencies' intelligence and the equality of exchanges has seen formal bilateral liaison being accepted as the preferred form of foreign intelligence liaison.[62]

(*e*) Managing bilateral intelligence liaison

Managing bilateral liaison is difficult because diverse intelligence agencies have different directorates in their foreign relationships, varied exchange deals and means of disseminating intelligence with their foreign counterparts and different intelligence specialisations that may not be consistent with the organisational structures of foreign intelligence agencies. The bilateral relationships that should be

[58] Lefebvre (note 56) 529, 532.
[59] M Rudner. 'Hunters and Gatherers: The Intelligence Coalition against Islamic Terrorism.' (2004) 17(2) *International Journal of Intelligence and Counterintelligence* 195.
[60] Rudner (note 59) 208–209, 211.
[61] Lefebvre (note 56).
[62] Lefebvre (note 56) 532–533.

pursued are therefore those that are easier and safer to manage on the basis of clearly specified shared objectives.[63]

Bilateral liaison can take the form of traditional alliances or new alliances between traditional adversaries. The war on terror, for instances, has seen liaison between traditional alliances expand. New alliances or renewed relationships liaison have centred mainly around Islamic terrorism and increased intelligence sharing in the greater Middle East, whereas non-traditional allies have included state sponsors of terrorism and non-traditional partners. However, the operational success of non-traditional allies in combating terrorism has been undermined by political disputes with other governments.[64]

In the context of the war on terror, multilateral liaison is actually a global network of bilateral liaison. In the long term, policy-makers will be challenged to defend their countries against threats of counterintelligence, while building useful alliances out of short-term tactical liaison. As liaison occurs not equally but asymmetrically, international law and norms should see to it that foreign policy decision-making is not manipulated or tailored by the abuse or misuse of foreign intelligence. Bilateral liaison should produce foreign intelligence that is not only trusted but also verifiable.[65]

(*f*) Foreign intelligence liaison via rendition

Legal systems and foreign and domestic policies frame the operations of liaison relationships. Not even allies will comply with requests that implicitly breach the domestic legitimacy of target activities or groups, privacy laws or statutory principles. However, the threat of terrorism can be used by foreign intelligence agencies as a reason for their not following the principle that foreign intelligence agencies do not perform operations in each others' territory.[66]

These counterterrorism measures have seen renditions occur where terrorists are transferred from the jurisdiction where they were detained to third countries in which brutal interrogations and detentions occur without due legal process. The

[63] DS Reveron. 'Old Allies, New Friends: Intelligence-sharing in the War on Terror.' (2006) 3 *Orbis 50* 458–459.
[64] Reveron (note 63) 460, 462, 465.
[65] Reveron (note 63) 467–468.
[66] Rudner (note 59) 215.

intelligence accrued from these extraordinary renditions has been traded for sensitive information, third-state intelligence and other exchanges with non-state actors. Therefore, liaison against counterterrorism between foreign intelligence agencies is often inconsistent with foreign policy and state liaison.[67]

(*g*) The costs and benefits of foreign intelligence liaison

A former US Deputy Assistant Secretary of State for Intelligence Co-ordination and the US State Department's first Co-ordinator for Intelligence Resources and Planning, Dr Jennifer E Sims, has described foreign intelligence liaison as a 'form of subcontracted intelligence collection based on barter'.[68] Foreign intelligence liaison can be characterised as a simple, complex, symmetrical, asymmetrical or adversarial relationship. Each form of foreign intelligence liaison brings with it different costs and benefits.[69]

The bartering of intelligence gathering between parties is known as simple intelligence liaison. Complex intelligence liaison sees a blend of operational, military, economic or political intelligence-gathering assets bartered through foreign intelligence platforms. Symmetrical liaison arises when the trade via intelligence platforms is equitable to both parties. However, when one party receives more utility from liaison than the other, the result is asymmetrical liaison. Adversarial liaison entails co-operation between foreign intelligence agencies that is asymmetrically forced, joint gathering on behalf of adversarial foreign policy representatives or allied deception.[70]

Foreign intelligence liaison can be calculated through the costs associated with loss if co-operation does not meet possible alternatives and direct gain, be it military, political or intelligence.[71] The requisite counterintelligence to maintain the benefits of decisions made under competitive circumstances, even within alliances, is an example of co-operation costs.[72] Even intelligence about one's allies can be as

---

[67] Rudner (note 59) 220.
[68] JE Sims. 'Foreign Intelligence Liaison: Devils, Deals, and Details.' (2006) 19(2) *International Journal of Intelligence and Counterintelligence* 196.
[69] Ibid.
[70] Sims (note 68) 196–197, 200.
[71] Sims (note 68) 198.
[72] Sims (note 68) 199.

much of a cost to liaison as a cost of liaison that does not outweigh other military, political or intelligence gains.

Targeting, communication and a covert presence can have benefits if the ethno-geographical or ethno-historical relationships of foreign intelligence liaisons are used. Counterintelligence that is effectively used by a smaller power can result in its asymmetrical benefit over a bigger power within that foreign intelligence relationship. Also, the foreign policy decisions of other parties can be influenced through foreign intelligence liaison and, in so doing, provide an agency with further benefit.[73]

A state's foreign intelligence liaison that is unable to withstand threats from others increases costs. Costs rise as a result of actionable intelligence through dangerous relationships and unverified information. The counterintelligence operations of other parties in foreign intelligence liaison increase costs. Classified source-based prosecutions of terrorists put the protection of the information at risk and, in turn, increase costs.[74]

These costs and benefits have resulted in the international oversight of foreign intelligence liaison being endangered when:

- the policies of governments develop with contradictory objectives;
- foreign intelligence directorates' liaison loses the benefits of intelligence gathering through too much caution, and
- covert activities are undertaken without authority.

Accountability for foreign intelligence liaison through bilateral co-ordination between ambassadors and foreign intelligence chiefs has been suggested as an additional accountability measure by which to regulate foreign intelligence liaison internationally. In addition, the Executive and Legislative branches of state governments should ensure that foreign intelligence liaison is neither politicised nor driving foreign policy.[75]

---

[73] Sims (note 68) 203–204, 206.
[74] Sims (note 68) 203–205.
[75] Sims (note 68) 207, 211.

(*h*) Overcoming mistrust through foreign intelligence liaison

States can engage in mutually fruitful liaison and overcome mistrust through pacts – international legal agreements – and institutions. This is because as the costs of breaching a pact increase, the provisions that enable states to track one another's compliance with a pact garner further trust through institutions. Therefore, foreign intelligence dissemination would not only see better analysed and more openly dispersed intelligence between parties through institutions but also allow each party to track the way the beneficiary disseminates and uses the intelligence.[76]

Foreign intelligence liaison could see more effective reform of foreign intelligence sharing through tracking and overseeing the foreign intelligence analysis and gathering of states through enlarged independent powers. Alternatively, liaison could be achieved through smaller groups' encouraging safer foreign intelligence sharing between states. In the case of the enlarged independent powers, foreign intelligence sharing could be centralised and bolstered through making the sharing of credible foreign intelligence a prerequisite. Institutions could be empowered to monitor states' compliance with this prerequisite through a separate analysis and gathering agency, for instance. In addition, an agency could be developed with the resources and staff to oversee and track foreign intelligence liaison between states' respective agencies. In the case of smaller groups, realistically accepting that complete sharing will not evolve between mistrusting member states, a more cogent database network of foreign intelligence could be developed and groups of states' policy-makers could be encouraged to hold more frequent meetings.[77] These are policy suggestions for more effective liaison around intelligence.

The enlarged independent powers could decrease the efficiency of effective foreign intelligence sharing through technical hurdles and excessive management; the sharing of foreign intelligence between different groups of states could create third-party misunderstandings about where the foreign intelligence is being sent. While decentralised foreign intelligence liaison may realise fewer overall gains in foreign intelligence sharing than an institutionally centralised alternative, the

[76] JI Walsh. 'Intelligence-sharing in the European Union: Institutions are not Enough.' (2006) 44(3) *Journal of Common Market Studies* 630.
[77] Walsh (note 76) 626, 639–640.

decentralised option would probably be a more realistic and humble development in foreign intelligence sharing.[78]

It has also been argued that foreign intelligence liaison via best-practice methods will develop trust between foreign intelligence agencies over time. In this context, foreign intelligence liaison may become more standardised and homogenised. Whereas this increased participation of foreign intelligence agencies may see benefits in the realm of policy, it should be noted that the implications for foreign intelligence liaison would necessitate significant methodological developments such as scenarios methodology.[79]

V CONCLUSION

A state-centric as opposed to a private-sector definition of foreign intelligence has been suggested; the foreign intelligence process, organisation and product were differentiated, and it was argued that foreign intelligence requires clear mandates, central co-ordination, independent judicial oversight and independent parliamentary oversight and accountability. The suggested objectives of a regime for international law in liberal democracies were to create a democratic oversight, control and review regime of the propriety, effectiveness, transparency and government accountability over foreign intelligence liaison. Examples of the challenges to effective oversight of foreign intelligence liaison were apparent in executives, legislatures, judiciaries, foreign intelligence agencies and international instruments, while a three-pronged accountability mechanism was suggested.

The evolving nature of international intelligence co-operation, the forms it takes and some of the problems associated with it require the international co-operation of foreign intelligence among agencies to be founded on the ministerial approval of minimum safeguards through formal agreements, international legal obligations and frameworks. The need for the international regulation of foreign intelligence liaison has increased as accountability mechanisms have not been able to keep up with the global expansion of foreign intelligence operations. For this reason, national, regional and international accountability mechanisms were compared. It

---

[78] Walsh (note 76) 640–641.
[79] A Svendsen. 'The Globalisation of Intelligence since 9/11: Frameworks and Operational Parameters.' (2008) 21(1) *Cambridge Review of International Affairs* 136, 139.

was suggested that a close relationship exists between intra-alliance foreign intelligence agencies' liaison partnerships and secret intelligence activities.

A cost–benefit analysis of the utility behind international intelligence co-operation appeared to offer a rationale as to why international legal restrictions may be overlooked in practice. This can occur when the law is interpreted as a cost by foreign intelligence agencies. Multilateral, plurilateral and bilateral forms of foreign intelligence liaison were then contrasted, with most states appearing to prefer more formal bilateral relationships. Bilateral intelligence liaison was categorised into traditional alliances, new alliances and traditional adversaries. And while those that should be pursued are those that are easier and safer to manage around clearly specified objectives, international law and norms should oversee that foreign policy decision-making is not manipulated or tailored by the abuse or misuse of foreign intelligence. Foreign intelligence liaison via rendition evidenced foreign intelligence agencies' counterterrorism liaison as often being inconsistent with foreign policy and government liaison when terrorists are transferred from the jurisdiction where they were detained to third countries where brutal interrogations and detentions occur without due legal process.

A cost–benefit assessment of simple, complex, symmetrical, asymmetrical and adversarial foreign intelligence liaison aimed at effectiveness indicated that the accountability of foreign intelligence liaison through bilateral co-ordination between ambassadors and foreign intelligence chiefs should enhance accountability measures. It also indicated that the executive and legislative branches of states should ensure that foreign intelligence liaison is neither being politicised nor driving foreign policy. An analysis of the advantages and disadvantages of centralised or decentralised foreign intelligence sharing reform suggested that decentralised foreign intelligence liaison would probably be a more realistic and humble development in foreign intelligence sharing but that significant methodological developments would be necessary in order to enhance trust via best practice.

CHAPTER II: INTERNATIONAL REGULATION OF FOREIGN INTELLIGENCE LIAISON: A LEGAL ANALYSIS

I INTRODUCTION

Chapter I argued that the globalisation of foreign intelligence liaison has resulted in the deepening of the challenges that confront the international regulation of foreign intelligence liaison. This is so because regulatory mechanisms have not been able to keep up with the global expansion of foreign intelligence operations. This emergence of foreign intelligence liaison, particularly with regard to SIGINT activities, has challenged the ability of international law effectively to regulate foreign intelligence agencies. While this challenge was set out in theory, the international regulatory challenge posed by the globalisation of liaison has also put pressure on national and regional regulation in practice.[80]

Since the Snowden revelations of 2013, foreign intelligence liaison has become increasingly regulated by the judiciary at both the national and regional levels. State practice is summarised and analysed through a criticism of a recent landmark judgment in the United Kingdom – *Liberty (The National Council of Civil Liberties) and Others v The Secretary of State for Foreign and Commonwealth Affairs and Others* (*Liberty III*).[81] There it is argued that independent judicial oversight and supervision of foreign SIGINT liaison, particularly with regard to judicial pre-authorisation of communications interception warrants, shows that legal regulatory mechanisms are less subject to abuse or misuse than political controls.

However, regional legal regulatory mechanisms are less effective tools for regulating SIGINT liaison than national legal regulatory mechanisms because, even though the threats to national security have become transnational, the solutions to such threats still generally lie within national jurisdictions. This is concluded through a prediction of the outcome of the current *Liberty* appeal (*Liberty IV*) to the European Court of Human Rights' challenging the UK Investigatory Power Tribunal's (IPT)

---

[80] Aldrich (note 30) 1–3, 9–12.
[81] *Liberty (The National Council of Civil Liberties) and Others v The Secretary of State for Foreign and Commonwealth Affairs and Others* IPT/13/77/H.

December 2014 ruling (*Liberty II*).[82] The *Liberty II* case will function as a forecast that international regulation of foreign SIGINT liaison is more likely to take place at the national level in the short term.

In the *Liberty II* case, which is criticised here, the IPT did not find the lack of judicial pre-authorisation for communications interception warrants to be problematic in the *Liberty I* case; in the *Kennedy* case, the Court was satisfied with the role of the Commissioner, and this reasoning was developed further in the *Telegraaf Media* case.[83] My criticism of the *Liberty II* judgment centres on this position.

I strongly disagree with the view that a lack of judicial pre-authorisation for communications interception warrants is not problematic. Communications interception is a form of SIGINT, just as SIGINT is a form of foreign intelligence liaison. It therefore follows that if foreign intelligence liaison should be subject to judicial regulation, so should communications interception warrants. Accordingly, I argue that judicial pre-authorisation for communications interception warrants should be obligatory.

II NATIONAL REGULATION OF FOREIGN SIGINT LIAISON: *LIBERTY II* AND *LIBERTY III*

(*a*) Facts

In the *Liberty II* judgment, Liberty, Privacy International, American Civil Liberties Union, Amnesty International, Bytes for All and others (the claimants) alleged that the actions assumed to be attributable to the Secretary of State for the Foreign and Commonwealth Office (Foreign Secretary), the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ) [intelligence services] were unlawful because they violated the European Convention of Human Rights. As a result of Snowden's leaks, the claimants asserted that their privacy had been unlawfully infringed. The judgment only assumed these

---

[82] *Liberty (The National Council of Civil Liberties) and Others v The Government Communications Headquarters and Others* IPT/13/77/H.

[83] *Kennedy v United Kingdom* 2011 52 EHRR 4 at para 119; *Liberty v United Kingdom* 2009 48 EHRR 1 at para 57; *Telegraaf Media Nederland v the Netherlands* 2012 34 BHRC 193 para 98; *Liberty II* supra note 81 at paras 116–117.

'facts' because of the Neither Confirm Nor Deny (NCND) policy.[84] NCND is a legal principle that allows the respondents neither to confirm nor deny that a certain set of facts are true for reasons of national security.

With court oversight, the US government's 'Prism' system collects SIGINT. Prism might have obtained the claimants' private communications. Thereafter, the intelligence services might have received these private communications from the US government. The intelligence services might then have stored the claimants' private communications as requested.[85] The Prism disclosure was found to have been consented to by the respondents and could be declassified.[86]

The information that was assumedly given by the NSA to the respondents was assumed by the IPT to have been lawfully obtained. After all, the United States is the centre of global telecommunications and a significant amount of international correspondence crosses its borders.[87]

The Tribunal accepted that its specific function was to oversee complaints investigations and to co-ordinate its own rules in this regard.[88] It was agreed that communications interception can take place without anyone listening to, seeing or reading the correspondence because it can occur through communications gathering and recording alone.[89]

The Director of GCHQ, the Chief of MI6 and the Director-General of MI5 are some of the few people who can make an application for interception warrants. Only the Secretary of State, acting as MI5's Home Secretary and MI6 and GCHQ's Foreign Secretary, can grant interception warrants subject to extraordinary circumstances. The complaints in the judgment deal with what are known as 'untargeted, strategic or certificated warrants'.[90]

The Tribunal interpreted the Commissioner's Report on the warrants and whether the respondents abused their bulk collection capabilities. The Commissioner highlighted the breadth of his supervisory role. A notable quantity of information was released into the public space as was consistent with national security.[91]

---

[84] *Liberty II* (note 81) at paras 3–4.
[85] *Liberty II* (note 81) at para 14.
[86] *Liberty II* (note 81) at para 47.
[87] *Liberty II* (note 81) at para 15.
[88] *Liberty II* (note 81) at para 45.
[89] *Liberty II* (note 81) at para 62.
[90] *Liberty II* (note 81) at paras 64–65.
[91] *Liberty II* (note 81) at para 92.

(*b*) Issues

The claims were understood in two sections. The first issue dealt with the NSA's Prism and 'Upstream programme' liaison with the respondents and the second issue addressed the alleged 'Tempora interception operation'. The Tribunal interpreted Tempora as the 's 8(4)' issue.[92]

The Prism issue was understood as follows:

> '… does the statutory regime … satisfy the Art 8(2) "in accordance with the law" requirement?'[93]

The following four questions, according to the Tribunal, encapsulated the arguments on the s 8(4) issue:

> '(1) Is the difficulty of determining the difference between *external* and *internal* communications, whether as a theoretical or practical matter, such as to cause the s 8(4) regime not to be *in accordance with law* contrary to Article 8(2)? (See definition of art 8(2) in part II (*c*) below.)
>
> (2) Insofar as s 16 of RIPA [Regulation of Investigatory Powers Act] is required as a safeguard in order to render the interference with Article 8 *in accordance with law*, is it a sufficient one?
>
> (3) Is the regime, whether with or without s 16, sufficiently compliant with the Weber requirements, insofar as such is necessary in order to be *in accordance with law*? (See explanation in part II(*c*) below.)
>
> (4) Is s 16(2) indirectly discriminatory contrary to Article 14 of the Convention [prohibition of discrimination], and, if so, can it be justified?'[94]

(*c*) Laws

The Tribunal allowed for 'general challenges to the relevant legislative regime' because it found legal standing for the claimants through the *Kennedy v United Kingdom* decision.[95] This legal standing was allowed 'in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them'.[96] General challenges applied to the claimants

---

[92] *Liberty II* (note note 81) at para 5; Interception of Communications Code of Practice (note 100).
[93] *Liberty II* para 14.
[94] *Liberty II* para 80.
[95] *Liberty II* para 4; *Kennedy* (note 82) at para 119.
[96] Ibid.

because they were 'unable to demonstrate that the impugned measures had actually been applied to them' as followed in the *Liberty I* case.[97]

The Tribunal cleared up the matter of the ECHR protection by expressly citing art 8 of the ECHR:

> 'Right to Respect for Private and Family Life:
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[98]

Foreign intelligence communications liaison between the United Kingdom and the United States is governed by a recently declassified bilateral UK–US Communication Intelligence Agreement dating from 1946.[99] External communications were defined in s 8(4) Chap 5(1) of the Interception of Communications Code of Practice (Code) in line with s 71 of RIPA as:

> '… those which are both sent or received outside the British Islands … whether or not they pass through the British Islands in course of their transit. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route.'[100]

The Tribunal agreed with the claim made in the Commissioner's Report that:

> 'The section 8(4) structure does not permit random trawling of communications. This would be unlawful. It only permits a search for communications referable to individuals the examination of whose communications are certified as necessary for a statutory purpose.'[101]

The lack of judicial pre-authorisation for communications interception warrants was not found to be problematic in the *Liberty I* case, in the *Kennedy* case the Court was content with the position of the Interception of Communications

---

[97] *Liberty II* (note 81) at para 4; *Kennedy* (note 82) at para 57.
[98] *Liberty II* para 12; ECHR art 8.
[99] *Liberty II* para 15.
[100] *Liberty II* para 69; Interception of Communications Code of Practice.
[101] *Liberty II* para 71; Commissioner's Report para 6(5)(38).

Commissioner (the Commissioner) and this reasoning was further developed in the *Telegraaf Media* case.[102]

The IPT was satisfied that the s 8(4) programme was compliant with the *Weber* case prerequisites, they being the minimum statutory safeguards intended to avoid abuses of secret surveillance powers:

> '… (1) the nature of the offences that may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed.'[103]

This application of the *Weber* requirements found authority in the *Kennedy* case judgment from the ECtHR. The IPT held that the signposting in the reports of the Commissioner, the Code and the statute was adequate.[104]

(*d*) Applications

This part of my discussion now turns to the *Liberty III* judgment that was delivered on 6 February 2015, two months after the original *Liberty II* judgment was delivered on 5 December 2014. The facts, issues and laws pertaining to the *Liberty II* judgment, which are generally indistinguishable from the facts, issues and laws relating to the *Liberty III* judgment, have been summarised in part II (*a*), (*b*) and (*c*) above.

The two remaining issues arising out of the *Liberty II* judgment dealt with in the *Liberty III* judgment were:

> '(*i*) Whether by virtue of the fact that any of the matters now disclosed in the judgment of 5 December 2014 were not previously disclosed, there had prior thereto been a contravention of Articles 8 or 10 ECHR (The First Issue).
>
> (*ii*) Whether by virtue of the facts and matters set out in … the judgment of 5 December 2014, there is a contravention of Articles 8 or 10 ECHR (The Second Issue).'[105]

The Upstream and Prism program was applicable only to the first issue.[106]

---

[102] *Liberty II* (note 81) at para 116.
[103] *Liberty II* (note 81) at para 33
[104] Ibid; *Liberty II* (note 81) at para 140.
[105] *Liberty III* (note 82) at para 11.

The Tribunal agreed with counsel Ryder's submission that:

> 'It is only by reference to the Disclosures that [counsel was] satisfied that there was a sufficiently accessible indication to the public of the legal framework and any safeguards. In the absence of the Disclosures any such indications would have been insufficient and the intelligence sharing regime would not have been in "accordance with the law/prescribed by law".'[107]

The IPT conceded that there would not have been the sufficient signposting if the disclosures had not occurred. In this context, 'legal signposting' refers to legal information that is available to one via a legal expert. This required signposting was put in place through the *Liberty III* judgment.[108] With regard to the second issue, identical safeguards should be applied for in a s 8(4) warrant to be referenced in an exceptional s 1(*b*) request.[109]

(*e*) Conclusion

Consequently, the IPT's *Liberty III* order declared:

> '(*i*) that prior to the disclosures made and referred to in the First Judgment [*Liberty II*] and the Second Judgment [*Liberty III*], the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or (on the Claimants' case) Upstream, contravened Articles 8 or 10 ECHR but,
>
> (*ii*) that it now complies with the said Articles.'[110]

This was the first ruling in the 15-year history of the IPT's jurisprudence to find the activities of the intelligence agencies arbitrary and unlawful.

III NATIONAL REGULATION OF FOREIGN SIGINT LIAISON: CRITICISM OF *LIBERTY I*

(*a*) Criticism

---

[106] *Liberty III* (note 82) at para 12.
[107] *Liberty III* (note 82) at para 19.
[108] *Liberty III* (note 82) at para 21.
[109] *Liberty III* (note 82) at para 26.
[110] *Liberty (The National Council of Civil Liberties) and Others v The Secretary of State for Foreign and Commonwealth Affairs and Others* No IPT/13/77/H.

Judicial pre-authorisation for communications interception warrants should be obligatory. The IPT's argument for why a lack of judicial pre-authorisation for communications interception warrants is not a problem is insufficient. It cites only three cases as authority for this premise – the *Liberty I*, *Kennedy* and *Telegraaf Media* cases.

The first problem with this is that *Liberty I*, *Kennedy* and *Telegraaf Media* appeared before two different courts: *Liberty I* and *Kennedy* appeared before the ECHR and the *Telegraaf Media* case was heard before one of the highest courts in the Netherlands. Secondly, the three cases went about entirely different aspects of communications interceptions. The *Liberty I* case dealt with the interceptions of the applicants' communications. The lawfulness of the granting of communications interception warrants was interpreted in the *Kennedy* case. The *Telegraaf Media* case involved the arbitrary and unlawful abuse of special state surveillance powers of communications interception.

Moreover, the Court does not provide sufficient reasons as to why the lack of judicial pre-authorisation for communications interception warrants was not found to be problematic in the *Liberty v UK* case, why the Court was satisfied with the position of the Commissioner in the *Kennedy* case, and why this reasoning was developed in the *Telegraaf Media* case. This is not to say that the Court's interpretation of the *Liberty v UK*, *Kennedy* and *Telegraaf Media* cases is inaccurate or misleading. It may, however, be incomplete.

I intend to apply a deeper analysis of the Court's interpretation of the three cases in the hope of arriving at a more complete interpretation of the precedent. Below I reproduce the 15 lines out of the *Liberty I* case' s 161-paragraph judgment that the IPT applied to this issue:

> 'There is also in our judgment no basis for objection by virtue of the absence for judicial pre-authorisation of a warrant. The United Kingdom system is for the approval by the highest level of government, namely by the Secretary of State. The absence of such judicial authorisation in *Liberty* [*I*] was not a matter of criticism, and the court in *Kennedy* concluded … that, whereas "it has previously indicated that 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", it was satisfied, not only by virtue of the existence of the Commissioner (then, as now, a distinguished retired Judge), which it had examined at length … but also by virtue of the fact that "the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful

> interception". This approval of the absence of judicial pre-authorisation was further addressed by the Court in *Telegraaf Media*.'[111]

The fact that the UK system approves communications interception warrants through the Secretary of State does not mean that such a high level of government approval renders the interception immune to judicial oversight and accountability in a liberal democracy such as the United Kingdom.[112] Judicial accountability mechanisms, such as those provided by an independent judge of the high court and/or court of appeal, are less inclined to party political bias or the abuse or misuse of foreign intelligence liaison than political accountability mechanisms in the form of a Secretary of State. Furthermore, judicial pre-authorisation of communication interception warrants could overcome mistrust in foreign intelligence liaison through international judicial best-practice methods that have been inspired by the *Liberty I* and *Liberty II* judgments.

(i) Liberty I

The absence of judicial authorisation was not raised in the *Liberty I* case.[113] However, this case can be distinguished on the facts from the *Liberty II* and *Liberty III* judgments before us. By distinguishing the facts of *Liberty I* from the facts of the *Liberty II* and *Liberty III* cases, it will become evident that simply because an absence of judicial pre-authorisation of communication interception warrants was not a matter of criticism in the *Liberty I* case does not mean that we should not be deeply critical of its absence in *Liberty II* and as a general rule. Such judicial pre-authorisation could and should become an international judicial best practice.

On the facts of *Liberty I*, the applicants alleged that the Defence Ministry's Electronic Test Facility (ETF) intercepted thousands of public telephone, facsimile and email communications that were radio channeled between Telecom's radio stations in Dublin and London.[114] However, the facts of the *Liberty II* and *Liberty III* judgments showed that the United States is the centre of global telecommunications and a far more significant amount of international correspondence moves through its

---

[111] *Liberty II* (note 81) at para 116.
[112] Ibid.
[113] Ibid.
[114] *Liberty I* (note 83) at para 5.

borders.[115] According to Glen Greenwald, the journalist who leaked the Snowden revelations on which the facts of *Liberty II* and *Liberty III* are based, the bulk of private communications intercepted by the United States and the United Kingdom number well into the billions.[116] Therefore, in addition to the fact that the US–UK bulk interceptions capabilities are active on a global scale and not only between the United Kingdom and Ireland, we cannot begin to compare the facts of a case where 10 000 telephone channels were alleged to have been intercepted with the facts of a case where Greenwald exposed that 'PRISM allows the NSA to collect data directly from the servers of nine of the biggest internet companies' – gmail, facebook, hotmail, yahoo, google, apple, skype, aol and youtube.[117] This distinguishability may not apply to the legal principles but it does appear to apply to the facts. Therefore, the scale of bulk communications interceptions in the *Liberty v UK* case is factually distinguishable from those of the *Liberty I* and *Liberty II* judgments.

Moreover, the need for an independent judge of the high court and/or court of appeal as opposed to the existence of the Commissioner is evidenced by three criticisms of the Commissioner in the *Liberty v UK* case. First, on a point of relevant domestic law and practice, the Commissioner's safeguard does not routinely account for pre-judicial authorisation of a warrant in practice. That is, the role is merely one of restrospective supervision and oversight to ensure that warrants were granted in accordance with the statute and for checking procedural appropriateness. The potential abuse and misuse of foreign intelligence liaison highlighted in Chapter I is accordingly not prevented by the Commissioner's 'safeguard.'[118]

Secondly, also on a point of relevant domestic law and practice, the Commissioners have no capacity to review whether the interception of communications security arrangements ('arrangements') had been achieved on a case-by-case (individual) basis even though they are generally authorised to review the arrangements' adequacy – which entirely undermines the horizontal accountability solution suggested in Chapter I.[119] (Chapter I's horizontal

[115] *Liberty II* (note 81) at para 15.
[116] G Greenwald. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (2014, Hamish Hamilton, London) 108–119.
[117] Greenwald (note 116) 108.
[118] *Liberty I* (note 83) at para 32.
[119] *Liberty I* (note 83) at para 44.

accountability solution refers to the restraint of state institutions by other state institutions, public agencies and the three branches of government.)

Thirdly, with regard to the independence and powers of oversight and supervision of the Commissioners, because the Commissioner's reports were unable to open the arrangements to public scrutiny and knowledge, the Commissioners' conclusions on compliance with the arrangements did not enhance access to or the certainty of the programme.[120] Therefore, the *Liberty II* and *Liberty III* conclusion that the lack of judicial authorisation was not an issue that was criticised is problematic.

(ii) Kennedy

The potential for the abuse or misuse of foreign intelligence liaison necessitates that, particularly in a liberal democratic society, an independent judge of the high court and/or court of appeal play a role in controlling supervision and oversight. However, the precedent set by the *Kennedy* case below suggests that the advantages of the IPT as highlighted in part III (*b*)(*i*) renders the IPT preferable to the Commissioner in being entrusted with supervision and oversight of the authorisation for communication interception warrants in the United Kingdom. It is, nonetheless, important to note that the advantages of the IPT's supervisory and oversight role in the judicial authorisation for communications interception warrants, while investigatory, is retroactive. Moreover, as with the criticism of the role of the Commissioner identified in part III (*b*)(*i*), it does not function as a judicial pre-authorisation of communications interception warrants – the supervisory control of the IPT is subject to the whim of the Executive through the Secretary of State. The potential for unlawful and arbitrary abuse or misuse of foreign intelligence liaison is therefore is such that it can only be remedied but not prevented by the courts.

On the background facts surrounding the circumstances of the *Kennedy* case, an applicant who had been found guilty of manslaughter in 1994 was suspicious that his communications had been intercepted via mail, telephone and email in 1996 and alleged that interception warrants continued to be unlawfully granted by the security

[120] *Liberty I* (note 83) at para 67.

services to disadvantage his business and for intimidation purposes.[121] As with the comparison of the facts of the *Liberty I* case to *Liberty II* and *Liberty III* in part III (*b*)(*i*) above, we cannot fairly compare the circumstances of a case where one man with a criminal record alleges that the security services unlawfully and arbitrarily intercepted his communications to a case that involves the UK foreign intelligence liaison with the US centre of global communications and the almost immeasurable quantity of international correspondence that this liaison is responsible for. The circumstances surrounding the facts of the *Kennedy* case and those surrounding the facts of the *Liberty II* and *Liberty III* judgments can, therefore, not be compared for the same reasons that the factual circumstances of the *Liberty I* case could not be compared with the facts of the *Liberty II* and *Liberty III* judgments with regard to the scale of bulk communications interceptions.

With regard to the applicable legislation governing the relevant domestic law and practice of the Commissioner, it first appears worth noting that in terms of inspections, the Commissioner's 2005–2006 report highlighted that the warrant samples are chosen randomly in a biannual review. This is disconcerting because it is arbitrary.[122] Secondly, the Commissioner's 2001 report identified that, though practically highly improbable, it is possible in theory for procedures overseeing the authorisation of warrants to be circumvented. However, a theoretical possibility is not acceptable in the realm of national security and the right to private and family life because if something is theoretically possible, then it is by definition not impossible.[123] Thirdly, the Commissioner's 2005–2006 report similarly was of the opinion that codes, safeguards and legislation render it almost impossible for private communications to be intentionally intercepted unlawfully is sufficient. This oversight and supervision also does not avoid the theoretical possibility of an intentionally unlawful interception of private communications.[124] Fourthly, in 2004 the Commissioner claimed that the Secretary of State can deny a warrant application for reasons of necessity and proportionality but it should be the function of an independent Judiciary and not the Executive to determine what is and/or is not necessary and proportional in authorising warrants for the interception of private

[121] *Kennedy* (note 83) at paras 6–7.
[122] *Kennedy* (note 83) at paras 60, 166.
[123] *Kennedy* (note 83) at para 65.
[124] *Kennedy* (note 83) at para 70.

communications.[125] Fifthly, even the Commissioner felt that the 24 interception mistakes and contraventions accounted for in the 2007 report were excessive. [126] Excessive errors are a slippery slope towards arbitrary and unlawful abuses and misuses of foreign intelligence, as cautioned in Chapter I, as opposed to evidence that no intentional abuse of interception of private communications powers is occurring, as the *Kennedy* case concludes.[127]

This conclusion established that the supervision necessary to avoid an abuse of foreign intelligence liaison stems, in part, from the extensive role of the IPT's oversight of communications interceptions:

> 'The Court recalls that it has previously indicated that 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. In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom.'[128]

With regard to the *Kennedy* judgment's argument for the independence, oversight and supervisory implementation capacity of the Commissioner,[129] the IPT raises sound arguments in *Liberty II* and *Liberty III*. These arguments suggest a preference for the IPT's potential to pre-authorise communications interception warrants rather than the Commissioner.[130] First, the IPT is empowered to create continual inspections and investigations in accordance with its own rules and

---

[125] *Kennedy* (note 83) at para 71.
[126] *Kennedy* (note 83) at para 73.
[127] *Kennedy* (note 83) at para 168.
[128] *Kennedy* (note 83) at para 167.
[129] *Kennedy* (note 83) at paras 57–74, 166, 168.
[130] *Liberty II* (note 81) at paras 45–46.

procedures.[131] Secondly, the IPT's hearings benefit from arguments between parties.[132] Thirdly, the IPT can hold a hearing in public based on facts that are assumed.[133] Fourthly, arrangements can be analysed by the IPT in a closed hearing and it can access all information even if it is secret.[134] Fifthly, the IPT can decide whether matters that it hears in closed chambers can be openly disclosed and publicised.[135] The *Liberty II* and *Liberty III* judgments consequently concluded that the presence of the Commissioner was examined in depth and that and the jurisdiction of the IPT is extensive.[136] However, it is clear that the role of the Commissioner was not examined in length and the jurisdiction of the IPT is not satisfactorily extensive.

(iii) Telegraaf Media

On the facts, Telegraaf Media Nederland Landelijke Media BV (Telegraaf Media) and two journalists complained that the state secret service's (AIVD) special powers of transcription and interception of their telecommunications recordings involved surveillance that was too extensive, stored for too long and therefore arbitrary and unlawful.[137] However, Telegraaf Media did not allege that the governmental supervisory and monitoring procedures were insufficient.[138] Following a similar line of reasoning to my criticism of the *Liberty I* and *Kennedy* cases in part III (*b*)(i) and (ii) above, we must differentiate the facts of this case where a media company and two journalists complained about the unlawfulness and arbitrariness of the excessive and overextended storage of their intercepted communications by the AIVD from those in *Liberty II* and *Liberty III* (where four international NGOs complained about the arbitrary and unlawful interceptionof their and billions of other communications, which occurred out of the US core of the global telecommunications network). The factual circumstances of the *Telegraaf Media* case are comparable to those of the

[131] *Liberty II* (note 81) at para 45.
[132] *Liberty II* (note 81) at para 46.
[133] Ibid.
[134] Ibid.
[135] Ibid.
[136] *Liberty II* (note 81) at para 116.
[137] *Telegraaf Media* (note 83) at para 43.
[138] *Telegraaf Media* (note 83) at para 94.

Liberty II and *Liberty III* judgments because of the scale of the bulk communications interceptions.

The *Liberty I* and *Kennedy* precedents followed in this case reiterated that there is an eminent risk of arbitrariness when the secretive powers of the Executive are made use of because the rule of law is not in accord with such a potentially uncontrolled discretionary power.[139] However, in this case, the Court found that the authorisation of the government's special powers was not subjected to an independent review body empowered to prevent or end this authorisation before the communications were intercepted, and that, once the confidence of journalists' sources had been breached, it could not be restored.[140] This absence of judicial pre-authorisation for communications interception warrants had clearly been a point of concern in the *Liberty I*, *Kennedy* and *Telegraaf Media* cases, in which an arbitrary, uncontrolled abuse and misuse of executive discretionary power contrary to the rule of law was at issue. Thus, for *Liberty II* to have interpreted the *Telegraaf Media* case as having dealt with approving the absence of judicial pre-authorisation is an inaccurate analysis of the case. There is, therefore, even more motivation for Chapter I's recommendation of a horizontal accountability solution to be applied to the judicial pre-authorisation of communications interception warrants in foreign intelligence liaison.

The *Telegraaf Media* ruling compared the independent supervision of communications interceptions by the Dutch Commission in the *Klass v Germany* case against that of the IPT and the Commissioner in the *Kennedy v UK* case:

> 'However, in both cases [*Klass v Germany* and *Kennedy v UK*] the court was prepared to accept as adequate the independent supervision available. In *Klass v Germany*, this included a practice of seeking prior consent to surveillance measures of the Commission, an independent body chaired by a president who was qualified to hold judicial office and which moreover had the power to order the immediate termination of the measures in question. In *Kennedy v UK* the court was impressed by the interplay between the Investigatory Powers Tribunal, an independent body composed of persons who held or had held high judicial office and experienced lawyers which had the power, among other things, to quash interception orders, and the Interception of Communications Commissioner, likewise a functionary who held or had held high judicial office and who had access to all interception warrants and applications for interception warrants.'[141]

---

[139] *Telegraaf Media* (note 83) at para 90.
[140] *Telegraaf Media* (note 83) at paras 100–101.
[141] *Telegraaf Media* (note 83) at para 98.

The independent supervision purported to be adequate appears rather inadequate for the same reasons as found in my criticism of the *Liberty I* and *Kennedy* cases in part III(*b*)(*i*) and (*ii*) above. The Commission's prior agreement for surveillance in the *Klass* case and the interplay between the IPT and the Commissioner in the *Kennedy* case are simply incomparable. This is because judicial pre-authorisation for surveillance by a Commission is an example of the judicial pre-authorisation for communications interception warrants argued for in Chapter II, whereas the interplay between the IPT and the Commissioner is an example of the retroactive authorisation of communications interception warrants criticised in part III (*b*)(*i*) and (*ii*) above. Therefore, the acceptance of the lack of judicial pre-authorisation was in fact not further dealt with in the *Telegraaf Media* case as the *Liberty II* judgment claims.[142]

This comparison further reveals that independent judicial oversight, supervision and accountability of foreign intelligence liaison is unavoidably subject to abuse and misuse in a liberal democracy. Legal systems should frame the operations of and not retroactively react to foreign intelligence liaison relationships and international best practices. The precedent created by the *Liberty I*, *Kennedy* and *Telegraaf Media* judgments was criticised because these cases offered unconvincing reasons for why judicial pre-authorisation of communications interceptions warrants should not be obligatory. However, the precedent created by the *Liberty I* and *Liberty II* judgments and order with regard to the unlawfulness and arbitrariness of the foreign intelligence agencies' activities should be encouraged as a means of overcoming mistrust between foreign intelligence agencies over time.

IV CONCLUSION

I have argued that independent judicial oversight and supervision of foreign SIGINT liaison, particularly with regard to judicial pre-authorisation of communications interception warrants, are more effective national regulatory mechanisms than political regulatory mechanisms as they are less likely to be subject to abuse or misuse. This was borne out in the criticism of the *Liberty II* case, which also

[142] *Liberty II* (note 81) at para 116.

functioned as a forecast that international regulation of foreign SIGINT liaison is more likely to happen at the national level in the short term.

The argument that there must be judicial pre-authorisation of communications interception warrants should have been posited in the *Liberty II* judgment. This is because the actions of the intelligence services were unlawful as they violated arts 8 and 10 of the ECHR and as the IPT's role was shown to be the oversight of complaint investigations of, in this case, untargeted, strategic or certified warrants. The lack of judicial pre-authorisation of communications interception warrants was not found to be problematic in the *Liberty I* case. The *Kennedy* case saw the Court satisfied with the position of the Commissioner for similar reasons to those in the *Telegraaf Media* case. The IPT's ruling in the *Liberty II* case that the signposting in the reports of the Commissioner, the Code and the statute was adequate was shown to be highly problematic. This was shown by the applications in the *Liberty III* judgment, where the Tribunal conceded that there would not have been the sufficient signposting if the disclosures had not occurred. Moreover, the IPT declared that the communications interception regime contravened arts 8 and 10 of the ECHR.

My criticism of *Liberty II* showed that the court's interpretation, application and development of the relevant *Liberty I*, *Kennedy* and *Telegraaf Media* precedents was incomplete. Judicial accountability mechanisms were argued to be less subject to party political bias and the abuse, misuse and mistrust of foreign intelligence liaison than to political accountability mechanisms. The circumstances of the *Liberty*, *Kennedy* and *Telegraaf* precedents were all shown to be different on the facts and incomparable to those of *Liberty II* and *Liberty III*, mostly for reasons of the scale or quantity of bulk communications interceptions.

The *Liberty I* case taught us that the Commissioner can supervise and oversee only retrospectively, does not have the capacity to review communications interceptions security arrangements and that compliance with arrangements did not enhance programme access or certainty. We learnt more about the Commissioner from the *Kennedy* case in that, while the IPT's investigations were retroactive at best, the Commissioner's role duplicates duties, their review of communications interceptions is arbitrary, it is theoretically possible for the oversight of warrants authorisation to be bypassed and for the interception errors to be excessive. It was suggested that it should be the function of an independent judiciary to determine necessity and proportionality when authorising interception warrants.

On these criticisms, *Liberty II* and *Liberty III* convincingly showed the IPT as being preferable to the Commissioner for pre-authorising communications interception warrants. But the *Telegraaf Media* case ultimately showed us that the absence of judicial pre-authorisation of communications interception warrants is a point of concern because arbitrary, uncontrolled abuse and misuse of executive discretionary power that is contrary to the rule of law can be the outcome. Moreover, its comparison of the *Klass* and *Kennedy* cases was criticised because judicial pre-authorisation for surveillance by a commission in the *Klass* case was an example of judicial pre-authorisation for communications interception warrants argued for in Chapter II, whereas the interplay between the IPT and the Commissioner in the *Kennedy* case was an example of the retroactive authorisation for communications interception warrants criticised in part III (*b*)(*i*) and (*ii*).

CHAPTER III: INTERNATIONAL REGULATION OF FOREIGN INTELLIGENCE LIAISON: RECOMMENDATIONS

I INTRODUCTION

Chapter I reviewed the international regulation of foreign intelligence liaison and Chapter II summarised and criticised the international regulation of foreign intelligence liaison through a legal analysis of the relevant case law. Chapter III analyses the international regulation of foreign intelligence liaison through a case study. The case study focuses on the regulation of SIGINT in South Africa, and on national and regional applications of art 17 of the International Covenant on Civil and Political Rights (ICCPR) with regard to private communications. Ultimately, legal reform is suggested through a General Intelligence Laws Amendment Bill (GILAB) 2015.

Part II (*a*) defines the problem in law, what SIGINT is, how it is intercepted and whether it is regulated. Part II (*b*) presents an executive summary of the legal issues. Here, the chapter on 'Interception of Communication and the National Communications Centre (NCC)' in the 2008 Ministerial Review Commission on Intelligence Report, which defined three legal problems, is reviewed. Legal problems arose because SIGINT monitoring was not constitutional, the National Strategic Intelligence Amendment Bill (NCC Bill) had insufficient protections against privacy infringements, and the NIA (National Intelligence Agency) policy on communications interceptions was not consistent with the constitution and the legislation then currently in force. For these reasons, the NCC Bill, which offered a definition of SIGINT and provided for the functions of the NCC, was withdrawn on 15 October 2008. Moreover, the NCC's SIGINT seemed unlawful and unconstitutional in not complying with RICA's requirements of judicial pre-authorisation for communications interceptions.

Part II (*c*) analyses the legal issues surrounding the NCC, the NCC interim policy, the NCC Bill, the NIA policy and the South African Secret Service (SASS) policy.

Part III of the chapter was originally written as part of a group research paper on national and regional applications of art 17 of the ICCPR with regard to private communications.[143] Part III (*a*) analyses the legal framework, scope and limitations, and development and interpretation of the right in South Africa. Part III (*b*) compares the legal framework, scope and limitations, and development and interpretation of the right in Africa.

Part IV takes the form of the solution: the General Intelligence Laws Amendment Bill 2015. The Bill was drafted as a private member's Bill for the South African Shadow Minister for Defence and Military Veterans, David Maynier, between 14 January 2015 and 13 February 2015. The definitions, functions, components and matters connected therewith have been sourced from South African legislation and foreign legislation from Australia, New Zealand, the United Kingdom and the United States.

II REGULATION OF SIGINT IN SOUTH AFRICA

(*a*) Defining the problem in law

(*i*) What is signals intelligence, how is it intercepted and is it regulated?

The National Communications Centre (NCC) intercepts SIGINT as per the State Security Agency's (SSA) counter-intelligence function, mandated by the National Strategic Intelligence Act (NSIA).[144] However, the withdrawal of the NCC Bill on 15 October 2008 means that

- s 1 of the NSIA has not been amended to include the definition of SIGINT;
- s 2 of the NSIA has not been amended to provide for the functions of the NCC, and
- s 3 of the Intelligence Services Act (ISA) has not been amended to provide for the government components that absorb into and make up the SSA.[145]

---

[143] D Brookbanks, K Handschumacher, A Watzlawick, A Whall & C Wirtz. 'National and Regional Applications of art 17 of the ICCPR: A Comparative Study of the Federal Republic of Germany, the United States of America and the Republic of South Africa with regard to Private Communication' (2015, unpublished paper, University of Cape Town) 15–18.
[144] National Strategic Intelligence Act 39 of 1994.
[145] Intelligence Services Act 65 of 2002.

Consequently, SIGINT and the NCC are not regulated by the NSIA or the ISA. However, the NCC should be regulated by the NSIA, the ISA and the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) because the SIGINT collected by the NCC fall within RICA's definition of 'intercept' and 'indirect communication', as per s 1(1) of RICA.[146] As will be discussed, government practice seems to suggest that neither SIGINT nor the NCC has been regulated effectively by RICA.

(*b*) Summary of the legal issues

The chapter on 'Interception of Communication and the NCC' in the 2008 Ministerial Review Commission on Intelligence Report's defined three core legal problems.[147] First, the NCC seemed to have been involved in SIGINT monitoring in a way that was neither constitutional nor lawful because it was not compliant with legislation or the constitution. Secondly, the NCC Bill did not include sufficient protections against infringements of the right to privacy. Thirdly, the National Intelligence Agency's (NIA) policy on communications interception was inconsistent with the constitution or the then current legislation.[148]

The NCC's SIGINT seemed to be unlawful and unconstitutional because it was not compliant with the requirements of RICA that necessitate judicial pre-authorisation in order for communications interceptions to be permissible.[149] As will be seen in the case law in part III (*a*)(*iii*) of this chapter, the Constitutional Court has emphasised the necessity for legislative protections when privacy is being infringed. The changes to the NCC Bill, which encapsulate the NCC's functions, might make the Bill constitutional. The NIA Directive on Communications Monitoring and Interception (NIA policy) limited the right to privacy to citizens but this limitation is not consistent with the applicability of this right to all in South Africa.[150]

---

[146] Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, s 1(1).
[147] J Matthews, F Ginwala & L Nathan 'Intelligence in a Constitutional Democracy' *Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (2008) 180–201.
[148] Matthews et al (note 147) 180.
[149] Matthews et al (note 147) 180–201.
[150] Mathews et al (note 147).

(*c*) The legal issues in detail

(*i*) The National Communications Centre (NCC)

Section 14(*d*) of the South African Bill of Rights enshrines the right not to have the privacy of one's communications infringed.[151] Accordingly, s 2 of RICA does not permit communications interceptions.[152] However, an exception to s 2 is s 16, which permits law-enforcement or security services to intercept communications.[153] As a protection within s 16, judicial pre-authorisation is most important to this exception. The protections are indicative of the will of the Legislature and the Executive to safeguard the right to the privacy of one's communications, and at the same time to justify infringements and independently oversee interceptions that are lawful.[154]

RICA regulates the NCC, in part because the SIGINT collected by the NCC fall within RICA's definition of 'intercept' and 'indirect communication', as per s 1(1) of RICA.[155] Therefore, the NCC's SIGINT must be RICA compliant. However, whether the NCC Bill will be tabled again is unclear because there has been no evidence of its being revisited since it was withdrawn in 2008.[156]

(*ii*) The NCC interim policy

The NCC interim policy tried to bolster the internal checks and balances of the NCC through regulation. However, the policy did not refer to RICA and the legal duty of judicial pre-authorisation of NCC communications interceptions.[157] It should also be noted that the discussion under part II (*c*)(*ii*), (*iv*) and (*v*) of this chapter is limited due to the classification of the NCC, NIA and SASS policies under analysis. Although the NCC Bill is not classified, any policy of the NCC, NIA or SASS is technically classified.

---

[151] Constitution of the Republic of South Africa, s 14(*d*).
[152] Regulation of Interception of Communications and Provision of Communication-related Information Act, s 2.
[153] Section 16.
[154] Mathews et al (note 147) 187–188.
[155] Regulation of Interception of Communications and Provision of Communication-related Information Act, s 1(1).
[156] Mathews et al (note 147) 189.
[157] Regulation of Interception of Communications and Provision of Communication-related Information Act, ss 6, 7, 8, 14 and 15; Mathews et al (note 147) 190–191.

(*iii*) The NCC Bill

The functions and purposes of the NCC were defined by the NCC Bill. Constitutionally, the Bill's reasons for SIGINT communications interceptions applications seemed too broad to justify any infringement of the right to privacy. These grounds would have even permitted state SIGINT over lawful private communications.[158]

The NCC Bill did not cater for judicial pre-authorisation of NCC SIGINT because ministerial approval was considered to be a sufficient alternative to judicial pre-authorisation by those who wrote the Bill. The foreign law of the 'five eyes' SIGINT alliance (Australia, Canada, New Zealand, the United Kingdom and the United States) would not be applicable in other constitutional jurisdictions where judicial pre-authorisation of communications interceptions was a prerequisite. Lawful SIGINT authorised by both ministers and the judiciary should also have been considered by the drafters of the Bill.[159]

RICA's requirement that intelligence officials must obtain judicial pre-authorisation of communications interception was not sufficiently provided by the NCC Bill. The assumption that judges cannot be entrusted with classified information is ill-founded: RICA provides for a designated judge whose very role challenges this assumption.[160]

(*iv*) The NIA Policy

The NIA policy regulates SIGINT operationally and managerially.[161] As mentioned in the summary above, the NIA policy's statutory interpretation is flawed because the protection of the right applies to all in South Africa.[162] That is, the protection does not apply only to South Africans but all who live in South Africa. The NIA cannot make up different levels of rights protection. Therefore, the NIA and other

[158] Mathews et al (note 147) 195–196.
[159] Mathews et al (note 147) 196–197.
[160] Ibid.
[161] National Intelligence Agency 'NIA Operational Directive (OD.08): Authorisation and Management of Communications Monitoring and Interception' 2008 s 1.
[162] Mathews et al (note 147) 198–200; Constitution (note 151).

intelligence organisations are acting outside of the constitution and the law if they undertake communications interceptions without judicial pre-authorisation.[163]

(*v*) The SASS policy

The summary of RICA contained in the South African Secret Service (SASS) Policy on Interception of Communications (SASS policy) does not include RICA sections about the legislative grounds for communications interceptions warrant applications by the intelligence services. However, policies are subject to legislation, whether they include it or not. The SASS policy also states that the SASS director-general should take it upon him- or herself to consent to such policy changes as are deemed best for the service.[164] This is not conducive to rules and procedures of good governance.[165]

III NATIONAL AND REGIONAL APPLICATION OF ART 17 OF THE ICCPR WITH REGARD TO PRIVATE COMMUNICATIONS

Article 17 of the ICCPR states that:

> '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.'[166]

This article has been incorporated into South African law, and this part of Chapter III studies the extent to which art 17 of the ICCPR has been applied in South African law and African regional law. At a national level, the constitutional and statutory framework, scope and limitations, and the courts' development and interpretation of the right are set out. At a regional level, I study the African Charter on Human and Peoples' Rights (Banjul Charter), the African Commission on Human and Peoples' Rights (Commission), the African Court on Justice and Human Rights (African Court) and the respective protocols.

---

[163] Matthews et al (note 147) 200.
[164] South African Secret Service 'Technical Intelligence Policy' s 5.
[165] Mathews et al (note 147) 201.
[166] UNGA ICCPR 2200 (XXI), art 17; Brookbanks et al (note 143).

(*a*) South Africa

(*i*) Legal framework

Section 14(*d*) of the South African Bill of Rights enshrines the right not to have the privacy of one's communications infringed.[167] Accordingly, s 2 of RICA does not permit communications interceptions.[168]

(*ii*) Scope and limitations

However, an exception to s 2 is s 16, which permits intelligence services to intercept communications.[169] Judicial pre-authorisation of communications interception warrants is the most important of the protections against this exception. The protections are indicative of the will of the Legislature and Executive to safeguard the right, justify infringements and independently oversee interceptions that are lawful.[170]

(*iii*) Development and interpretation

In *Bernstein v Bester*, Ackermann J characterised the sphere of the right to privacy on a continuum:

> 'A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation.'[171]

Ackermann J's reasoning was followed by Langa J in the *Hyundai* case:

---

[167] Constitution (note 151).
[168] Regulation of Interception of Communications and Provision of Communication-related Information Act, s 2.
[169] Section 16.
[170] Mathews et al (note 147) 187–188.
[171] *Bernstein and Others v Bester NO and Others* 1996 (4) BCLR 449 (CC) at para 67.

> '[P]rivacy is a right which becomes more intense the closer it moves to the intimate personal sphere of the life of human beings, and less intense as it moves away from that core.'[172]

In the *Hyundai* and *Park-Ross*[173] cases, the Court interpreted the intensity of the sphere of the right by emphasising the importance of judicial authorisation for infringements of the right.[174]

Even if the ICCPR had not been incorporated in South Africa, the Court has used unincorporated conventions as criteria for reviewing the validity of domestic legislation:[175]

> '[T]he reasonableness of parliamentary action to give effect to a provision in the Bill of Rights should be tested against obligations undertaken by the Republic when ratifying an international agreement.'[176]

(*b*) Africa

(*i*) Legal framework

The Banjul Charter does not expressly protect the right not to have the privacy of one's communications infringed.[177] However, the Protocol on the Statute of the African Court of Justice and Human Rights (Protocol) regards international treaties, international custom and general principles of law expressly as applicable law.[178] International treaties, international custom and general principles of law all protect the right.[179] Therefore, the African Court must have regard to the right in carrying out its functions.

Similarly, the Commission draws applicable principles expressly from:

> '… international law on human and peoples' rights … the Universal Declaration of Human Rights, other instruments adopted by the United Nations … in the fields of

---

[172] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2000 (10) BCLR 1079 (CC) at 18.
[173] Ibid; *Park-Ross and Another v Director: Office for Serious Economic Offences* 1995 (2) SA 148 (C).
[174] Ibid.
[175] TW Bennett & J Strug. 'The Relationship between International and Municipal Law.' *Introduction to International Law* (2013) 38.
[176] *Glenister v President of the RSA and Others* 2011 (3) SA 347 (CC) at paras 403–410.
[177] OAS The Banjul Charter CAB/LEG/67/3 rev. 5 1981 arts 1–26.
[178] AU Protocol on the Statute of the African Court of Justice and Human Rights 1998 art 31.
[179] ICCPR (note 166).

> human and peoples' rights as well as from the provisions of various instruments adopted within the Specialised Agencies of the United Nations ….'[180]

The Commission must also consider as subsidiary applicable principles '… general or special international conventions … customs generally accepted as law … legal precedents and doctrine …'.[181] International human-rights law, the ICCPR, the European Convention on Human Rights, the Inter-American Convention on Human Rights (ACHR), customs, legal precedents and doctrines protect the right.[182] Therefore, the Commission must also draw inspiration from the right in carrying out its functions.

(*iii*) Development and interpretation

There are no finalised cases of the African Court or the Commission that develop and interpret the right. The international standard protected by art 17 of the ICCPR, art 12 of the UDHR custom, and general principles of law applies in South Africa.[183] South Africa's modern constitution and statutes expressly protect the right. However, even though South Africa is arguably the most stable regional hegemon, the right is not protected in Africa as it is in Europe and the Americas because the African Court and the Commission must only have regard to and draw inspiration from the right in carrying out their functions.

IV GENERAL INTELLIGENCE LAWS AMENDMENT BILL (THE BILL) 2015

(*a*) Introduction

The Bill's definitions, functions and components have been sourced from South African legislation and foreign legislation from Australia, New Zealand, the United Kingdom and the United States. The South African legislation comprises the National Strategic Intelligence Act, Intelligence Services Oversight Act, Intelligence Services Act, Regulation of Interception of Communications and Communications-

---

[180] AU Protocol (note 177).
[181] Ibid.
[182] ICCPR (note 165); Council of Europe ECHR 4.XI., art 8; OAS ACHR 'Pact of San Jose,' art 11; UNGA UDHR, art 12.
[183] Ibid.

related Information Act and National Strategic Intelligence Amendment Bill.[184] The comparative foreign legislation is made up of the Intelligence Services Act (Australia), the Government Communications Security Bureau Act (New Zealand), the Intelligence Services Act and the Regulation of Investigatory Powers Act (United Kingdom) and the Freedom Act (United States).[185]

(*b*) Summary and analysis

(*i*) Definitions applied to the National Strategic Intelligence Act

The amendments to s 1 of the National Strategic Intelligence Act are changes to key definitions. The definition inserted for 'signals intelligence' and 'foreign signals intelligence' was sourced from the National Strategic Intelligence Amendment Bill because it was the only piece of proposed South African intelligence legislation that defined such intelligence and offered a broadly workable definition. The definition inserted for 'incidentally obtained intelligence' was sourced from the Intelligence Services Act and the Government Communications Security Bureau Act because they were the only pieces of foreign comparative legislation that defined such intelligence and captured the kind of intelligence obtained from bulk communications that are unintentionally intercepted.

(*ii*) Functions applied to the National Strategic Intelligence Act

The amendments to s 2 of the National Strategic Intelligence Act are insertions of the functions of the NCC. The inserted functions were sourced from the National Strategic Intelligence Amendment Bill, the Intelligence Services Act (NZ), the Government Communications Security Bureau Act and the Intelligence Services Act (UK). Whereas the prohibition of SIGINT clause, the exception to the prohibition clause, the functions, the objectives of the functions and the authorisation procedure of the NCC are applied from the National Strategic Intelligence Amendment Bill, the

[184] National Strategic Intelligence Act; Intelligence Services Oversight Act 1994; Intelligence Services Act 2002; Regulation of Interception of Communications and Provision of Communication-related Information Act; National Strategic Intelligence Amendment Bill; General Intelligence Laws Amendment Act 2013.
[185] Intelligence Services Act 2001; Government Communications Security Bureau Act 2013; Intelligence Services Act 1994; Regulation of Investigatory Powers Act 2000; Freedom Act 2015.

limitations to the NCC's functions are applied from the Intelligence Services Act and the communication of incidentally obtained intelligence is applied from the Government Communications Security Bureau Act. The authorisation procedure of the NCC functions as the sunset clause that ultimately protects the judicial pre-authorisation of communications interception warrants:

> 'The agency shall follow the following authorisation procedure:
>
> (*a*) A designated judge shall regulate and authorise in writing the activities of the agency under this section, and in particular authorise each interception target or communication which is to be monitored or intercepted, if the designated judge is satisfied that such activities are necessary to achieve the objectives set out in paragraph (*b*);
>
> (*b*) Any official of the agency who monitors or intercepts any communication without the authorisation of a designated judge as contemplated in paragraph (*a*), or who acts contrary to such authorisation, shall be guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding three years.'[186]

(*iii*) Government components applied to RICA

The amendments to s 3 of RICA are insertions of the 'National Communications Centre' and 'Office for Interception Centre' government components. This is because these government components, the organs of state that regulate SIGINT in South Africa, were not originally included in RICA. This insertion is part of the recent absorption of the government components that now make up the SSA.

(*iv*) Definitions applied to RICA

The amendments to s 1 of RICA are changes to key definitions. The definition inserted for 'account identifier' was sourced from the Freedom Act (US) and expressly provides for means of more strategically targeting bulk communications interceptions. The definitions inserted for 'archived-communication related information' and 'communication-related information' were sourced from the Freedom Act and expressly provide for email and social media information that can and cannot be corresponded or stored. The definition inserted for 'private communication' was sourced from the Government Communications Security

[186] Government Communications Security Bureau Act; Intelligence Services Act; National Strategic Intelligence Amendment Bill.

Bureau Act and acts as a safeguard of the right not to have the privacy of one's communications infringed.

(*v*) Reporting on interception requests, directions and devices

The amendments after s 25 of RICA are insertions of s 26, 38, 42 and 58 about judicial and government reporting on interception requests, third-party reporting on interception directions and Inspector-General reports on interception devices sourced from the National Strategic Intelligence Amendment Bill and the Freedom Act. The judicial reporting includes statistics, information disclosure and the dates when the report needs to be tabled; the government reporting includes which minister must table the report, where the report must be tabled and the necessary disclosure of statistics; the third-party reporting notes the service providers that must provide statistical financial statements and a liability limitation clause; the Inspector-General report provides for the number of reports on the activities of the NCC that need to be made to Parliament. Cumulatively, part V (*b*)(*i*), (*ii*), (*iii*), (*iv*) and (*v*) are an innovative application of the horizontal accountability mechanism and international best practice that can better regulate SIGINT in South Africa. The Bill solves the problems of abuse and misuse of foreign intelligence in law by applying foreign legislation to the process of legal writing and drafting.

V CONCLUSION

Part II (*c*) unpacked the legal issues surrounding the regulation of SIGINT in South Africa. With regard to the NCC, judicial pre-authorisation was found to be the most important of the protections against the exception that permits communications interceptions. However, the NCC interim policy did not refer to RICA and the legal duty for judicial pre-authorisation of NCC communications interceptions. Similarly, the NCC Bill did not cater for judicial pre-authorisation of NCC SIGINT because ministerial approval was considered to be a sufficient alternative to judicial pre-authorisation by those who wrote the Bill, and RICA's requirement that intelligence officials must obtain judicial pre-authorisation for communications interceptions was not sufficiently provided for by the NCC Bill. As for the NIA policy, the NIA and other intelligence organisations were acting outside of the constitution and the law if

they undertook communications interceptions without judicial pre-authorisation. The SASS Policy on Interception of Communications summary of RICA did not include RICA's section about the legislative grounds for communications interceptions warrant applications by the intelligence services.

Part III's national and regional applications of art 17 of the ICCPR with regard to private communications were considered in South Africa and Africa.

In South Africa, the legal framework of the right showed that s 2 of RICA, which does not permit communications interceptions, and judicial pre-authorisation are the most important of the protections against the exception to s 2 with regard to the scope and limitations of the right. The development and interpretation of the right was seen in the *Hyundai* and *Park-Ross* cases, where Ackermann J and Langa J's reasons were applied by the Court when it developed and interpreted the intensity of the sphere of the right by emphasising the importance of judicial authorisation for infringements of the right.

In Africa, the legal framework, scope and limitations of the right showed that the African Court must have regard to the right in carrying out its functions and that the Commission must also draw inspiration from the right in carrying out its functions. With regard to the development and interpretation of the right, I did not find finalised cases of the African Court of the Commission that developed and interpreted the right, but South Africa's modern constitution and statutes expressly protect the right.

Part IV suggested legal reform in South Africa through applying to key South African intelligence legislation international legal best practice arising out of comparative foreign legislation. The international best practice was drawn from the foreign legislation from Australia, New Zealand, the United Kingdom and the United States. The key South African intelligence legislation that I recommended amending through this application was the National Strategic Intelligence Act, the Intelligence Services Act and the Regulation of Interception of Communications and Provision of Communication-related Information Act. Foreign legislation arising out of international best practice from Australia (Intelligence Services Act), New Zealand (Government Communications Security Bureau Act), United Kingdom (Intelligence Services Act and Regulation of Investigatory Powers Act) and United States (Freedom Act) was applied when drafting the Amendment Bill.

CONCLUSION

Snowden emphasised that 'the balance of power between the citizenry and the government is becoming that of the ruling and the ruled as opposed to the elected and the electorate'.[187] The relationships between citizens and government, the ruling and the ruled and the elected and the electorate helped shape this thesis and underlie the importance of the international regulation of foreign intelligence, particularly foreign SIGINT liaison. These themes were apparent throughout Chapter I's review of the international regulation of foreign intelligence liaison as a phenomenon, Chapter II's legal analysis of the international regulation of foreign intelligence liaison and through the *Liberty II* and *Liberty III* judgments and Chapter III's analysis of the international regulation of foreign intelligence liaison through recommendations.

Chapter I's key argument posited that the inevitable abuse and misuse of foreign intelligence liaison should be regulated through the horizontal accountability mechanism as an international best practice. Chapter II's core argument claimed that communications interception warrants should be regulated by judicial pre-authorisation. Chapter III applied Chapter I and II's primary arguments by recommending legal reform through an Amendment Bill.

I conclude my dissertation by applying the sub-arguments that Chapter I made for the international regulation of foreign intelligence liaison to Chapter II's and Chapter III's central arguments. Chapter I defined foreign intelligence and argued that foreign intelligence liaison must be regulated by independent judicial oversight and accountability in liberal democracies.[188] The Ottawa Principles on Anti-terrorism and Human Rights suggested that an essential element of a regime for international law in liberal democracies such as the UK and US regimes is judicial controls.[189] There are, however, challenges to effective judicial oversight of foreign intelligence liaison as we learnt that independent judicial oversight brings with it the problems of sensitive information being shared outside of foreign intelligence services – as in Chapter II's example of sharing foreign intelligence with the Commissioner and the IPT in the United Kingdom.[190] The Bill's recommendations

[187] Poitras (note 1).
[188] Hannah et al (note 3) 12.
[189] Forcese et al (note 12).
[190] Caparini (note 13) 13.

for judicial reporting on interception requests are an important application of these principles.[191]

Chapter I argued that the horizontal (specifically the restraint of state institutions by the judicial branch of government) and third dimension (international actors' role in restraining state institutional actors) are potential accountability solutions to the challenges to effective judicial oversight of foreign intelligence liaison.[192] I also claimed that the problems associated with the trading of information and the circumvention of domestic law have drawn attention to the need for more effective judicial oversight. Non-compliance with domestic laws has become apparent when information is unaccountably traded between intelligence agencies. For example, intercepted bulk communications were traded between the UK and US foreign intelligence agencies, as evidenced in my summary of the *Liberty II* and *Liberty III* judgments. Therefore, the Bill's insertion of government reporting on interception requests, third-party reporting on interception directions and Inspector-General reports on interception devices in Chapter III functions as a pertinent example of this horizontal accountability mechanism.[193]

Chapter I focused on the globalisation of foreign intelligence liaison and showed that this phenomenon has increased the need for accountability mechanisms at national, regional and international levels. These accountability tools were dealt with nationally through judicial co-operation, often in the form of rendition, and in the case of Chapter II, through foreign SIGINT liaison.[194] In Chapter II, I continued to defend the proposition that judicial co-operation over intelligence liaison shone light on legal accountability mechanisms as a more effective national accountability mechanism over intelligence liaison than political equivalents. This was inspired by the *Liberty II* and *Liberty III* judgments. Therefore, Chapter III's analysis of the national and regional applications of art 17 of the ICCPR with regard to private communication become all the more relevant to understanding different levels of accountability.[195]

Chapter I asserted that regional inquiries have functioned as a more effective tool for oversight, particularly with regard to rendition, than national mechanisms.

---

[191] Freedom Act.
[192] Caparini (note 13) 7–10.
[193] National Strategic Intelligence Amendment Bill; Freedom Act.
[194] Aldrich (note 30) 12; *Liberty II* (note 81).
[195] Brookbanks et al (note 166).

However, Chapter II challenged this assertion in the context of the regional regulation of foreign SIGINT liaison. The challenge offers a prediction about the appeal to the 5 December 2014 and 6 February 2015 UK judgments and rulings that Liberty has filed to the European Court of Human Rights. This regional appeal is expected to be heard sometime during 2015. Partly because of the number of UK reservations to the jurisdiction of the ECtHR, I predict that even if the appeal is successful for reasons similar to those argued in my critique, it will be the *Liberty II* and *Liberty III* judgments in the United Kingdom and not the ECtHR regional appeal that ultimately leads to significant surveillance law reform in the United Kingdom and internationally. The focus on national jurisdictional discretion on matters such as national security is a reason for this. A stronger national application of the right in South Africa as opposed to the weaker regional application of the right in Africa was argued for in Chapter III and my conclusion on this question helps to illustrate why national mechanisms for oversight have been more effective than regional alternatives.[196]

Chapter I noted that the international regulation of foreign intelligence liaison has also been considered by international organisations such as the United Nations. The international regulation of foreign SIGINT liaison as confronted by the *Liberty II* and *Liberty III* judgments in Chapter II strongly suggested the need for a third dimension or an international accountability solution to the problem of its effective judicial oversight. There is an emerging global administrative legal scholarship that I envisage could potentially provide novel solutions to the problems of the international judicial regulation of foreign intelligence liaison, but these were not within the scope of this dissertation.[197] From Chapter III's summary and analysis of international best practice that has arisen out of legislation from Australia, New Zealand, the United Kingdom and the United States a case has been argued for a third dimension or international accountability solution.[198]

Chapter I identified different forms of foreign intelligence liaison, notably bilateral liaison between allies such as the United Kingdom and the United States.[199]

---

[196] Brookbanks et al (note 166).
[197] B Kingsbury, N Krisch & I Stewart 'The Emergence of Global Administrative Law' (2005) 68 *Law and Contemporary Problems* 15.
[198] Intelligence Services Act; Government Communications Security Bureau Act; Intelligence Services Act; Regulation of Investigatory Powers Act; Freedom Act.
[199] Lefebvre (note 56) 534.

It was argued that formal rather than informal bilateral liaison was the preferred form of foreign intelligence co-operation to come under regulation between traditional alliances. This commonly included original and synchronised intelligence systems such as that under scrutiny between the United Kingdom and United States in the *Liberty II* and *Liberty III* judgments.[200] My Chapter II summary and critique of these landmark judgments asserted that the United States is the hub of the global telecommunications network. However, beyond intelligence-gathering capabilities, the formal bilateral liaison between the United Kingdom and the United States, as evidenced in the *Liberty II* and *Liberty III* cases, seems reminiscent of a symmetrical traditional alliance which requires an independent judiciary in international law to regulate against the abuse or misuse of foreign intelligence liaison.[201] This inevitable abuse or misuse served as the primary reason for my critique of the *Liberty II* judgment. The need for an independent judiciary to regulate against the abuse or misuse of foreign intelligence liaison is a reason for Chapter III's proposed Bill not only including a definition of the designated judge to the amendments to the National Strategic Intelligence Act but suggesting amendments to RICA by the insertion of a clause that provides for judicial reporting on interception requests.[202]

My first Chapter posited that legal systems should frame the operations of liaison relationships. It was assumed that even allies such as the United Kingdom and the United States would not, in theory, co-operate with requests that breach the domestic legitimacy of privacy laws or statutory principles.[203] The analysis of the *Liberty II* and *Liberty III* cases in Chapter II has clearly shown that this theoretical assumption does not hold true in practice because the intelligence agencies' activities were ruled to be arbitrary and unlawful for the first time in the 15-year history of the IPT's jurisprudence. Moreover, this theoretical assumption seemed to be even more dubious in practice as Chapter III showed that the unregulated NCC SIGINT programme in South Africa infringed everyone's constitutional and legislative right not to have the privacy of their communications infringed.[204]

---

[200] Lefebvre (note 56) 532–533.
[201] Reveron (note 63) 467–468.
[202] Regulation of Interception of Communications and Provision of Communication-related Information Act; Freedom Act.
[203] Rudner (note 59) 215.
[204] Mathews et al (note 147) 198–200; Constitution (note 151).

Chapter I mapped out the cost and benefit of foreign intelligence liaison. We saw this in practice through the *Liberty II* and *Liberty III* judgments as an example of complex symmetrical liaison because a blend of intelligence-gathering assets was bartered equitably between the United Kingdom and the United States through foreign intelligence platforms.[205] The co-operation costs of the foreign intelligence liaison between these two states in the *Liberty II* judgment ought to be calculated through the costs associated if the loss of UK–US co-operation did not meet potential intelligence and counterintelligence alternatives.[206] Chapter II showed that these alternatives should have been lawful and not arbitrary, as was held to have been the case in the *Liberty III* judgment. In other words, the law should never be interpreted as a cost but should be embraced as a regulatory benefit. Chapter III spoke to the regulatory benefit of the law rather than the cost and benefit of foreign intelligence liaison through the rulings in the *Bernstein v Bester*, *Hyundai*, *Park-Ross* and *Glenister* cases and the legal reform recommended in the Bill.[207]

I argued in Chapter I that mistrust between, for example, the United Kingdom and the United States, can be overcome through decentralised foreign intelligence liaison and via best-practice methods that develop trust between foreign intelligence agencies overtime.[208] While decentralised international and independent judicial regulation of foreign intelligence liaison may realise fewer overall gains in foreign intelligence sharing than an institutionally centralised alternative, decentralised foreign intelligence liaison would probably be a more realistic and humble development in the regulation of foreign intelligence sharing.[209] The foundational building block of any international best-practice methodology ought to be an independent international judiciary that helps to regulate practice. Chapter II, therefore, asserted that international judicial regulation of foreign intelligence liaison will lead, in the long term, to international best-practice methodologies of the kind inspired by the legal reform being pressured to arise out of the *Liberty II* and *Liberty III* judgments. Furthermore, Chapter III's application of the argument for judicial pre-authorisation of communications interception warrants to the Bill through the functions of the NCC authorisation procedure is a useful example of how

[205] Sims (note 68) 196–197, 200.
[206] Sims (note 68) 199.
[207] Sims (note 68) 170–172, 175.
[208] Svendsen (note 79) 136, 139.
[209] Svendsen (note 79) 640–641.

international best-practice methods can develop trust and regulate foreign intelligence liaison in the long run. The case study achieved this through the best-practice method of legal reform – the Bill.

IV APPENDIX

REPUBLIC OF SOUTH AFRICA

_____

GENERAL INTELLIGENCE LAWS AMENDMENT BILL 2015

_____

(As introduced in the National Assembly (proposed section ?);
explanatory summary of Bill published in Government Gazette No. 1 of 1 September 2015)
(The English text is the official text of the Bill)

_____

(DAVID MAYNIER, MP)

[B 1-2015]

ISBN 1-2-3-4-5

No. of copies printed ……. ?

GENERAL EXPLANATORY NOTE:

[ ] Words in bold type in square brackets indicate omissions from existing enactments.

_____ Words underlined with a solid line indicate insertions in existing enactments.

BILL

To amend the National Strategic Intelligence Act, 1994, so as to insert new definitions; and to provide for the functions of the agency; and to provide for matters connected therewith. To amend the Intelligence Services Act, 2002, so as to provide for the government components that absorb into and make up the State Security Agency. To amend the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002, so as to insert new definitions; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:–

Amendment of section 1 of Act 39 of 1994, as amended by section 1 of Act 37 of 1998, section 1 of Act 66 of 2000, section 1 of Act 67 of 2002, section 1 of Act 52 of 2003 and section 1 of Act 11 of 2013

1. Section 1 of the National Strategic Intelligence Act, 1994 (hereinafter referred to as the principal Act),

is hereby amended-

(a) by the insertion after the definition of "Cabinet" of the following definition:
"communication" means communication as defined in the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002;"[210];

(b) by the insertion after the definition of "departmental intelligence" of the following definition:
" **'designated judge'** means designated judge as defined in the in the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002;"[211];

(c) by the insertion after the definition of "foreign military intelligence" of the following definition:
" **'foreign signals intelligence'** means intelligence derived from the interception of electromagnetic, acoustic, and other signals, including the equipment and encrypted material that produces such signals, and includes any communication that eminates from a foreign person or a foreign organisation outside the borders of the Republic, or passes through or ends in the Republic;"[212];

(d) by the insertion after the definition of "foreign signals intelligence" of the following definition:

---

[210] Regulation of Interception of Communications and Provision of Communication-Related Information Act.
[211] Ibid.
[212] National Strategic Intelligence Amendment Bill.

" (a) **'incidentally obtained intelligence'** means intelligence that is obtained in the course of gathering intelligence about the capabilities, intentions, or activities of foreign persons or foreign organisations; but
(b) that is not intelligence of the kind referred to in paragraph (a);"[213];
(e) by the insertion after the definition of "interception direction" of the following definition:
" **'interception target'** means interception target as defined in the notice in terms of section 31 of the Regulation of Interception of Communications and Provision of Communication-related information Act No. 70 of 2002;"[214];
(f) by the insertion after the definition of "Minister" of the following definition:
" **'monitor'** means monitor as defined in the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002;"[215];
(g) by the insertion after the definition of "National Prosecuting Authority Act" of the following definition:
" **'national security'** means national security as defined in the General Intelligence Laws Amendment Act No. 11 of 2013;"[216];
(h) by the insertion after the definition of "national security" of the following definition:
" **'signals intelligence'** means intelligence derived from the interception of electromagnetic, acoustic, and other signals, including the equipment and encrypted material that produces such signals, and includes any communication that eminates from inside the borders of the Republic;"[217];

Amendment of section 2 of Act 39 of 1994, as amended by section 2 of Act 37 of 1998, section 2 of Act 67 of 2002 and section 2 of Act 11 of 2013

2. Section 2 of the principal Act is hereby amended by the insertion after subsection (2A) of the following subsection:
" (2B) The agency is prohibited from collecting signals intelligence unless:

(i) for the collection of foreign signals intelligence as stated in the functions of 2C(*a*)(i);
(ii) for the performance of the SSA's functions as stated in 2C(*a*);
(iii) the collection is authorised by the designated judge as stated in 2D;

but does not include:

(i) any activities for the purpose of furthering the interests of a South African political
party or other South African political organisation;
(ii) any activities that the agency does not perform with due regard for the functions

[213] Government Communications Security Bureau Act; Intelligence Services Act.
[214] Regulation of Interception of Communications and Provision of Communication-related Information Act.
[215] Ibid.
[216] Freedom Act.
[217] National Strategic Intelligence Amendment Bill.

contemplated in paragraph 2C(*a*), the rights set out in Chapter 2 of the Constitution
and subject to paragraph 2C(d);

(2C) *(a)* The functions of the agency shall, subject to section 3, be:
(i) to collect foreign signals intelligence about the capabilities, intentions or activities of foreign persons or foreign organisations outside of the Republic;
(ii) to control and advise on the provision and application of cryptographic solutions, communication and computer technologies and other specialised technologies acquired in connection with the performance of its other functions in the Republic, in consultation with the relevant stakeholders;
(iii) to promote the co-ordination and optimal usage of all national signals intelligence resources and platforms in the Republic; and
(iv) to undertake and co-ordinate research, design and development of all cryptographic solutions and information communications technology security systems and products for all organs of state, in consultation with the relevant stakeholders;
(b) The agency may contemplate the functions contemplated in paragraph *(a)* only for the following objectives:
(i) the function as stated in 2C(*a*)(i);
(ii) To identify any threat or potential threat to the national security of the Republic or its people;
(c) to intercept communication as a method of last resort that can only take place if non-intrusive methods are inadequate or inappropriate;
(d) The agency is prohibited from intercepting any communications that do not fall within the definition of "foreign signals intelligence";
(e) The function of the agency to co-operate with other entities to facilitate their functions is to co-operate with, and to provide advice and assistance to, the following for the purpose of facilitating the performance of their functions:
(i) Electronic Communications Security (Pty) Ltd;
(ii) the South African National Academy of Intelligence;
(iii) the National Intelligence Agency;
(iv) the South African Secret Service;
(v) the National Communications Centre; and
(vi) the Office for Interception Centre.
(f) To avoid doubt, the agency may perform its function under paragraph *(e)*-
(i) only to the extent that the advice and assistance are provided for the purpose of activities that the entities may lawfully undertake; and
(ii) subject to and in accordance with any limitations, restrictions, and protections under which those entities perform their functions and exercise their powers; and
(iii) even though the advice and assistance might involve the exercise of powers by, or the sharing of the capabilities of, the agency that the agency is not, or could not be, authorised to exercise or share in the performance of its other functions.
(g) Any advice or assistance provided by the agency under paragraph *(e)* to another entity is subject to-
(i) the jurisdiction of any other body or authority to the same extent as the other entity's actions are subject to the other body's or authority's jurisdiction; and

(ii) the oversight of the Inspector-General of Intelligence under his or her functions in section 7 of the Intelligence Services Oversight Act No. 40 of 1994;"[218];

2D The agency may communicate incidentally obtain intelligence only if:
(ii) to communicate incidentally obtained intelligence to appropriate State authorities or to authorities of other countries approved by a designated judge as being capable of assisting the agency in the performance of its functions if the intelligence relates to the involvement, or likely involvement, by a person in one or more of the following activities:

(ii.i) activities that present a significant risk to a person's safety;
(ii.ii) acting for, or on behalf of, a foreign power;
(ii.iii) activities that are a threat to national security; and
(ii.iv) committing a serious crime; and

2E The agency shall follow the following authorisation procedure:
(a) A designated judge shall regulate and authorise in writing the activities of the agency under this section, and in particular authorise each interception target or communication which is to be monitored or intercepted, if the designated judge is satisfied that such activities are necessary to achieve the objectives set out in paragraph *(b)*;
(b) Any official of the agency who monitors or intercepts any communication without the authorisation of a designated judge as contemplated in paragraph *(a)*, or who acts contrary to such authorisation, shall be guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding three years;"[219];

Amendment of section 3 of Act 65 of 2002, as amended by section 3 of Act 11 of 2013

1. Section 3 of the Intelligence Services Act, 2002 (hereinafter referred to as the principal Act),

is hereby amended by the insertion after subsection 3(1) of the following subsection:
"3(1A) The following government components listed in Part A of Schedule 3 to the Public Service Act, 1994 (Proclamation No. 103 of 1994), as that Part read immediately prior to the commencement of the General Intelligence Laws Amendment Act, 2013, are hereby absorbed into and make up the State Security Agency:
(a) Electronic Communications Security (Pty) Ltd;
(b) the South African National Academy of Intelligence;
(c) the National Intelligence Agency;
(d) the South African Secret Service;
(e) the National Communications Centre; and
(f) the Office for Interception Centre.

[218] Government Communications Security Bureau Act; Intelligence Services Act; Intelligence Services Act; National Strategic Intelligence Amendment Bill.
[219] Government Communications Security Bureau Act; Intelligence Services Act; National Strategic Intelligence Amendment Bill.

Amendment of section 1 of Act 70 of 2002, as amended by section 1 of Act 36 of 2005, section 1 of Act 48 of 2008, section 1 of Act 1 of 2011 and section 1 of Act 11 of 2013

1. Section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (hereinafter referred to as the principal Act),

is hereby amended-

(a) by the insertion after "definitions and interpretation" of the following definition:

" **'account identifier'** means a telephone or instrument number, other subscriber number,

email address, or username used to uniquely identify an account;"[220];

(b) by the insertion after the definition of "archived communication-related direction" of the following definition:

" '**archived-communication related information'** means any communication-related information in the possession of a telecommunication, email or social media service provider and which is being stored by that telecommunication, email or social media service provider in terms of section 30(1)(*b*) for the period determined in a directive referred to in section 30(2)(*a*), beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;

(c) by the insertion after the definition of "communication" of the following definition:

" **'communication-related information'** means-

(1) any information relating to an indirect communication which is available in the records of a telecommunication, email or social media service provider, and includes switching, dialing, signaling information and the "to" and "from" lines in an email that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication, email or social media service provider;

(2) does not include-

(a) the substantive content of any communication as defined in the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002;

(b) the name, address or financial information of a subscriber or customer; or

(c) cell site location information;"[221];

(d) by the insertion after the definition of "informal settlement" of the following definition:

" **'information'** means information as defined in the Protection of Information Bill No. 28

of 2008;"[222];

(e) by the insertion after the definition of "private body" of the following definition:

" **'private communication'-**

---

[220] Freedom Act.
[221] Ibid.
[222] Protection of Information Bill 2008.

(a) means a communication between two or more parties made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication but;
(b) does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so;"[223];

Insertion after section 25 of Act 70 of 2002

1. Section 26 is hereby inserted into the principal Act:

"**26. Judicial Reporting on Interception Requests**

[In general,] a report regarding the functions performed by the designated judge in terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002, including statistics regarding such functions, together with any comments or recommendations which the designated judge may deem appropriate, must

(a) disclose any information contained in an application or direction referred to in the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002; and
(b) be tabled annually in September in the National Assembly"[224];

Insertion after section 37 of Act 70 of 2002

2. Section 38 is hereby replaced by the insertion of the following reporting provisions:

"**38. Government Reporting on Interception Requests.-**

"The Minister of State Security must table an annual report to the National Assembly disclosing statistics regarding any application(s) made under Chapter 3 of the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002;"

Insertion after section 41 of Act 70 of 2002

3. Section 42 is hereby inserted into the principal Act:

"**42. Third-party Reporting on Interception Directions.-**

(1) (a) Any decryption key holder, telecommunication, postal, email and social media service provider must disclose in its annual financial statements statistical information as any applications received and direction complied with in terms of Chapter 3 and section 25 of the Regulation of Interception of Communications and Communication-related Information Act No. 70 of 2002;

[223] Government Communications Security Bureau Act.
[224] Freedom Act.

(2) Limitation on liability – any holder or service provider contemplated in subsection (1), who discloses information contemplated in that subsection and whom reasonably believes, in good faith, that such disclosure is authorised by this section, is not criminally or civilly liable in any court for such disclosure;"[225];

Insertion after section 57 of Act 70 of 2002

5. Section 57 of the principal Act is hereby replaced by the insertion after Chapter 10 of the following reporting provisions:

"**58. Inspector General Reports on Interception Devices**.-

The Inspector-General of Intelligence contemplated in section 7 of the Intelligence Services Oversight Act No. 40 of 1994, shall report annually to Parliament on the activities of the NCC, and in such report indicate any contraventions by the NCC of the provisions of the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002;"[226].

[225] Freedom Act.
[226] National Strategic Intelligence Amendment Bill.

REFERENCES

Primary sources

Constitutions

South Africa:

Constitution of the Republic of South Africa, 1996.

Statutes

Foreign:

Intelligence Services Act 2001 (Australian).
Government Communications Security Bureau Act 2013 (New Zealand).
Intelligence Services Act 1994 (United Kingdom).
Regulation of Investigatory Powers Act 2000 (United Kingdom).
Foreign Intelligence Surveillance Act 1978 (United States).
Freedom Act 2015 (United States).
Patriot Act 2001 (United States).

International:

African Charter on Human and Peoples' Rights CAB/LEG/67/3 rev. 5 1981 Organisation of African Unity, Addis Ababa.
American Convention on Human Rights 'Pact of San Jose' Organisation of American States 1969 Inter-American Specialised Conference on Human Rights, Costa Rica.
Council of Europe 'European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment' 2002 European Court of Human Rights, Strasbourg 3-33.
Council of Europe 'European Convention on Human Rights' 4.XI., 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, Rome.
Council of Europe 'European Convention on Human Rights' 2002 European Court of Human Rights, Strasbourg 3–55.
Protocol on the Statute of the African Court of Justice and Human Rights 1998 Tanzania, Arusha.
United Nations General Assembly 'Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment' 1984 United Nations Secretariat, New York.
United Nations General Assembly 'International Covenant on Civil and Political Rights' 2200 (XXI) 1976 United Nations Secretariat, New York.
United Nations General Assembly 'Universal Declaration of Human Rights' 1948 United Nations Secretariat, New York.
United Nations Security Council 'Resolution 1595' 2005 S/RES/1595 UN Department of Public Information, New York 1–3.

South African:

General Intelligence Laws Amendment Act 11 of 2013.
Intelligence Services Act 65 of 2002.
Intelligence Services Oversight Act 40 of 1994.
National Strategic Intelligence Act 39 of 1994.
National Strategic Intelligence Amendment Bill [B 38-2008].
Protection of Information Bill 2008.

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

Cases

Foreign:
El-Masri v the former Yugoslav Republic of Macedonia 2012 39630/09 ECHR (European).
General Prosecutor at the Court of Appeals of Milan v Adler and ors 46340/2012 ILDC 1960 (IT 2012) (Italian).
Kennedy v United Kingdom 2011 52 EHRR 4 (European).
Klass v Germany [1978] ECHR 5029/71 (European).
Liberty v United Kingdom 2009 48 EHRR 1 (European).
Liberty (The National Council of Civil Liberties) and Others v The Government Communications Headquarters and Others IPT/13/77/H (United Kingdom).
Liberty (The National Council of Civil Liberties) and Others v The Secretary of State for Foreign and Commonwealth Affairs and Others IPT/13/77/H (United Kingdom).
Liberty (The National Council of Civil Liberties) and Others v The Secretary of State for Foreign and Commonwealth Affairs and Others IPT/13/77/H (United Kingdom).
Telegraaf Media Nederland v the Netherlands 2012 34 BHRC 193 (Dutch).

South African:
Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449 (CC).
Glenister v President of the RSA and Others 2011 (3) SA 347 (CC).
Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2000 (10) BCLR 1079 (CC).
Park-Ross and Another v Director: Office for Serious Economic Offences 1995 (2) SA 148 (C).

Secondary sources

Articles

Aldrich, RJ. 'Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem.' 24(1) *Intelligence and National Security* (2009, Taylor & Francis, London) 1–39.
Alexander, MS. 'Introduction: Knowing your Friends, Assessing your Allies – Perspectives on Intra-alliance Intelligence.' *Intelligence and National Security* (2008, Routledge, London) 1–17.
Born, H. 'Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices.' 3(4) *Connections: The Quarterly Journal* (2004, Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Garmisch-Partenkirchen) 1–12.
Born, H & Leigh I. 'Democratic Accountability of Intelligence Services.' *Geneva Centre for the Democratic Control of Armed Forces (DCAF) Policy Paper No. 19* (2007, Geneva Centre for the Democratic Control of Armed Forces, Geneva) 1–21.

Brookbanks, D, Handschumacher, K, Watzlawick, A, Whall, A & Wirtz, C. 'National and Regional Applications of art 17 of the ICCPR: A Comparative Study of the Federal Republic of Germany, the United States of America and the Republic of South Africa with regard to Private Communication' (2015, unpublished paper, University of Cape Town) 2–19.

Caparini, M. 'Controlling and Overseeing Intelligence Services in Democratic States.' In H Born & M Caparinin (eds) *Democratic Control of Intelligence Services: Containing Rogue Elephants* (2007, Ashgate Publishing, Hampshire) 3–24.

Forcese, C & LaViolette, N. 'Ottawa Principles on Anti-terrorism and Human Rights.' *The Human Rights of Anti-terrorism: A Colloquium* (2007, Human Right Research and Education Centre, Ottawa).

Hannah, G, O'Brien, KA & Rathmell, A. 'Intelligence and Security Legislation for Security Sector Reform.' *Technical Report for the United Kingdom's Security Sector Development Advisory Team* (2005, Rand Corporation, Cambridge) 1–41.

Lander, S. 'International Intelligence Co-operation: An Inside Perspective.' 17(3) *Cambridge Review of International Affairs* (2004, Carfax Publishing, London) 481–493.

Lefebvre, S. 'The Difficulties and Dilemmas of International Intelligence Co-operation' 16(4) *International Journal of Intelligence and Counterintelligence* (2011, Taylor & Francis, London) 527–542.

Reveron, DS. 'Old Allies, New Friends: Intelligence-Sharing in the War on Terror.' 3 *Orbis 50* (2006, Elsevier, Amsterdam) 453–468.

Rudner, M. 'Hunters and Gatherers: The Intelligence Coalition against Islamic Terrorism.' 17(2) *International Journal of Intelligence and Counterintelligence* (2004, Taylor & Francis, London) 193–230.

Sims, JE. 'Foreign Intelligence Liaison: Devils, Deals, and Details.' 19(20) *International Journal of Intelligence and Counterintelligence* (2006, Taylor & Francis, London) 195–217.

Svendsen, A. 'The Globalisation of Intelligence since 9/11: Frameworks and Operational Parameters.' 21(1) *Cambridge Review of International Affairs* (2008, Taylor & Francis, London) 131–144.

Walsh, JI. 'Intelligence-Sharing in the European Union: Institutions Are Not Enough.' (2006) 44(3) *Journal of Common Market Studies* 625–643.

Wright, A. 'Casting a Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight, and Review.' In N LaViolette & C Forcese (eds) *The Human Rights of Anti-terrorism* (2008, Irwin Law, Toronto) 327–367.

Books

Bennett, TW & Strug, J. *Introduction to International Law* (2013, Juta, Cape Town).

Greenwald, G. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (2014, Hamish Hamilton, London) 108–119.

Montague, LL. *General Walter Bedell Smith as Director of Central Intelligence, October 1950–February 1953* (1992, Penn State Press, Philadelphia).

Commissions

Matthews, J, Ginwala, F & Nathan, L. 'Intelligence in a Constitutional Democracy' *Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (2008, Ministerial Review Commission on Intelligence, Cape Town) 180–201.

Documentaries

Poitras, L 'Citizen Four' *Documentary* 2014 Radius TWC.

Directives and Policy

British Government. 'British Government Briefing Papers on Iraq.' *Declassified Draft of British Government's White Paper* (2002, British Government, London) 1–44.

British Government. 'Iraq's Weapons of Mass Destruction: The Assessment of the British Government.' *Final Version of British Government's White Paper* (2002, Stationery Office, London) 1–51.

Director of Central Intelligence. 'Iraq's Weapons of Mass Destruction Programs.' *CIA White Paper* (2002, Intelligence Community, Washington, DC) 1–25.

Ford, CW. 'Niger/Iraq Uranium Story and Joe Wilson (S/NF).' *Unclassified Memorandum* (2003, Department of State, Washington, DC).

National Intelligence Agency. 'NIA Operational Directive (OD.08): Authorisation and Management of Communications Monitoring and Interception.' (2008) s 1.

South African Secret Service. 'Technical Intelligence Policy' s 5.

Reports

Butler, R. 'Review of Intelligence on Weapons of Mass Destruction.' *Report of a Committee of Privy Counselors* (2004, The Stationery Office, London) 1–196.

9/11 Commission. *The 9/11 Commission Report* (2004, National Commission on Terrorist Attacks upon the United States, Washington, DC) 1–567.

Commissioner's Report.

Davis, T. 'Secretary General's Report under Article 52 ECHR on the Question of Secret Detention and Transport of Detainees Suspected of Terrorist Acts, notably by or at the Instigation of Foreign Agencies.' *Council of Europe Information Documents* (2006, SG/Inf 5 Council of Europe, Strasbourg) 1–50.

Davis, T. 'Secretary General's Supplementary Report under Article 52 ECHR on the Question of Secret Detention and Transport of Detainees Suspected of Terrorist Acts, notably by or at the Instigation of Foreign Agencies.' *Council of Europe Information Documents* (2006, SG/Inf 13 Council of Europe, Strasbourg) 1–35.

Fava, GC 'Report on the Alleged Use of European Countries by the CIA for the Transportation and Illegal Detention of Prisoners (2006/2200(INI)).' *Temporary Committee on the Alleged Use of European Countries by the CIA for the Transportation and Illegal Detention of Prisoners Final Session Document* (2007, A6-0020/2007 European Parliament, Brussels) 1–77.

Hutton, B. *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly CMG.* (2004, The Stationery Office, London) 1–328.

Interception of Communications Code of Practice.

Marty, D. 'Abuse of State Secrecy and National Security: Obstacles to Parliamentary and Judicial Scrutiny of Human Rights Violations.' *Committee on Legal Affairs*

and Human Rights Report (2011, Doc. 12714 Parliamentary Assembly of the Council of Europe, Strasbourg) 1–23.

Marty, D. 'Alleged Secret Detentions and Unlawful Inter-state Transfers of Detainees Involving Council of Europe Member States.' *Committee on Legal Affairs and Human Rights Report* (2006, Doc. 10957 Parliamentary Assembly of the Council of Europe, Strasbourg) 1–76.

Marty, D. 'Secret Detentions and Illegal Transfers of Detainees Involving Council of Europe Member States: Second Report' *Committee on Legal Affairs and Human Rights Explanatory Memorandum* (2007, AS/Jur 36 Parliamentary Assembly of the Council of Europe, Strasbourg) 1–72.

Mehlis, D. 'Report of the International Independent Commission Established Pursuant to Security Council Resolution 1595.' *United Nations International Independent Commission (UNIIIC) Reports* (2005, UNIIIC, Beirut) 7–61.

National Intelligence Council. 'Iraq's Weapons of Mass Destruction Programs.' *NIC Draft Report* (2002, National Intelligence Council, Washington, DC) 1–24.

Websites

Snowden, E. 'Edward Snowden: Here's how we take back the Internet.' *Ted Talk* 2014, available at http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet?language=en#t-2034380 (accessed on 25 August 2015).

Wilson, J. 'What I Didn't Find in Africa.' *The New York Times*, available at http://www.nytimes.com/2003/07/06/opinion/what-i-didn-t-find-in-africa.html?src=pm&pagewanted=1 (accessed on 25 November 2014).