STATE SECRETS LAW AND NATIONAL SECURITY

HITOSHI NASU*

Abstract With the increased awareness of national security concerns associated with unauthorized disclosure of State secrets, the legal protection of State secrets on national security grounds has assumed renewed significance, while raising ever growing concerns about its impact on freedom of information. Between these competing policy concerns lies a discrete area of law that defines and protects State secrets from unauthorized communication or disclosure. This article aims to ascertain the actual State practice concerning State secrets protection on national security grounds across different countries, and examines common challenges to the delimitation of national security grounds for State secrets protection in light of the changing national security environment.

Keywords: accountability, freedom of information, national security, public interest disclosure, State secrets.

I. INTRODUCTION

The legal protection of national security information has assumed renewed significance with the increased awareness of national security concerns associated with unauthorized disclosure of State secrets. Edward Snowden's unauthorized disclosure of United States (US) official secrets in June 2013 revealed US National Security Agency's international surveillance programmes. On 31 July 2013, Private Bradley Manning was convicted in the US court martial under the Espionage Act 1917 (US) for his involvement in the transmission of State secrets to WikiLeaks—the first successful conviction for mass digital disclosure of State secrets in history.[1] On 6 December 2013, the Japanese Diet adopted by the ruling party's majority the Special Secrecy Protection Act,[2] and on 17 April 2014, the Turkish Parliament enacted

* Senior Lecturer in Law, The Australian National University, Canberra, Australia. The author gratefully acknowledges Daniel Stewart and the anonymous reviewers for insightful comments on earlier drafts and Amanda Neilson and Helen Trezise for their research assistance.

[1] 'Bradley Manning Verdict: Cleared of "Aiding the Enemy" But Guilty of Other Charges', *The Guardian* (online) 31 July 2013 <http://www.theguardian.com/world/2013/jul/30/bradley-manning-wikileaks-judge-verdict>.

[2] Law No 108 of 2013. The enactment was part of the Second Abe Administration's national security agenda, 'protective pacifism': Editorial, 'NSC and Secrecy Bills Pose Dangers', *The*

[*ICLQ* vol 64, April 2015 pp 365–404] doi:10.1017/S0020589315000056

amendments to the National Intelligence Organization Law,[3] which marks the latest in the global move towards codification of State secrets protection.

On the other hand, over-classification of government information on ever expanding national security grounds has raised concerns about its impact on freedom of information, and the government's public accountability more generally. These concerns have motivated leading human rights experts and organizations around the world to set certain standards and principles to prevent actual or potential abuse of State secrets protection on national security grounds. Such attempts have resulted in the adoption of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information in 1997 and, most recently, the Global Principles on National Security and the Right to Information in 2013.[4] Non-governmental organizations (NGOs) with a special interest in freedom of information such as ARTICLE 19,[5] Freedom of Information Advocates Network,[6] and Open Society Foundations,[7] have also been advocating for greater openness in governments.

Between these two competing policy concerns lies a discrete area of law that defines and protects State secrets from unauthorized communication or disclosure, including disclosure in the public interest, or what is more widely known as 'whistle-blowing'. This protection is based on various policy grounds, most notably national security, and often entails a specific administrative and criminal sanctions regime. With the emergence of the modern 'national security state' and the rapidly increasing sophistication of intelligence gathering methods it is critical to understand the extent to which the amorphous notion of national security, particularly with its intrusion into many different aspects of our society,

Japan Times (online) 8 November 2013 <http://www.japantimes.co.jp/opinion/2013/11/08/editorials/nsc-and-secrecy-bills-pose-dangers/>.

[3] Law No 6532 of 2014.

[4] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, adopted on 1 October 1995, Johannesburg, South Africa <http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf> (hereinafter Johannesburg Principles); The Global Principles on National Security and the Right to Information, adopted on 12 June 2013, Tshwane, South Africa <http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf> (hereinafter Tshwane Principles). Even though the Principles have subsequently been referred to by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and by numerous scholars and NGOs, they are to be seen as best practice standards to be promoted, rather than codification of the existing state practice: JM Ackerman and IE Sandoval-Ballesteros, 'The Global Explosion of Freedom of Information Laws' (2006) 58 AdminLRev 85, 103; S Coliver, 'Commentary on the Johannesburg Principles' in S Coliver *et al*. (eds), *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information* (Martinus Nijhoff 1999) 11, 14.

[5] See its website at <http://www.article19.org>.

[6] See its website at <http://www.foiadvocates.net/>. See also, Freedom of Information Advocates Network, 'Global Right to Information Update: An Analysis by Region', July 2013 <http://www.access-info.org/documents/Access_Docs/FOIAnet/global_right_to_information_update_28-8-2013.pdf>.

[7] See its website on freedom of information at <http://www.opensocietyfoundations.org/topics/freedom-information>.

controls the legal regime regarding public access to government information. Does the existing legal regime effectively delimit the scope and extent of State secrets protection on ever expanding national security grounds? Or is the role of freedom of information in the current and future society eviscerated whenever national security is invoked?

In considering these questions, this article examines the scope and extent of State secrets laws with a specific focus on national security secrecy, in light of the changing national security environment.[8] It does not intend to discuss best practice in protecting the right to access information, nor does it provide an in-depth socio-legal analysis comparing relevant jurisprudence in different countries in light of their specific political or juridical contexts. Rather, this article aims to ascertain the actual State practice concerning State secrets protection on national security grounds across different countries,[9] with a view to examining common challenges to the delimitation of national security grounds for State secrets protection. One may presume that national approaches to disputes concerning freedom of information and national security in different political and judicial systems would vary reflecting the underlying legal philosophy and socio-legal context of each State that corresponds more or less with its political and legal structures. However, as this article shows, the impact of these differences in political and judicial systems is significantly diminished when it comes to the issue of national security for State secrets protection particularly in the changing national security environment. Draconian rules concerning State secrets protection on national security grounds do not fall solely within the purview of authoritarian regimes; liberal democracies such as Australia, Canada, Japan, the United Kingdom (UK) and the US also apply, and in some cases have even taken initiative in developing, such rules.

Section II of this article begins by providing a brief overview of different forms of State secrets law around the world. It demonstrates the existence of State secrets protection regardless of the State's political orientation, legal

[8] As this article focuses on the restrictions of public access to State secrets, it distinguishes and excludes the State secrets privilege as an evidentiary rule in court proceedings. Although some states distinguish 'official secrets' from 'State secrets' and 'documents' from 'information', the term 'State secrets' and 'information' is adopted for the purpose of this research to encompass any government-held information broadly.

[9] For an earlier comparative study with a more limited geographical scope, see, Amanda L Jacobsen, 'National Security and the Right to Information in Europe', Centre for Advanced Security Theory, University of Copenhagen, April 2003 <http://www.right2info.org/resources/pub lications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe>; C Pourgourides, 'Fair Trial Issues in Criminal Cases concerning Espionage or Divulging State Secrets', Report to the Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe Doc 11031 (2006) <http://assembly.coe.int/ASP/Doc/XrefDocDetails_ E.asp?FileID=9149>; Campbell Public Affairs Institute (ed), *National Security and Open Government: Striking the Right Balance* (Maxwell School of Syracuse University 2003).

system or socio-economic conditions, although these factors may well have a bearing upon the actual operation of the law. Section III then explains the socio-political backgrounds in which the concept of national security is expanding to encompass a significantly wide range of information for protection, as particularly observed in technologically advanced liberal democracies. The commonalities of the national security grounds for secrecy between State secrets laws in different jurisdictions are discussed in Section IV, which examines 108 countries where State secrets law exists in one form or another in terms of (1) classification of national security information, (2) disclosure thresholds, and (3) disclosure offences.[10] Section V turns the focus to liberal democracies, both established and newly emerged, to consider legal implications of the expanded notion of national security for the operation of State secrets law by examining how national security is balanced with the individual right of access to information and the more utilitarian quest for greater public accountability. The article concludes that with the growth of the modern 'national security state', existing legal criteria will become less and less effective in delimiting the national security grounds for State secrets protection, unless public interests are clearly expressed in legislation as overriding the national security interest.

II. AN OVERVIEW OF STATE SECRETS LAWS

There is probably no way to be certain about precisely when and where the practice of official secrets emerged in history because of the very nature of secrecy.[11] However, for a long time after the establishment of the Westphalian system government secrecy was a dominant practice. Indeed, secret treaties were used as a central instrument of balance-of-power diplomacy in the eighteenth and nineteenth centuries.[12] The need for legal protection of State secrets emerged in the nineteenth century as the media started to realize the commercial value of publishing State secrets for increasing the

[10] Including 99 countries where freedom of information law exists (see n 22) in addition to Brunei, Malaysia, Mongolia, Myanmar/Burma, Singapore, Sri Lanka, the Philippines, Turkmenistan and Vietnam where state secrets legislation exists without freedom of information law. In this section references are made to specific legislative provisions only where relevant provisions exist and in some cases only to representative examples, given that not all state secrets laws are equally well developed, are adequately translated into English, or provide a clear illustration of the point being made.

[11] It remains difficult even in the modern age because scholars are 'forced to rely upon a thin thread of evidence spun out in a bewildered array of mostly unverifiable writings and recollections by former officials (both disgruntled and not), defectors, journalists, parahistorians, and novelists': JL Gaddis, 'Intelligence, Espionage, and Cold War Origins' (1989) 13 Diplomatic History 191, 192.

[12] See generally, E Grosek, *Secret Treaties of History* (William S Hein & Co 2007); EJ Osmańczyk (A Mango, ed), *Encyclopedia of the United Nations and International Agreements*, vol 3 (3rd edn, Routledge 2003) 2092–3; M Toscano, *The History of Treaties and International Politics* (Johns Hopkins University Press 1966) 42.

sale of newspapers,[13] most notably with the UK responding by enacting the Official Secrets Act 1889 and 1911.[14] Other Commonwealth countries including Australia,[15] Canada,[16] and India,[17] soon followed suit, enacting specific laws dedicated to State secrets protection, modelled upon the Official Secrets Act 1911 (UK).[18] Many other former British colonial countries have also inherited State secrets law from colonial rule.[19]

Freedom of information law, on the other hand, developed much later in the twentieth century, though it is now widely recognized in universal human rights discourse as an essential component of the freedoms of opinion and expression. Access to government information provides an essential basis for individuals exercising their freedom of expression,[20] which is of particular significance in liberal democracies to make the government responsive and accountable through democratic processes.[21] In countries where freedom of information has been legislated, State secrets law is incorporated as an

[13] See D Hooper, *Official Secrets: The Use and Abuse of the Act* (Secker & Warburg 1987) 17–22.

[14] In France, by contrast, public disclosure of government information had tightly been controlled through censorship since the seventeenth century until the introduction of the 1881 *Press Law*: C Thogmartin, *The National Daily Press of France* (Summa Publications 1998) chs 1–2.

[15] Post and Telegraph Act 1901 (Cth) sections 9 and 127; Crimes Act 1914 (Cth) section 79. For details, see J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 9 Federal L Rev 49.

[16] Official Secrets Act 1890, 1939 and 1981 (Canada), replaced by Security of Information Act 2001 (Canada).

[17] Official Secrets Act 1923 (India).

[18] New Zealand enacted its Official Secrets Act much later in 1951, which was replaced by Official Information Act 1982 (NZ). In Hong Kong, the UK's successive Official Secrets Acts were applied until it was replaced by Official Secrets Ordinance (No 369 of 1997) (Hong Kong): J Chan, 'National Security and the Unauthorized and Damaging Disclosure of Protected Information' in F Hualing, CJ Petersen and SNM Young (eds), *National Security and Fundamental Freedoms: Hong Kong's Article 23 under Scrutiny* (Hong Kong University Press 2005) 251.

[19] For example, Official Secrets Act 1923 (as amended in Bangladesh); Official Secrets Act 1940 (Brunei); Official Secrets Act 1972 (Malaysia); Official Secrets Act 1923 (Myanmar/Burma); Official Secrets Act 1923 (Pakistan); Official Secrets Act 1935 (Singapore); Official Secrets Act 1955 (Sri Lanka); Official Secrets Act 1964 (Uganda); Official Secrets Act 1970 (Zimbabwe).

[20] See eg *Nurbek Taktakunov v Krygyzstan*, Human Rights Committee Communication No 1470/2006, UN Doc CCPR/C/101/D/1470/2006 (28 March 2011) para 7.4 (observing that freedom of information 'includes the two dimensions, individual and social, of the right to freedom of thought and expression that must be guaranteed simultaneously by the State'); *Stefaan Conrad Brümmer v Minister for Social Development and Others* [2009] ZACC 21 (Constitutional Court of South Africa) para 63 (Ngcobo J). For detailed analysis of different conceptions of freedom of information, see J Klaaren, 'The Human Rights to Information and Transparency' in A Bianchi and A Peters (eds), *Transparency in International Law* (CUP 2013) 223, 227–8; R Peled and Y Rabin, 'The Constitutional Right to Information' (2011) 42 ColumHumRtsLRev 357, 358–60.

[21] See eg *Társaság A Szabadágjogokért v Hungary* (2011) 53 EHRR 3, 136 para 27; *Lingens v Austria* (1986) 8 EHRR 407, 418 para 41; *Handyside v United Kingdom* (1979–80) 1 EHRR 737, 754 para 49. These two rationales for freedom of information are further discussed in Section V.

exception to freedom of information.[22] The judiciary, including regional human rights courts, is prepared to uphold this exception as long as information is withheld in accordance with applicable rules of domestic and international law (as discussed in Section V).[23] In countries where freedom of information is constitutionally guaranteed without specific legislation to implement it,[24] the scope of State secrets can be delineated through executive orders and court jurisprudence. In the Philippines, for example, the common law jurisprudence developed by courts was incorporated into the President's Executive Order issued in 2005.[25]

In parallel to the growth in number of freedom of information laws, the enactment of specialized State secrets legislation has regained precedence. In Asia, for example, the People's Republic of China (PRC) enacted the Law on Guarding State Secrets of the People's Republic of China in 1988, replacing the Provisional Regulations on Guarding State Secrets enacted in 1951, and revised the law in 2010.[26] In Vietnam, an Ordinance was promulgated with a view to State secrets protection in 2000, and the list of confidential information has regularly been updated since then.[27] Within the last two decades, Central Asian States have also enacted legislation for the specific purpose of State secrets protection.[28] In Europe, many Central and Eastern European States rushed to enact State secrets legislation prior to the North Atlantic Treaty Organization (NATO) meeting in Prague in November 2002.[29] In order to join

[22] According to Open Society Justice Initiative, there are 99 countries as of February 2014 that have enacted freedom of information legislation: Open Society Justice Initiative, 'List of Countries with Access to Information (AIT) Provisions in their National/Federal Laws or Actionable Decrees, and Dates of Adoption & Significant Amendments', available via <www.justiceinitiative.org>.

[23] See eg *Stoll v Switzerland* (2008) 47 EHRR 59, 1312 paras 125–129; *Leander v Sweden* (1987) 9 EHRR 433, 456 para 74; *R v Shayler* [2003] 1 AC 247; *Meredith Larson v Department of State*, 565 F 3d 857 (DC Cir, 2009); *CIA v Sims*, 471 US 159 (US Supreme Court, 1985).

[24] For example, The Constitution of the Philippines 1987, Section 7, art III.

[25] Executive Order No 464, 28 September 2005, cited in *Senate of the Philippines et al v Eduardo R Ermita and Others* [2006] PHSC 1216 (20 April 2006) (ruling that the Executive Order No 464 is invalid to the extent that it allows the executive branch to avoid congressional requests for information without assertion of the privilege or its reasons).

[26] Law on Guarding State Secrets of the People's Republic of China 1988 as revised in 2010, Order No 6 of the President of the People's Republic of China (hereinafter Law on Guarding State Secrets 1988).

[27] Ordinance on State Secrets Protection 2000 (Vietnam). See also Decree No 33/2002/ND-CP (28 March 2002).

[28] Law on Protection of State Secrets 1994 (Kyrgyzstan); Law on State Secrets 1995 (Mongolia); Law on State Secrets 2003 (Tajikistan); Law on Protection of State Secrets 1995 (Turkmenistan); Law on Protection of State Secrets 1993 (Uzbekistan).

[29] Law on Information Classified 'State Secrets' 1999 (Albania); Classified Information Protection Act 1998 (Bulgaria); Data Secrecy Law 2007 (Croatia); Protection of Classified Information Act 1998 (Czech Republic); State Secrets Act 1999 (Estonia); Act on State and Official Secrets 1995 (Hungary); Law on State Secrets 1996 (Georgia); Law on State Secrets 1997 (Latvia); Law on State Secrets and Official Secrets 1999 (Lithuania); Law on State Secrets 1994 (Moldova); Classified Information Protection Act 1999 (Poland); Law on

NATO, these States were required to ensure that sufficient safeguards and procedures were in place to guarantee the security of sensitive information, in accordance with NATO's security policy.[30]

The fact that a State secrets protection clause is found in freedom of information legislation does not necessarily prevent States from enacting specialized State secrets protection legislation, as is the case with Japan's recent enactment of the Special Secrecy Protection Act 2013.[31] Indonesia also enacted the State Intelligence Act in 2011,[32] in response to the 9/11 terrorist attacks in New York and the Bali Bombings on 12 October 2002.[33] Both types of State secrets law generally play dual functions: they restrict the right of the public to have access to certain official information; and impose obligations upon government officials not to make that information public. The difference between specialized State secrets legislation and freedom of information exemption clauses tends to lie in what each emphasizes—the former, the prohibition and criminalization of disclosure of State secrets, and the latter, the restriction on the right to access official information.

State secrets law thus exists in the majority of States regardless of the State's political orientation, legal system or socio-economic condition. Unlike other areas of law, there are significant commonalities, at least on the face of the text, between State secrets laws in different States, presumably because the law in many States has largely been transplanted, instead of being developed indigenously to meet the peculiar need of each society. One such commonality is the inclusion of national security as a ground for the legal protection of State secrets. This does not mean that all the States, whether liberal democracies or authoritarian regimes, apply the national security ground for State secrets protection in exactly the same manner. However, any differences that may be expected to appear, for example, due to the existence or absence of democratic control, are increasingly diminishing with the expansion of the notion of national security and the consequent ramifications for its legal restriction.

Protecting Classified Information 2002 (Romania); Law on the Protection of Classified Information 2004 (Slovakia); Classified Information Act 2001 (Slovenia); Law on State Secrets 1994 (Ukraine).

[30] A Roberts, 'NATO's Security of Information Policy and the Right to Information' in Campbell Public Affairs Institute (ed), *National Security and Open Government: Striking the Right Balance* (Maxwell School of Syracuse University 2003) 149, 150.

[31] cf Law concerning Access to Information held by Administrative Organs 1999 (Japan).

[32] Law No 17 of 2011. cf Public Information Disclosure Act 2008 (Indonesia).

[33] Earlier attempts to enact this legislation were aborted due to resistance from human rights activists, Muslim community, and internal agency rivalries: International Crisis Group, 'Indonesia: Debate over a New Intelligence Bill' (Asia Briefing No 124, 12 July 2011) 1 <http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/B124-indonesia-debate-over-a-new-intelligence-bill.aspx>.

III. THE PLACE OF NATIONAL SECURITY IN STATE SECRETS LAWS

Although State secrets laws generally cover various categories of information such as trade and business secrets, national security concerns have been fundamental to the emergence and development of this area of law. Indeed, when the Official Secrets Act (UK) was hastily put together and enacted without much debate twice in 1899 and 1911, it was presented as an urgent national security issue, even though the true motivation lay elsewhere—to engineer a smooth passage through Parliament.[34] As Jonathan Aitken observed, 'it is doubtful whether the legislators who passed the three Official Secrets Acts intended in practice to sanction a law with the scope and severity it encompasses today'.[35] A century later, the legal protection of State secrets on national security grounds is widely adopted and encompasses a significant scope and severity, for the following five reasons.

First of all, what the term 'national security' covers has significantly changed and expanded. Central to the notion of national security was traditionally the protection of sovereign territory ('defence of the realm'), and in particular military intelligence, from foreign interference such as armed invasion, espionage and sabotage.[36] This essence of national security is still reflected in its statutory definition in different jurisdictions.[37] Principle 2 of the Johannesburg Principles also adopts this traditional definition of national security, describing it as the protection of 'a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force'.[38] However, in the modern-day context national security also encompasses counterterrorism and immigration. In the UK Court of Appeal decision in *Secretary of State for the Home Department v Rehman*, Lord

[34] C Moran, *Classified: Secrecy and the State in Modern Britain* (CUP 2013) 24–5, 36 (explaining that although most historians understood that the decision was a response to the exigencies of national security at that time, framed on the belief that Britain would soon be at war with Germany, it was in fact designed to deter the unprincipled behaviour of the free commercial press); K G Robertson, *Public Secrets: A Study in the Development of Government Secrecy* (Macmillan 1982) 58. Similarly in the US, see, JA Smith, *War and Press Freedom: The Problem of Prerogative Power* (OUP 1999).

[35] J Aitken, *Officially Secret* (Weidenfield and Nicholson 1971) 15. Aitkin himself was charged under section 2 of *Official Secrets Act* 1911 for passing on to the *Sunday Telegraph* a British diplomat's report about the UK Government's supply of arms to Nigeria during the Nigerian Civil War: *R v Cairns, Aitken and Roberts* (unreported), summarized in 'No Duty in Law for Editor to Run to Whitehall, Secrets Case Judge Says', *The Times*, 4 February 1971, 2

[36] Hooper (n 13) 17–44; M Supperstone, *Brownlie's Law of Public Order and National Security* (2nd edn, Butterworths 1981) 246–55; D Williams, *Not in the Public Interest: The Problem of Security in Democracy* (Hutchinson 1965) ch 1.

[37] For example, Security Service Act 1989 (UK), section 1(2); Australian Security Intelligence Organisation Act 1979 (Cth), section 4 (the definition of 'security'). See also *Church of Scientology v Woodward* (1982) 154 CLR 25, 76 (Brennan J observing that '[t]he secrecy of the work in an intelligence organisation which is to counter espionage, sabotage, etc is essential to national security').

[38] Johannesburg Principles (n 4), Principle 2 (which draws from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc E/CN.4/1985/4).

Woolf MR discusses the changing nature of national security and favours the view that national security is a 'protean concept',[39] observing that 'what may be regarded as affecting national security can vary according to the danger being considered'.[40] It is also possible that different States perceive threats to national security differently.

Second, national security concerns are arguably diversifying to reflect more contemporary, acute public concerns about various security threats posed by individuals or groups of individuals in a wide range of social contexts, including the economy, food, energy, resources, the environment and, most recently, cyberspace. Indeed, there are increased concerns that hostile activities in cyberspace may undermine national security, as evident in the 2010 revision of the Law on Guarding State Secrets, which reportedly reflects the PRC Government's policy to expand and tighten information control in the digital age.[41] The Critical Infrastructure Information Act 2002 of the US also articulates national security concerns broadly, to include 'actual, potential or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct … that violates Federal, State, or local law, … or threatens public health or safety'.[42]

Third, the transnational nature of terrorist threats, and the resulting need for greater international cooperation in intelligence gathering and sharing, means that the security of one State cannot be separated from the security of others. In other words, national security issues arise not only from a direct threat to the nation, but even from activities directed against foreign governments.[43] Lord Slynn of the UK House of Lords supported this view in *Rehman*, stating that:

> It seems to me that, in contemporary world conditions, action against a foreign state may be capable indirectly of affecting the security of the United Kingdom. The means open to terrorists both in attacking another state and in attacking international or global activity by the community of nations, whatever the objectives of the terrorist, may well be capable of reflecting on the safety and well-being of the United Kingdom or its citizens.[44]

[39] *Secretary of State for the Home Department v Rehman* [2000] 3 All ER 778, para 35 (adopting the government's submission on this point).

[40] ibid, para 39.

[41] Human Rights in China, 'China Sharpens Legal Weapon for Information Control' (29 April 2010) <http://www.hrichina.org/content/394>.

[42] PL 107–296, 116 Stat 2135, section 212(3)(A). Idris J of the Federal High Court of Nigeria adopted this description of national security information in *Boniface Okezie v Attorney-General*, Federal High Court of Nigeria, 22 February 2013 (Application No FHC/L/CS/514/2012).

[43] In the UK, for example, terrorism is broadly defined as 'the use or threat of action where… (b) the use or threat is designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public': Terrorism Act 2000 (UK) section 1(1), as amended by Terrorism Act 2006 (UK) section 34.

[44] *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153, 182.

The international cooperation in intelligence sharing is practised on the basis of a 'control principle', whereby intelligence material provided by one country to another will never be disclosed, directly or indirectly, by the receiving State without permission of its provider.[45] The evolving digital practice across security institutions in different countries is also contributing to the rapidly expanded web of confidential information particularly when, as has increasingly been the practice in Western States, agencies can only secure access to such information on the condition that they operate on equivalent information security rules.[46] Indeed, the recent enactment of the Special Secrecy Protection Act 2013 in Japan specifically draws from the costly lesson of the January 2013 hostage crisis in Algeria. In this event, Japan's inability to secure reliable information without intelligence cooperation from their main allies affected their handling of the crisis.[47]

Fourth, with the increased sophistication of intelligence gathering methods and the diverse sources of security threats, national security information is no longer limited to that which is directly relevant to the defence of the nation, such as armament, military technologies and defence strategies.[48] The nature of information has rapidly changed in the globalized, digital age, providing a greater rationale for what is often described as the 'mosaic theory'—the idea of fitting together a puzzle, drawing inferences from seemingly disparate pieces of information to form an assessment.[49] The US Court of Appeals in *United States v Marchetti* succinctly explained the relevance of mosaic theory to State secrets protection:

[45] The 'control principle', however, is not a principle of law, but merely a 'convenient description of the understanding on which intelligence is shared confidentially' between States: *Mohamed v Secretary of State for Foreign and Commonwealth Affairs* [2011] QB 218, 243 para 44. For the practice of intelligence sharing generally, see S Chesterman, *Shared Secrets: Intelligence and Collective Security* (Lowy Institute for International Policy 2006) 19–28.

[46] UK Secretary of State for Justice, 'Justice and Security: Green Paper', Cmnd 8194 (October 2011) 8 para 1.22; D Curtin, 'Digital Governance in the European Union: Freedom of Information Trumped by "Internal Security"' in Campbell Public Affairs Institute (ed), *National Security and Open Government: Striking the Right Balance* (Maxwell School of Syracuse University 2003) 101, 108.

[47] The government inquiry, established in the aftermath of the crisis, notes the difficulty to secure reliable information from the Algerian Government or through its own intelligence network: 'Zai Algeria Houjin ni taisuru Tero Jiken no Taiou ni kansuru Kenshou Iinkai Kenshou Houkokusho [Report by the Committee of Inquiry concerning Terrorist Attacks against Japanese Nationals in Algeria]' (28 February 2013) 4 <http://www.kantei.go.jp/jp/singi/alg_terotaiou/kensahoukokusho20130228.pdf>. Japanese Prime Minister Shinzo Abe explained at a press conference that he relied upon the information provided by British Prime Minister David Cameron in handling the hostage crisis in Algeria: the full text of the press conference in Japanese available at <http://synodos.jp/politics/6431>.

[48] See generally S Chesterman, *One Nation under Surveillance: A New Social Contract to Defend Freedom* (OUP 2011) ch 1.

[49] For 'mosaic theory', see CE Wells, 'CIA v Sims: Mosaic Theory and Government Attitude' (2006) 58 AdminLRev 845; DE Pozen, 'The Mosaic Theory, National Security, and the Freedom of Information Act' (2005) 115 YaleLJ 628. The 'mosaic theory', however, does not substitute the government's burden of proof required to justify detention of individuals: *Farbi Saeed Bin Mohammed v Obama*, 704 F Supp 2d 1, 7–8 (DDC, 2009).

> There is a practical reason for avoidance of judicial review of secrecy classification. The significance of one item of information may frequently depend upon knowledge of many other items of information. What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context. The courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve efficiently in the review of secrecy classification in that area.[50]

The 'mosaic theory' has also been recognized in the UK, with Lord Griffiths of the House of Lords observing in *Attorney-General v Guardian Newspapers Ltd (No 2)* that '[w]hat may appear to the writer to be trivial may in fact be the one missing piece in the jigsaw sought by some hostile intelligence agency'.[51] Likewise, Dowsett J of the Federal Court of Australia in *Plaintiff B60 of 2012 v Minister for Foreign Affairs and Trade* accepted the proposition that 'expert analysts are able to make much from a collection of relatively small scraps of apparently unconnected information'.[52] Thus conceived, national security is no longer a socially alienated matter that primarily concerns the intelligence community, but rather covers a wide range of information that may relate to a threat to public law and order.[53] This 'mosaic theory' therefore undermines the traditional exclusion from State secrets protection in instances where the information sought to be protected is already in the public domain.[54]

Fifth, the sophistication of intelligence gathering methods and technologies available, the speed of movement of persons and goods, and the speed of modern communication are all factors that need to be taken into account in deciding what may constitute a national security concern in the contemporary context.[55] There would be an increasing number of circumstances where a genuine national security concern exists about disclosing certain information

[50] *United States v Marchetti*, 466 F 2d 1309, 1318 (4th Cir 1972). The position has remained the same even after the US Congress amended its Freedom of Information Act in 1974, in the wake of the Watergate scandal, with the aim to allow courts to conduct direct, de novo review of classified records despite the government's assertion of national security. See Pozen (n 49) 636–45; M Fuchs, 'Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy' (2006) 58 AdminLRev 131, 156–68.

[51] [1990] 1 AC 109, 269.

[52] [2013] FCA 1303, para 31.

[53] See eg *Schering Chemicals Ltd v Falkman Ltd* [1982] QB 1, in which the information sought to be protected could have been gleaned by a diligent and painstaking search through scientific literature, but nonetheless the defendant was restrained from misusing the information.

[54] For example, one of the legal grounds for non-disclosure obligations in common law countries is the duty of confidence, which in principle does not extend to the protection of information which is available in the public domain: see *Woodward v Hutchins* [1977] 2 All ER 751, 754–755 (Lord Denning MR); *Seager v Copydex Ltd* [1967] 2 All ER 415, 417 (Lord Denning MR). See also 'Fair-Trial Issues in Criminal Cases Concerning Espionage or Divulging State Secrets', Parliamentary Assembly of the Council of Europe Res 1551 (2007) para 10.1.

[55] For details of the relationship between the information technology revolution and national security, see EO Goldman, 'Introduction: Security in the Information Technology Age' in EO Goldman (ed), *National Security in the Information Age* (Frank Cass 2005) 1–2; A Roberts, *Blacked Out: Government Secrecy in the Information Age* (CUP 2006) ch 2.

that might also indicate or prove politically controversial or legally unjustifiable activities of the government. This inseparability of information poses a fundamental challenge to the segregation practices that have been implemented in some countries such as the US and European States,[56] by allowing agencies to classify even 'reasonably segregable' information as potentially damaging to national security interests when combined with other information.[57] It may also potentially prevent a very large pool of government secrets from disclosure for the purpose of public accountability.[58] The same situation arises from the confidential nature of the intelligence gathering methods or technologies employed to collect particular information that, of itself, may not be a national security concern.[59]

These contemporary changes to the national security environment pose challenges to the conventional precept that the notion of national security 'need[s] to be applied with restraint and to be interpreted restrictively'.[60] State authorities are increasingly finding it necessary to prioritize policies that address contemporary security threats over other aspects of political, economic and social life; this has been described as the growth of the 'national security state'.[61] The national security ground for State secrets protection is not an exception to this global trend towards the modern 'national security state', but is already the prevailing State practice and has the potential for almost unlimited expansion.

IV. THE SCOPE AND EXTENT OF NATIONAL SECURITY CONSIDERATIONS IN STATE SECRETS LAWS

As outlined in Section II, State secrets law takes different legislative forms in different jurisdictions. However, there are certain commonalities between State

[56] See eg *Heidi Hautala v Council of the European Union* (Case C-353/99P) [2001] ECJ I-9594, para 29 (holding that 'a refusal to grant partial access would be manifestly disproportionate').

[57] Pozen (n 49) 669–70.

[58] In the US, Blanton observes that the introduction of the 'critical infrastructure information exemption' by the Homeland Security Act 2002 essentially gave companies that voluntarily share information with the government about the vulnerability of their infrastructure not only the guarantee of confidentiality, but also immunity from civil liability even if the information contained evidence of illegal conduct: TS Blanton, 'National Security and Open Government in the United States: Beyond the Balancing Test' in Campbell Public Affairs Institute (ed), *National Security and Open Government: Striking the Right Balance* (Maxwell School of Syracuse University 2003) 33, 60. See also S Chesterman, '"We Can't Spy … If We Can't Buy!": The Privatization of Intelligence and the Limits of Outsourcing "Inherently Governmental Functions"' (2008) 19 EJIL 1055, 1060.

[59] For example, *Plaintiff B60 of 2012* (n 52) paras 25–39.

[60] *Stoll v Switzerland* (n 23) 1299 para 54. See also Report of the Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc E/CN.4/1995/32 (14 December 1994) para 48 (stating that 'the right to freedom of expression and information can be restricted only in the most serious cases of a direct political or military threat to the entire nation').

[61] For discussion of different definitions of the 'national security state', see NM Ripsman and TV Paul, *Globalization and the National Security State* (OUP 2010) 10–11.

secrets laws, which form the basis for structuring the analysis in this section to examine their similarities and differences in terms of the scope and extent of State secrets protection on national security grounds. According to the author's survey of State secrets laws, there are three main aspects that are commonly found and derived from national security concerns: (1) the classification of State secrets; (2) the disclosure threshold; and (3) the disclosure offence.

A. Classification of State Secrets

The way in which State secrets law defines the scope of national security information for protection is generally divided into three different approaches, or a combination thereof: (1) the source-based protection; (2) the class-based protection; and (3) the prejudice-based protection.[62] In cases where any of these approaches are combined, a distinct classification method is usually formed (in particular, a combination of the first and second approaches). As is the case in Australia and the UK, each of these approaches can also be adopted separately to provide different classification methods within one legal system.[63] The US is unique in that the classification methods are set by the President's Executive Order and change according to the national security information policy of the government in power.[64]

The source-based protection means that information is classified as an official secret by a designated public authority.[65] According to this approach, the intention or the official decision of the person who has produced or assessed the information determines the legal status of that information. An extended version of this protection relies upon presumed intention, whereby information is entrusted to a person in confidence owing to his or her position in government.[66] In Australia, for example, information 'prescribed' as an official secret is broadly defined to include any information obtained by a Commonwealth officer or a person holding office under the Queen, when 'by reason of its nature or the circumstances under which it was entrusted to him or her or it was made or obtained by him or her or for any other reason,

[62] cf Pourgourides (n 9) paras 56–68.

[63] Australian Law Reform Commission, 'Secrecy Laws and Open Government in Australia' (Report 112, 2009) ch 3; J Wadham, 'National Security and Open Government in the United Kingdom' in Campbell Public Affairs Institute (ed), *National Security and Open Government: Striking the Right Balance* (Maxwell School of Syracuse University 2003) 75, 84.

[64] For an overview, see KR Kosar, *Classified Information Policy and Executive Order 13526* (Congressional Research Service 2010).

[65] For example, Data Secrecy Act 2007 (Croatia) arts 5, 11 and 13; Freedom of Information Law 1999 (Israel) section 14; Law on Transparency and Access to Public Information 2002 (Peru) art 15(a).

[66] For example, Official Secrets Act 1923 (Bangladesh) section 5(1); Official Secrets Act 1940 (Brunei) section 5; Official Secrets Act 1923 (Myanmar/Burma) section 5(1); Official Secrets Act 1935 (Singapore) section 5(1); Official Secrets Act 1964 (Uganda) section 4(1); Official Secrets Act 1989 (UK) section 1.

it is his or her duty to treat it as secret'.[67] Finland prohibits disclosure of any information 'obtained in the service of the authority, where covered by a duty of non-disclosure provided in an Act'.[68] Typically, these States regulate government information on the premise that any official document should be kept secret unless and until public access is requested and duly authorized, which tends to promote a culture of government secrecy.[69] Even under the source-based approach, however, the scope of State secrets may be limited to certain categories, such as national defence and foreign relations, whilst leaving designated authorities with discretionary powers.[70]

The class-based approach lists and categorizes information into different classes of State secrets in legislation.[71] Determinative is the type or nature of information, document and/or material, irrespective of the intention of the producer or the possessor. In some countries the class-based protection is combined with the source-based protection, presumably so that no gap is left between different categories of State secrets.[72] Conversely, in other countries, the classification of information can only be made in accordance with legislative requirements and procedures.[73]

[67] Crimes Act 1914 (Cth) section 79(1). With respect to other official information, government employees must not disclose information 'if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs': Public Service Regulations 1999 (Cth) section 2.1(3). For discussion of the constitutional validity of this regulation, see *R v Goreng Goreng* (2008) 220 FCR 21, 30 (Refshauge J).

[68] Act on Openness of Government Activities 1999 (Finland) section 23.

[69] For discussion, see D Vincent, *The Culture of Secrecy: Britain, 1832–1998* (OUP 1998) 9–12; CR Sunstein, 'Government Control of Information' (1986) 74 CLR 889, 912–20.

[70] For example, Law on Information Classified 'State Secrets' 1999 (Albania) arts 4 and 6; Special Secrecy Protection Act 2013 (Japan) art 3; Law on Protection of State Secrets 1994 (Kyrgyzstan) arts 5 and 14.

[71] For example, Decree on Access to Public Information 2003 (Argentina) art 16; Law relating to Classification and Authorisation of Security 1998 (Belgium) arts 3 and 26 (excluding application of the Law relating to Public Access to Administrative Documents 1994); Classified Information Protection Act 2002 (Bulgaria) art 25; Freedom of Information Law 2013 (Côte d'Ivoire) art 9; Organic Law on Transparency and Access to Information 2004 (Ecuador) art 17; State Secrets Act 1999 (Estonia) sections 5–7; Law on Free Access to Administrative Documents 1978 (France) art 6; Law on State Secrets 1996 (Georgia) art 7; Free Access to Information Law 2008 (Guatemala) art 23(1); Organic Law on the Right to Access to Public Information 2010 (Guinea) art 16; Public Information Disclosure Act 2008 (Indonesia) art 17; Law on Access to Public Documents 2010 (Kosovo) art 12(1) and Law on Classification of Information and Security Clearances 2010 (Kosovo) art 4(1); Law on Official Secrets 1996 (Latvia) section 4(2); Law on Access to Public Information 2007 (Nicaragua) art 15; Right to Information Act 2013 (Pakistan) section 8; Law on Transparency and Public Administration 2002 (Panama) art 14(1); Right of Access to Information Law 2012 (Yemen) art 24.

[72] For example, Official Secrets Act 1972 (Malaysia) section 2; Law on Guarding State Secrets 1988 (PRC) section 8; Law on State Secrets 1993 (Russia) arts 4–5 and 9; Law on Protection of State Secrets 1995 (Turkmenistan) art 7; Ordinance on State Secrets Protection 2000 (Vietnam) arts 1 and 5–6.

[73] For example, Law on State Secrets and Official Secrets 1999 (Lithuania) arts 4–5; Law on State Secrets 1994 (Moldova) arts 5 and 8; Law on State Secrets 1995 (Mongolia) arts 5–6 and 8; Act on the Protection of Classified Information 2004 (Slovakia) arts 1–2.

According to the prejudice-based approach, information is protected only where disclosure has prejudicial effects.[74] For example, in India, information is not to be disclosed only when it 'would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State' and 'would endanger the life or physical safety of any person … for law enforcement or security purposes'.[75] Toby Mendel observes that this harm test, thus expressed, sets a very high threshold by requiring that the harm 'would' in fact occur as a result of the disclosure of the information.[76] Liberia and Montenegro appear to be setting even higher thresholds, requiring that the disclosure 'significantly endanger' or cause 'substantial harm' to national security.[77] By contrast, lower and more ambiguous thresholds are adopted in other countries, where public access to information is exempted when disclosure 'is likely to',[78] 'could reasonably be expected to',[79] or 'may' (or 'could'),[80] prejudice national security or cause substantial harm.

[74] For example, Freedom of Information Act 2004 (Antigua and Barbuda) art 31; Freedom of Information Act 1994 (Belize) art 22(a); Access to Information Law 2011 (Brazil) art 23(I); Law on Access to Public Information 2008 (Chile) art 21(3); Law on Access to Public Information 2011 (El Salvador) art 19(b); Law on Transparency and Access to Public Information 2006 (Honduras) art 17; Access to Information Act 2002 (Jamaica) section 14; Law on Access to Public Information and Administrative Documents 2011 (Niger) art 13; Law on Free Access to Information of Public Importance 2003 (Serbia) art 9(3); Freedom of Information Act 2003 (St Vincent and Grenadines) section 26(1)(a); Law on the Right to Information 2003 (Turkey) art 16; Law on Access to Public Information 2008 (Uruguay) art 9(a).

[75] Right to Information Act 2005 (India) sections 8(1)(a) and (g).

[76] T Mendel, *Freedom of Information: A Comparative Legal Survey* (UNESCO 2008) 59.

[77] Freedom of Information Act 2010 (Liberia) section 4.2; Law on Free Access to Information 2011 (Montenegro) art 9.

[78] For example, Law on Access to Administrative Documents 2002 (Angola) art 5(1); Law on Freedom of the Mass Media and Access to Information 2008 (Ethiopia) art 23(1); Access to Information Law 2011 (Guyana) art 28; Law on Intelligence and Security Services 1977 (Italy) art 12; Official Information Act 1982 (New Zealand) section 6; Freedom of Information Act 2004 (Switzerland) art 7(c); Freedom of Information Act 1999 (Trinidad and Tobago) section 25; Access to Information Act 2005 (Uganda) section 32(1)(a). The New Zealand Court of Appeal interpreted 'would be likely to' as meaning no more than a distinct or significant possibility, given the seriousness of national security: *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385, 65.

[79] For example, Freedom of Information Act 1982 (Cth) section 33; Freedom of Access to Information Act 2001 (Bosnia) art 6(a); Freedom of Information (Amendment) Act 2003 (Ireland) section 24(1); Freedom of Information Act 2008 (Malta) art 29; Right to Information Act 2013 (Sierra Leone) art 15; Promotion of Access to Information Act 2000 (South Africa) section 41(1). In Australia, the term 'could reasonably be expected to' has been interpreted as requiring less than a balance of probabilities but more than a reasonable possibility that the harm will occur: see *Attorney-General's Department v Cockcroft* (1986) 10 FCR 180, 190.

[80] For example, Classified Information Protection Act 2002 (Bulgaria) art 25; Act on the Protection of Classified Information 2005 (Czech) sections 2–3; Federal Act Governing Access to Information Held by the Federal Government 2005 (Germany) section 3; Freedom of Information Law 1999 (Israel) section 9(1); Protection of State Secrets and Documents Provisional Law 1971 (Jordan) art 3; Federal Law on Transparency and Access to Government Public Information 2003 (Mexico) art 13(1); Government Information (Public Access) Act 1991 (Netherlands) section 10(1); Classified Information Protection Act 1999 (Poland) art 2(1); Law Relating to Access to Information 2013 (Rwanda) art 4(1); Classified Information Act 2001

The harm test adopted for the national security exemption in Thailand involves the even more ambiguous criteria, requiring that the disclosure will jeopardize national security, 'having regard to the performance of duties of the State agency under the law, public interests and the interests of the private individuals concerned'.[81]

The concept of national security is better articulated in the State secrets laws that adopt a class-based or prejudice-based approach in the sense that it identifies the specific types or nature of information or criteria for non-disclosure, as opposed to the source-based approach which allows the government to keep information secret on many undefined grounds. Principle 2 of the 2013 Tshwane Principles states that '[i]t is good practice for national security, where used to limit the right to information, to be defined precisely in a country's legal framework in a manner consistent with a democratic society'. However, the critical question is: what is considered a precise definition of national security, and what definition of national security is considered 'consistent with a democratic society'?

In examining the wording of national security employed in State secrets laws more closely, it is notable that national security is in many countries distinguished from, or broader than, national defence.[82] For example, the Official Secrets Act 1972 of Malaysia lists as one of the different categories of State secrets, 'documents concerning national security, defence and international relations'.[83] Likewise, the PRC's Law on Guarding State Secrets lists 'secrets concerning activities for safeguarding state security' separately from 'secrets in the building of national defence'.[84] The Law on Access to Public Information 2008 of Chile allows non-disclosure when, among other things, 'disclosure affects the security of the nation, particularly if it relates to the

(Slovenia) art 5; Decree on Access to Administrative Documents of Public Authorities, No 41 of 2011 (Tunisia) art 17; Law on Protection of State Secrets 1993 (Uzbekistan) art 3.

[81] Official Information Act 1997 (Thailand) section 15.

[82] For a similar finding, see Jacobsen (n 9) 7–8.

[83] Official Secrets Act 1972 (Malaysia) section 2. Similarly, Classified Information Protection Act 2002 (Bulgaria) art 25; Access to Public Administration Files Act 1985 (Denmark) art 13(1); Law on Access to Public Information 2011 (El Salvador) art 19(b); Law on Freedom of the Mass Media and Access to Information 2008 (Ethiopia) art 23(1); Freedom of Information Act 1997 as amended in 2003 (Ireland) section 24; Law on Access to Public Documents 2010 (Kosovo) art 12 (1); Freedom of Information Act 2010 (Liberia) section 4.2; Federal Law on Transparency and Access to Government Public Information 2003 (Mexico) art 13(1); Freedom of Information Act 2008 (Malta) art 29(1)(a); Law on Access to Public Information and Administrative Documents 2011 (Niger) art 13; Freedom of Information Act 2006 (Norway) section 21; Law on Free Access to Information of Public Importance 2003 (Serbia) art 9(3); Promotion of Access to Information Act 2000 (South Africa) section 41(1)(a); Law on Transparency, Public Access to Information and Good Governance 2013 (Spain) art 14(1); Law on the Right to Information 2003 (Turkey) art 16.

[84] Law on Guarding State Secrets 1988 (PRC) sections 8(2) and (6). It appears, however, that any of the different categories of official secrets can be seen to have the potential to cause different degrees of harm to state security according to section 9.

national defence *or the maintenance of public order or public safety*' (emphasis added).[85] In Bulgaria, national security broadly encompasses protection of sovereignty, fundamental freedoms and human rights, and the democratic functioning of the State.[86] Belgium, Germany, Liechtenstein, and Switzerland distinguish internal security of the nation from external security.[87] In *Chavez v Presidential Commission on Good Governance*, the Supreme Court of the Philippines recognized 'the common law holding that there is a governmental privilege against public disclosure with respect to State secrets regarding military, diplomatic and *other* national security matters' (emphasis added).[88] It should also be noted that in some countries national security is distinguished from national economic or financial security.[89] Although the term 'national security' in each statutory provision must be interpreted in accordance with the relevant statutory interpretation rules of each State, this observation suggests a general trend whereby the contemporary notion of national security is not limited to the security of a sovereign State from external threats.

This interpretation of national security, derived from the statutory provisions of many States, is markedly different and distinguished from the traditional meaning as protection of national independence and territorial integrity from external violence and interference.[90] The notion of national security thus conceptualized, if not defined, provides a pathway through which government can expand the scope of classified information, within the established legal framework, as the nature of security threats and security-related information changes. In other words, by utilizing the amorphous language of national security as distinguished from national defence, the legal framework on the protection of State secrets in many States is already capable of accommodating diverse security concerns. Nowadays it is exceptional for States to provide a detailed list of classified information with a certain degree of specificity and without using the nebulous language of national security.[91]

[85] Law on Access to Public Information 2008 (Chile) art 21(3). Similarly, Access to Information Law 2011 (Brazil) art 23; Law on Free Access to Administrative Documents 1978 (France) art 6.

[86] Classified Information Protection Act 2002 (Bulgaria) supplementary provisions, Item 13.

[87] Law relating to Classification and Authorisation of Security 1998 (Belgium) art 26; Federal Act Governing Access to Information Held by the Federal Government 2005 (Germany) section 3 (1); Data Protection Act 2002 (Liechtenstein) art 12(2); Federal Administrative Transparency Act 2004 (Switzerland) art 7(1)(c).

[88] *Chavez v Presidential Commission on Good Governance* [1998] PHSC 762. See also *Francisco I Chavez v Public Estates Authority and Amari Coastal Bay Development Corporation* (2002) 433 Phil 506, 534.

[89] For example, Official Information Act 1997 (Thailand), section 14(1); Public Information Disclosure Act 2008 (Indonesia) art 17; Right to Information Act 2005 (India) section 8(1)(a).

[90] As discussed above in Section III.

[91] For example, Law on State Secrets 1996 (Georgia) art 7(1); Law on State Secrets and Official Secrets 1999 (Lithuania) art 5; Law on State Secrets 1994 (Moldova) art 5.

B. Disclosure Threshold

State secrets law may set certain thresholds for disclosure, which often form an integral part of the classification method adopted or an exception to State secrets protection. Typically, disclosure thresholds involve a harm test and a public interest test and, as will be discussed in Section V, reflect a national interpretation of what is necessary to protect national security, and what is proportionate to the national security interest to be protected, in accordance with international and regional human rights obligations.

An element of harm is an integral part of the State secrets law under the prejudice-based approach. As discussed above in the context of the prejudice-based protection, there are different degrees of risk of harm associated with disclosure that States are prepared to accept; however, only a few States go so far as to restrict national security secrecy to situations where a real and identifiable risk of significant harm is posed to a legitimate national security interest, as proposed by the 2013 Tshwane Principles.[92] In the US, it was only under the Clinton Administration that a 'foreseeable harm' standard was adopted.[93] Where a source-based or a class-based protection is adopted, the basic position is that there is no harm or public interest disclosure threshold,[94] nor is there any need to prove actual damage for prosecution in the case of an unauthorized disclosure.[95] Nevertheless, the element of harm may well still be taken into account in determining the degree of punishment for the disclosure offence, as will be discussed below.

A public interest threshold has been adopted in some countries as a mandatory consideration, and takes two different forms: one as part of a balancing test, and the other as an absolute disclosure threshold. For example, the Freedom of Information Act 2010 of Liberia requires public authorities to justify protection by clearly demonstrating that 'the harm to be caused by the disclosure is greater than the public interest in having the information disclosed'.[96] The Law on Access to Information 2000 of Moldova also provides that 'no restriction may be imposed on the freedom of information, unless the information provider

[92] Tshwane Principles (n 4) Principle 3(b).

[93] KE Uhl, 'The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security' (2003) 53 AmULRev 261, 269–74. Under the Obama Administration information shall not be classified 'unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security': Executive Order 13526, 29 December 2009, section 1.4.

[94] cf *Minister of Energy, Water and Communication & Another v Malaysian Trade Union Congress and Others* [2011] MLJU 1382 (Mohd Hishamudin Yunus JCA dissenting judgment arguing that 'in order to qualify as an official secret under the OSA [Official Secrets Act], it must be proven that disclosure of the Audit Report is detrimental to national security or public interest').

[95] S Kenny, 'Secrecy Provisions: Policy and Practice' [2011] Federal Judicial Scholarship 10 <http://www.austlii.edu.au/au/journals/FedJSchol/2011/10.html>; J MacDonald and CH Jones (eds), *The Law of Freedom of Information* (OUP 2003) 391–3; J Griffith, 'The Official Secrets Act 1989' (1989) 16 J Law&Soc 273, 280.

[96] Freedom of Information Act 2010 (Liberia) section 4.8(c).

can successfully prove that such a restriction … is necessary in a democratic society for the protection of the rights and legitimate interests of the person or national security, and that the damage to those interests would be larger than the public interest for that kind of information'.[97] A similar balancing provision is found primarily in African countries including Ethiopia, Nigeria, Rwanda, Sierra Leone, South Africa, Tunisia, and Uganda,[98] but also in newly emerged European States such as Bosnia and Herzegovina, Croatia, the Former Yugoslav Republic of Macedonia, and Kosovo.[99]

Absolute public interest disclosure thresholds are generally adopted in Latin America, but are also found in a small number of States in Africa and Eastern Europe. They represent the overriding public interests unique to each State or region, such as human rights violations and crimes against humanity committed by public officials,[100] abuse of authority or negligence in the performance of official duties,[101] public health,[102] and environmental risks.[103] Notably, Armenia and Zimbabwe prohibit non-disclosure of official information if it involves any matter that threatens national security or public

[97] Law on Access to Information 2000 (Moldova) art 7(4).

[98] Law on Freedom of the Mass Media and Access to Information 2008 (Ethiopia) art 28; Freedom of Information Law 2011 (Nigeria) art 12(2); Law relating to Access to Information 2013 (Rwanda) art 6; Right to Information Law 2013 (Sierra Leone) art 12(2); Promotion of Access to Information Act 2000 (South Africa) section 46(b); Decree on Access to Administrative Documents of Public Authorities, No 41 of 2011 (Tunisia) art 18; Access to Information Act 2005 (Uganda) section 34.

[99] Freedom of Access to Information Act 2001 (Bosnia) art 9; Act on the Right of Access to Information 2013 (Croatia) art 16 (however, with respect to the information classified in accordance with the Data Secrecy Act 2007, only upon consent of the Office of the National Security Council); Law on Free Access to Information of Public Character 2006 (Former Yugoslav Republic of Macedonia) art 6(3); Law on Access to Public Documents 2010 (Kosovo) art 12(2). See also Law on Access to Public Information 2011 (Ukraine) art 6(2) (incorporating a public interest balancing test as part of the prejudice-based protection requirements).

[100] For example, Access to Information Law 2011 (Brazil) art 21; Law on Access to Public Information 2011 (El Salvador) art 19; Law on State Secrets 1996 (Georgia) art 8(1); Free Access to Information Law 2008 (Guatemala) art 24; Law on Official Secrets 1996 (Latvia) section 5(3); Federal Law on Transparency and Access to Government Public Information 2003 (Mexico) art 14; Law on State Secrets 1994 (Moldova) art 12(1)(a); Promotion of Access to Information Act 2000 (South Africa) section 46(a)(i); Decree on Access to Administrative Documents of Public Authorities, No 41 of 2011 (Tunisia) art 18; Law on Access to Public Information 2008 (Uruguay) art 12.

[101] For example, Law on Information Classified 'State Secret' 1999 (Albania) art 10; Law on State Secrets 1996 (Georgia) art 8(4)(c); Access to Information Law 2011 (Guyana) art 38(a); Law on State Secrets 1994 (Moldova) art 12(1)(d); Law on Free Access to Information 2011 (Montenegro) art 10; Freedom of Information Act 2003 (St Vincent and Grenadines) section 35 (a); Freedom of Information Act 1999 (Trinidad and Tobago) section 35(a).

[102] For example, Law on State Secrets 1996 (Georgia) art 8(4)(b); Access to Information Law 2011 (Guyana) art 38(c); Law on Official Secrets 1996 (Latvia) section 5(2); Law on State Secrets 1994 (Moldova) art 12(1)(b); Freedom of Information Act 2003 (St Vincent and Grenadines) section 35(c); Freedom of Information Act 1999 (Trinidad and Tobago) section 35(c); Access to Information and Protection of Privacy Act 2002 (Zimbabwe) art 28(1)(i).

[103] For example, Law on State Secrets 1996 (Georgia) art 8(4)(b); Law on State Secrets 1994 (Moldova) art 12(1)(b); Promotion of Access to Information Act 2000 (South Africa) section 46 (a)(ii); Access to Information and Protection of Privacy Act 2002 (Zimbabwe) art 28(1)(ii).

security, which suggests that their definition of national security is wider than what the government may consider to be threats to national security.[104]

Public interest tests are not so widely adopted in other parts of the world, including Asia, Europe, and the Middle East, and where they do exist, they may take a discretionary form. For example, the Right to Information Act 2005 of India qualifies State secrets protection by stating that 'a public authority *may* allow access to information, if public interest in disclosure outweighs the harm to the protected interests' (emphasis added).[105]

C. Disclosure Offence

The severity of disclosure offence varies across States where unauthorized disclosure is expressly criminalized, but can be grouped into four types. The first type is found, for example, in Australia, Bangladesh, Brunei, India, Ireland, Malaysia, Myanmar/Burma, Singapore, Sri Lanka, Uganda and Zimbabwe, where drawing from Section 2 of the Official Secrets Act 1911 (UK),[106] criminal penalties apply widely to anyone who: discloses official secrets to foreign countries; retains official secrets without authority; fails to take reasonable care of official secrets; or even has merely received official secrets unless it is proven to be contrary to his or her desire.[107] Similarly in the US, '[w]hoever knowingly and wilfully communicates, furnishes, transmits, or otherwise makes [classified information] available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States' is criminally liable.[108] In Albania, anyone who obtains information that constitutes a State secret is criminally liable for divulging, spreading or communicating it.[109] In Indonesia, criminal penalties apply to anyone who discloses or communicates State secrets, even if it does not

[104] Law on Freedom of Information 2003 (Armenia) art 8(3); Access to Information and Protection of Privacy Act 2002 (Zimbabwe) art 28(1)(iii)&(iv).

[105] Right to Information Act 2005 (India) section 8(2).

[106] For a detailed analysis in the context of Singapore, see A Kwong, 'A Duty to Communicate: The Public Interest Defence to Offences under Section 5 of the Official Secrets Act' (1999) 20 SingLRev 177–238; C W Cheong, 'Section 5 of the Official Secrets Act, Bridges and Beyond' (1998) SJLS 260–98. In the UK, the new Official Secrets Act 1989 replaced section 2 of the 1911 Act with a series of more specific offences, many of which incorporate a harm test.

[107] Crimes Act 1914 (Cth) section 79; Official Secrets Act 1923 (as amended in Bangladesh) section 5; Official Secrets Act 1940 (Brunei) section 5; Official Secrets Act 1923 (India) section 5; Official Secrets Act 1963 (Ireland) section 13 and Freedom of Information (Amendment) Act 2003 (Ireland) section 48; Official Secrets Act 1972 (Malaysia) section 8; Official Secrets Act 1923 (Myanmar/Burma) section 5; Official Secrets Act 1935 (Singapore) sections 5 and 17; Official Secrets Act 1955 (Sri Lanka) sections 7–9; Official Secrets Act 1964 (Uganda) section 4; Official Secrets Act 1970 (Zimbabwe) art 4.

[108] Espionage Act 1917 (US) 18 US Code section 798.

[109] Criminal Code 1995 (Albania) art 295. Similarly, Law on State Secrets and Official Secrets 1999 (Lithuania) art 15; Criminal Code 2005 (Slovakia) arts 319–320; Criminal Code 1937 (Switzerland) art 293.

cause any harm and even in the case of negligent disclosure.[110] The blanket criminalization of State secrets disclosure has been criticized for failing to distinguish different purposes of disclosure, such as espionage and public interest disclosure (whistle-blowing),[111] and also for their 'chilling-effect' on freedom of the press.[112] However, the fact that there is no explicit reference to a harm test or a public interest defence in the State secrets legislation does not necessarily mean that a defence is not available against criminal prosecution. Indeed, a defence could still well be argued through an interpretation of the relevant statutory provision (such as 'national interests' and 'without authority'), or on the basis of general exceptions under the criminal code of a relevant jurisdiction (such as necessity).[113] Furthermore, although perhaps uniquely, the Delhi High Court introduced a harm test by holding that for the supply of sensitive secret documents to constitute an offence under the Official Secrets Act or under the Penal Code, 'it has to be shown that the nature of the documents was such which imperiled the security of India'.[114]

The second type of disclosure offence is limited to unauthorized disclosure of information by a public official who is under an obligation not to disclose the information that he or she has received by virtue of his or her position, or during the performance of his or her duties.[115] This type of disclosure offence often forms part of the liability regime applicable to a breach of freedom of information law provisions more generally.[116] In Georgia, where the

[110] State Intelligence Act 2011 (Indonesia) arts 44 and 45.

[111] For example, I Leigh, 'Indonesian Draft Legislation on State Secrets' in P Fluri (ed), *The Indonesian Draft State Secrecy Law: Four International Perspectives* (Geneva Centre for the Democratic Control of Armed Forces 2010) 1, 2.

[112] For example, Human Rights Watch, 'Indonesia: Repeal New Intelligence Law' (26 October 2011) <http://www.hrw.org/news/2011/10/26/indonesia-repeal-new-intelligence-law>; D Banisar, 'Comments on Legal Regulations on Access to Information and State Secrets in Albania', Organization for Security and Co-operation in Europe, April 2006, available at <http://www.osce.org/fom/18934>.

[113] For example, A Bailin, 'The Last Cold War Statute' [2008] Crim LR 625, 627 (discussing the 'defence of necessity').

[114] *K K Sarin v Meenakshi Datta Ghosh and Another* [1978] ILR (Delhi) 178, para 17. Note that the decision was handed down long before the Right to Information Act 2005 (India) established a prejudice-based approach to State secrets protection.

[115] For example, Crimes Act 1914 (Cth) section 70; Criminal Code 1992 (Estonia) section 73; Criminal Code 1889 (Finland) ch 38 section 1 (as amended by Law No 578/1995) and ch 40 section 5 (as amended by Law No 604/2002); Organic Law on the Right of Access to Public Information 2010 (Guinea) arts 22–23; Law on Classification of Information and Security Clearances 2010 (Kosovo) art 50; Criminal Code 1998 (Kyrgyzstan) art 300; Law on Official Secrets 1996 (Latvia) section 15; Criminal Code 1996 (Russia) art 283; Criminal Code 1995 (Spain) art 199 (2); Official Secrets Act 1989 (UK) section 1.

[116] For example, Access to Information Law 2011 (Brazil) art 34; Organic Law on Transparency and Access to Public Information 2004 (Ecuador) art 18; Law on Access to Public Information 2011 (El Salvador) arts 76–77; Law on Free Access to Information of Public Character 2006 (Former Yugoslav Republic of Macedonia) art 40; Free Access to Information Law 2008 (Guatemala) art 67; Access to Information Law 2011 (Guyana) art 50; Freedom of Information Act 2010 (Liberia) section 7.1; Federal Law on Transparency and Access to Government Public Information 2003 (Mexico) art 63; Law on Free Access to Information 2011 (Montenegro) art 27; Law on Access to Public Information 2007 (Nicaragua) art 47; Decree on Access to

class-based protection is combined with the absolute public interest disclosure threshold, no liability can be considered until the validity of imposing secrecy on the particular information at issue is established.[117] There are also countries such as Turkey where the elements of the disclosure offence incorporate mental factors such as wilfulness, recklessness and negligence.[118]

In the third type of disclosure offence, the harm test is expressly incorporated into criminal offence clauses. Serbia limits disclosure offences only in relation to information 'whose disclosure would or could cause harm to the security, defence or political, military or economic interests of Serbia'.[119] In the Philippines, different degrees of penalty will apply 'if the revelation of such secrets or the delivery of such papers shall have caused serious damage to the public interest'.[120] In the PRC, persons who, in violation of the provisions of the Law on Guarding State Secrets, divulge State secrets intentionally or through negligence, will be investigated for criminal responsibility 'if the consequences are serious'.[121] Likewise, Vietnam's Ordinance on State Secrets Protection provides that '[t]hose who violate the provisions of this Ordinance… shall, *depending on the nature and seriousness of their violations*, be disciplined, administratively sanctioned or examined for penal liability' (emphasis added).[122] In reality, however, it is the State authorities themselves, whether authoritarian regimes or liberal democracies, that assess the damage to the public interest or consequences of disclosure and consider whether criminal prosecution is warranted, or proportionate to the seriousness of the damage or consequence as they see it.[123]

The fourth type of disclosure offence incorporates a public interest defence. Denmark, for example, protects a person from criminal prosecution for disclosing State secrets when there is an 'obvious public interest' in the disclosure.[124] In Thailand, the Official Information Act 1997 provides that officials are not to be held liable for good faith disclosure aimed at securing an overriding public interest, where the disclosure is reasonable.[125] In Niger, legal protection is

Administrative Documents of Public Authorities, No 41 of 2011 (Tunisia) art 20; Law on Access to Public Information 2008 (Uruguay) art 31.

[117] Law on State Secrets 1996 (Georgia) art 38(3).

[118] Law on Access to Information 2003 (Turkey) art 29.

[119] Criminal Code 2005 (Serbia) art 316.

[120] Revised Penal Code of the Philippines, Act No 3815 (the Philippines) art 229.

[121] Law on Guarding State Secrets 1988 (PRC) art 31 (punishable with imprisonment of not more than 7 years, criminal detention or deprivation of political rights: Criminal Law 1979 (PRC) art 186).

[122] Ordinance on State Secrets Protection 2000 (Vietnam) art 20.

[123] cf A Kiss, 'Permissible Limitation on Rights' in L Henkin (ed), *The International Bill of Rights* (Columbia University Press 1981) 290, 296–7 (arguing that '[r]estrictions on human rights can be imposed under this concept only if the interest of the whole nation is at stake. This excludes restrictions in the sole interest of a government, regime or power group').

[124] Criminal Code 1930 (Denmark) art 152.

[125] Official Information Act 1997 (Thailand) section 20.

provided for 'any person who discloses or reports actions that constitute wrongdoing, breach of legal obligation, judicial error or grievous acts of negligence in the management of public administration'.[126] Australia has recently adopted the Public Interest Disclosure Act 2013 (Cth), which is designed to protect from prosecution and any other liability individuals who disclose information involving suspected or probable illegal conduct, or other wrongdoing, in the public interest under defined circumstances.[127]

It is perhaps not surprising to see a public interest defence available in countries where a public interest disclosure threshold is adopted, or where the classification of State secrets is prejudice-based. Thus in Ethiopia, Niger, Nigeria, Rwanda, South Africa, Sierra Leone, Ukraine, and Uganda, those who have breached their non-disclosure obligations will be exonerated from liability if they acted in good faith, and if the information was disclosed in the public interest, such as a serious threat to the security of citizens and the environment.[128] In Canada and the UK, on the other hand, the public interest defence is not available when the disclosure concerns national security.[129] Serious concerns about making a public interest defence available are strongly rooted in many government circles. This is because individuals, typically with self-righteous motives, may make an independent and ill-informed assessment as to what is in the 'public interest', with the risk that the disclosure may cause serious damage to the wider community.[130] Indeed, the assumption behind the source-based and class-based protection of State secrets is that the public disclosure of national security information can never be in the public interest.[131]

Irrespective of the type of disclosure offence adopted, a wide discretion tends to be given to State authorities in deciding whether to prosecute someone who has divulged classified information under State secrets laws. In Commonwealth countries, for example, discretion is given to the Attorney-General or the Director of Public Prosecutions as an independent authority to assess the merits of the case for prosecution in light of the public or national interest, without political or other pressure. The question of injury to the nation, however, is

[126] Law on Access to Public Information and Administrative Documents 2011 (Niger) art 33. Similarly, Freedom of Information Act 2004 (Antigua and Barbuda) art 47(1).

[127] Public Interest Disclosure Act 2013 (Cth) sections 10, 26 and 29.

[128] Law on Freedom of the Mass Media and Access to Information 2008 (Ethiopia) art 39(2); Law on Access to Information 2000 (Moldova) art 7(5); Ordinance on Access to Public Information and Administrative Documents 2011 (Niger) art 33; Freedom of Information Law 2011 (Nigeria) section 28(2); Law relating to Access to Information 2013 (Rwanda) art 16; Protected Disclosures Act 2000 (South Africa) section 9; Right to Information Law 2013 (Sierra Leone) section 50; Law on Access to Public Information 2011 (Ukraine) art 11(1); Whistleblowers Protection Act 2010 (Uganda) section 2.

[129] Security of Information Act 1985 (Canada) sections 16–18 (offences in respect of safeguarded information to a foreign entity or to a terrorist group); Employment Rights Act 1996 (UK) section 193.

[130] Griffith (n 95) 282–3.

[131] I Cram, *Terror and the War on Dissent* (Springer 2009) 148; RM Thomas, 'The British Official Secrets Act 1911–1939 and the Ponting Case' [1986] CrimLR 491, 507.

generally considered 'essentially political, in the broadest sense of the term, not judicial'.[132] As the UK Franks Committee, which reviewed the operation of Official Secrets Act 1911 (UK), observed:

> these decisions are irremediably decisions of a political nature, in that they are concerned with questions of public policy although not partisan advantage. Control by the Attorney-General is a safeguard, which has the effect of reducing and not increasing the number of actual prosecutions.[133]

Nevertheless, political intervention into prosecutorial decisions on the initiation and extent of criminal prosecutions has not been an uncommon experience, even in liberal democracies—no matter how entrenched the constitutional safeguards against it might be.[134] Disclosure offences exist primarily to close the loopholes in more traditional criminal offences such as treason and espionage, or other types of sanctions such as dismissal, when a political interest intervenes and demands criminal prosecution.

V. IMPLICATIONS OF THE EXPANDED NATIONAL SECURITY DISCOURSE FOR STATE SECRETS LAW

In various areas of law including criminal law, criminal procedure, evidence, and administrative law, the notion of national security has been posing challenges to the traditional legal framework by providing a justification for departure from pre-existing norms.[135] By contrast, as discussed above, State secrets laws have already been established in many jurisdictions as a pre-existing norm, in which national security provides a widely accepted ground for exemption from public access to official information. Nevertheless, their potential for almost unlimited expansion challenges the competing norm of freedom of information as the legal means to restrict the scope of State secrets protection on national security grounds.[136] In liberal democracies, the latter norm provides an essential basis for utilitarian agendas of open government and public accountability. In *Dagg v Canada*, for example, La Forest J of the Supreme Court of Canada observed that '[t]he overarching purpose of access to information legislation is to facilitate democracy … rights to state held information are designed to

[132] UK Home Office, 'Departmental Committee on Section 2 of the Official Secrets Act 1911', Cmnd 5104 (September 1972) vol 1, para 145(d).

[133] ibid para 255.

[134] JLlJ Edwards, 'The Integrity of Criminal Prosecutions: Watergate Echoes beyond the Shores of the United States' in PR Glazebrook (ed), *Reshaping the Criminal Law* (Stevens & Sons, London, 1978) 364, 377–80.

[135] I Vladeck, 'Is "National Security Law" Inherently Paradoxical?' (2011) 1 National Security Law Brief 11, 13–14.

[136] See eg P Birkinshaw, 'Freedom of Information and Openness: Fundamental Human Rights?' (2006) 58 AdminLRev 177, 194–6; S Sedley, 'Information as Human Rights' in J Beatson and Y Cripps (eds), *Freedom of Expression and Freedom of Information: Essays in honour of Sir David Williams* (OUP 2000) 239; NS Marsh, 'Access to Government-Held Information: An Introduction' in NS Marsh (ed), *Public Access to Government-Held Information* (Stevens & Sons 1987) 1, 2–5; A Cox, *Freedom of Expression* (Harvard University Press 1981) 3.

improve the workings of government; to make it more effective, responsive and accountable'.[137] The remainder of this article examines how these two complementary rationales for concerns about the expanded scope of State secrets protection on national security grounds—individual rights of access to information and a more utilitarian quest for greater public accountability—intersect with the notion of national security.

A. Balancing National Security and Freedom of Information

The right to freedom of information purports to protect the ground upon which individuals can exercise their freedom of expression.[138] This is particularly so in relation to the adequacy of government decisions, and to a lesser extent, public officials' own freedom of expression.[139] However, State secrets protection is recognized as an exception to freedom of expression, including access to information. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) relevantly provides that:

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

   …

   (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.[140]

In Europe, the Convention for the Protection of Human Rights and Fundamental Freedoms similarly provides for freedom of information 'subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests

[137] (1997) 148 DLR (4th) 385, 403. See also *Brümmer v Minister for Social Development* (n 20) para 62; *Claude-Reyes et al v Chile*, Inter-American Court of Human Rights, 19 September 2006, Series C No 151, para 86; *Handyside v United Kingdom* (n 21) 754 para 49; *S P Gupta v Union of India* (1982) 2 SCR 365, 598 (Supreme Court of India).

[138] See text (n 20).

[139] cf *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119, 144–6 (discussing the common law duty of loyalty and fidelity to the Commonwealth); *Osborne v Canada* [1991] 2 SCR 69, 97–101 (Sopinka J), 108–109 (Stevenson J) (discussing the extent to which precepts of loyalty, neutrality and impartiality justify restrictions on public servants exercising freedom of expression). For discussion, see D Feldman, Civil Liberties and Human Rights in England and Wales (2nd edn, OUP 2002) 794–5.

[140] International Covenant on Civil and Political Rights, adopted 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 19.

of national security'.[141] The American Convention on Human Rights guarantees the right to freedom of thought and expression including freedom to seek, receive and impart information 'subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: … (b) the protection of national security, public order or public health or morals'.[142] In Asia, the 2012 ASEAN Human Rights Declaration confirms freedom of information as one of the human rights and fundamental freedoms of every person,[143] whilst proclaiming in a general clause that such rights and freedoms are 'subject only to such limitations as are determined by law… and to meet the just requirements of national security, public order, public health, public safety, public morality, as well as the general welfare of the peoples in a democratic society'.[144] Similarly, under the African Charter on Human and Peoples' Rights, the right to receive information under Article 9 is only subject to a general restriction clause, which simply states that 'the rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest'.[145]

Under the ICCPR, and at least some of the regional human rights treaties, there are two basic requirements for any restrictions on freedom of information to be compatible with human rights obligations. The first is the procedural requirement that restrictions must be provided for by law, which establishes the foundational legal requirement for the enactment of a specific State secrets law. Indeed, the fact that there was no legislation in Chile that regulated the issue of restrictions on access to official information was decisive in finding a breach of the freedom of information obligation by the Inter-American Court of Human Rights in *Claude-Reyes et al v Chile*.[146] In Europe, this requirement has been interpreted to imply qualitative requirements such as foreseeability and an absence of arbitrariness or abuse of power.[147]

[141] Convention for the Protection of Human Rights and Fundamental Freedoms, adopted 4 November 1950, 213 UNTS 222 (entered into force 3 September 1953) art 10(2).

[142] American Convention on Human Rights, adopted 22 November 1969, 1144 UNTS 143 (entered into force 18 July 1978) arts 13(1) and (2). See also Access to Public Information: Strengthening Democracy, OAS Res 2252 (6 June 2006); Inter-American Declaration of Principles on Freedom of Expression, adopted by the Inter-American Commission on Human Rights, 108th reg sess, 19 October 2000 <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26&lID=1>.

[143] ASEAN Human Rights Declaration, adopted 18 November 2012, Phnom Penh, para 23 <http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration>.

[144] ibid para 8.

[145] African Charter on Human and Peoples' Rights, adopted 27 June 1981, 1520 UNTS 217 (entered into force 21 October 1986) art 27.

[146] Inter-American Court of Human Rights, Judgment of 19 September 2006, Series C No 151, para 94. Chile subsequently enacted the Law on Access to Public Information in 2008.

[147] For example, *Youth Initiative for Human Rights v Serbia* (Appl No 48135/06) [2013] ECHR 584, paras 25–26; *Kenedi v Hungary* (Appl No 31475/05) [2009] ECHR 786, para 44; *Rekvényi v Hungary* (2000) 30 EHRR 519, 553–4, para 59; *Leander v Sweden* (n 23) 450 paras 50–51.

The second, more substantive requirement is that restrictions must be necessary for, among other reasons, the protection of national security. This requirement involves two different aspects: the scope of restrictions (ie, the definition of national security); and the extent of restrictions (ie, the disclosure threshold and the severity of punishment in the case of an unauthorized disclosure). The ICCPR's Human Rights Committee elaborated in its General Comment No 34 on the scope of the national security exception to Article 19 of the ICCPR, observing that '[i]t is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information'.[148] The European Court of Human Rights has interpreted the adjective 'necessary' as implying the existence of a 'pressing social need',[149] whilst leaving a certain margin of appreciation for States to assess whether such a 'need' exists and what measures should be adopted to deal with it.[150] National security, and security in general, is an evolving and context-dependent concept and, therefore, restricting national security grounds to a traditional, military-oriented notion of defence against external threats may not adequately reflect the 'pressing social need' of the contemporary society.

The idea that the extent of restrictions must also be necessary is expressed in the Human Rights Committee's General Comment No 34 as the general principle of proportionality, which reiterates the earlier statement made in General Comment No 27 that restrictive measures, most relevantly, 'must be proportionate to the interest to be protected'.[151] Principle 15 of the 1997 Johannesburg Principles interprets this requirement as follows:

> No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.[152]

[148] Human Rights Committee, General Comment No 34, UN Doc CCPR/C/GC/34 (12 September 2011) para 30. See also American Convention on Human Rights (n 142) art 13(3).

[149] For example, *Lingens v Austria* (n 21) 418 para 39; *Handyside v United Kingdom* (n 21) 753–754 para 48; *Sunday Times v United Kingdom* (1979–80) 2 EHRR 245, 275 para 59.

[150] For example, *Grinberg v Russia* [2006] 43 EHRR 45, 1001 para 27; *Steel and Morris v United Kingdom* (2005) 41 EHRR 22, 433 para 87; *Hertel v Switzerland* (1999) 28 EHRR 534, 570–571 para 46; *Jersild v Denmark* (1995) 19 EHRR 1, 15–6, para 31.

[151] Human Rights Committee (n 148) para 34. See also, *Leander v Sweden* (n 23) 452 para 58; *Lingens v Austria* (n 21) 418 para 40.

[152] A non-governmental organization dedicated to the promotion of the freedom of information, ARTICLE 19, has also proposed a similar interpretation of this requirement in a three-pronged test: (i) the information must be related to a legitimate aim listed in the law; (ii) disclosure must threaten to cause substantial harm to that aim; and (iii) the harm to the aim must be greater than the public interest in having the information. See ARTICLE 19, 'Limitations' <http://www.article19.org/pages/en/limitations.html>.

The UN Special Rapporteur goes even further by proposing that 'necessary' restrictions 'be no more restrictive than is required for the achievement of the desired purpose'.[153]

These human rights requirements for national security exemptions are to varying degrees reflected in national State secrets laws, primarily through the adoption of a harm test and/or a public interest test as part of information classification methods, disclosure thresholds, or disclosure offences as examined in Section IV. In countries where a harm test or a public interest test is incorporated into the classification of information, disclosure thresholds, or disclosure offence clauses, it may appear that their State secrets laws are more likely to be consistent with the necessity and proportionality requirements for national security exemptions than those without such tests. The difficulty lies, however, in assessing the harm and in balancing that harm with the public interest in the disclosure of State secrets involving, for example, government misconduct or even illegal activities.

One way of looking at this balance is that with the growth of national security concerns, the extent to which individuals can exercise their right to freedom of information is reduced, if not denied. As the European Court of Human Rights observed in *Leander v Sweden*, when the individual right concerns an individual interest such as loss of an employment opportunity due to a confidential adverse security assessment, the public interest in national security is considered to prevail over that individual's interest in access to information concerning why he or she has lost that employment opportunity.[154] Here, the balancing concerns the two opposing policy interests—the access to certain information and the protection of national security through non-disclosure of that information.[155] The right to freedom of information itself is by no means denied or compromised in exchange, for example, for other individuals' right to security, for the balancing forms part of the right itself through such requirements as necessity and proportionality.[156] As long as the public interest adversely affected by State secrets protection is limited to a reduction in each individual's freedom to an extent that is necessary and proportionate to the protection of national security interests, recourse to the right of access to information is unlikely to see any success in penetrating the fortress of national security secrecy.

On the other hand, an individual's interest affected by the loss of an employment opportunity appears to have been a significant concern to the European Court of Human Rights in *Guja v Moldova.* In this case, then-Head of the Press

[153] F La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Doc A/HRC/14/23 (20 April 2010) para 79(g). See also Tshwane Principles (n 4) Principle 3(b).

[154] *Leander v Sweden* (n 23) 452 para 59.

[155] R Dworkin, *A Matter of Principle* (Harvard University Press 1985) 387–9.

[156] For discussion, see especially, J Waldron, 'Security and Liberty: The Image of Balance' (2003) 11 Journal of Political Philosophy 191, 198.

Department of the Prosecutor General's Office, Iacob Guja, lost his position for divulging to the media a letter written by the Deputy Speaker of Parliament to the Prosecutor General reportedly in order to apply pressure not to prosecute the four police officers who had been accused of ill-treatment and unlawful detention of ten persons suspected of election-related offences.[157] The interest at stake here involved wider public significance because access to information concerned discovery of illegal conduct or wrongdoing in public administration. In the words of the Court, '[t]he interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence'.[158] Yet, the latter is also a legally codified expression of a public interest. Indeed, there remain strong concerns even in liberal democracies that allowing unauthorized disclosure of State secrets will discourage frank and informed discussion in executive decision-making, undermine confidence in and between members of secret services,[159] and aid enemy nations and other hostile actors in understanding weaknesses and vulnerabilities of national security emergency preparedness.[160] It is unclear how the two competing 'public interests' were weighed in this instance in favour of disclosing illegal government conduct or wrongdoing.[161] One may wonder whether the Court would have reached a different conclusion in the *Leander* scenario if the individual had claimed a greater public interest in revealing how individual security assessments had been used, particularly for future government employees, or in the *Guja* scenario if the competing public interest at stake concerned national security.[162]

Another issue with the decision in *Guja v Moldova* is the requirement that 'disclosure should be made in the first place to the person's superior or other competent authority or body', and '[i]t is only where this is clearly

[157] *Guja v Moldova* (2011) 53 EHRR 16, 551 para 72.

[158] *Guja v Moldova* (n 157) para 74. See also *Stoll v Switzerland* (n 23) 1284, 1309; *Fressoz and Roire v France* (2001) 31 EHRR 2, 59 para 52.

[159] In common law countries at least, government employees are under a lifelong equitable duty of confidence owed to the government: see eg *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL), 264 (Lord Keith), 265 (Lord Brightman), 271 (Lord Griffiths), 284 (Lord Goff); *Commonwealth of Australia v John Fairfax & Sons Ltd* (1980) 147 CLR 39, 50–51 (Mason J). See also Feldman (n 139) 881–4.

[160] See eg *Attorney-General v Blake* [2001] 1 AC 268 (House of Lords), 287 (Lord Nicholls). cf GB Lee, 'The President's Secrets' (2008) 76 GeoWashLRev 197, 213–42.

[161] The Court only held that 'the public interest in having information about undue pressure and wrongdoing within the Prosecutor's Office revealed is so important in a democratic society that it outweighed the interest in maintaining public confidence in the Prosecutor General's Office': *Guja v Moldova* (n 157) para 91. For a critical view on the judiciary's ability to weigh competing public interests, see L Henkin, 'The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers' (1971) 120 UPaLRev 271, 272–3 and 279.

[162] In *Bucur and Toma v Romania*, the European Court of Human Rights simply noted that the Romanian Government did not invoke the existence of a considerable prejudice to the national interest and similarly held that 'la Cour considère que l'intérêt général à la divulgation d'informations faisant état d'agissements illicites au sein du SRI [Serviciul Român de Informaţii] est si important dans une société démocratique qu'il l'emporte sur l'intérêt qu'il y a à maintenir la confiance du public dans cette institution': (Appl No 40238/02) [2013] ECHR 14, paras 114–115.

impracticable that the information could, as a last resort, be disclosed to the public'.[163] The UK House of Lords shared the same view with regard to the first point in *R v Shayler*, holding that the ban on disclosure of information was necessary and proportionate as long as an internal process to request permission for official authorization to make a disclosure, and an opportunity to seek judicial review in case of refusal of that request, was available.[164] The House of Lords, however, did not go as far as to pronounce or implicate the second point. The differences between the two decisions appear to lie not only in the adequacy of reporting procedures,[165] but also in the weight given to a public interest in disclosing government misconduct. Lord Hutton of the UK House of Lords dismissed the claim that the administrative safeguards 'were inadequate because they did not provide protection against dishonesty or negligence on the part of the supervising officials',[166] drawing on another European Court of Human Rights' decision, *Klass v Federal Republic of Germany*.[167] In this case, which concerned a human rights compliance issue of surveillance in the interests of national security, the Court acknowledged that 'the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system', and then observed:

> The court notes in particular that the G 10 [Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications 1968] contains various provisions designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law. In the absence of any evidence or indication that the actual practice followed is otherwise, the court must assume that, in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue.[168]

The same Court in *Guja v Moldova* appears to have considered that sending a letter with the possible effect to put pressure on the Prosecutor General's Office was a sufficient indication that public officials were not carrying out their duties in strict accordance with the law, emphasizing the significance of open discussion in a democratic society.[169] It is not clear where the line was drawn between the surveillance of letters and telephone conversations that could be presumed to be in strict accordance with the law, and sending a letter that

[163] *Guja v Moldova* (n 157) para 73. The same position was adopted in *Heinsch v Germany* (2014) 58 EHRR 31, 883 para 65.

[164] *Shayler* (n 23) 270–4 paras 27–34 (Lord Bingham), 288 para 85 (Lord Hope), 294–6 paras 99–107 (Lord Hutton).

[165] Compare *Guja v Moldova* (n 157) paras 80–84; with *Shayler* (n 23) 270–274 (Lord Bingham).

[166] *Shayler* (n 23) 295.

[167] (1979–80) 2 EHRR 214.

[168] ibid 236–7 para 59.

[169] *Guja v Moldova* (n 157) paras 85–88 and 90–91. The Court merely observed that 'it cannot be excluded that the effect of the note [a letter by the Deputy Speaker of Parliament] was to put pressure on the Prosecutor General's Office': ibid para 86.

could not be presumed to be in strict accordance with the law. Nor is it shown with any reasonable degree of clarity why the inadequacy of the administrative procedures can justify legal protection for the individual who discloses confidential information in breach of his or her duty of confidence, in the absence of a statutory or treaty provision to that effect.[170]

What this brief comparison of select European cases demonstrates is that recourse to the right of access to public information necessarily involves value judgements, which may well be quite arbitrary at times, in weighing competing interests to assess what is necessary and proportionate as an integral component of the right. This arbitrariness is further exacerbated by the ambiguity of the 'public interest'. For example, was it in the public interest to disclose classified intelligence information on the alleged weapons of mass destruction programme in Iraq prior to the 2003 invasion? This was the question posed to Danish courts as a result of an unauthorized disclosure of such information by a former intelligence officer, Frank Grevil. The Eastern High Court of Denmark did not consider that this unauthorized disclosure was made in 'an obvious public interest' because it did not reveal any illegal activity or wrongdoing.[171] However, the Copenhagen City Court ruled otherwise, simply on the grounds that there was a considerable public interest in knowing the basis for the political decision regarding Denmark's involvement in the military action in Iraq.[172]

Furthermore, the notion of national security in many States is understood to include the maintenance of public order and stability, and is often expressed in a manner that encompasses even a lower probability of risk.[173] The public interest in freedom of information may well be seen as obscure and diluted when compared to the public interest in the maintenance of public law and order. To the extent that national security, particularly internal national security concerning the maintenance of public law and order, is considered an overriding public interest, no other public interest may prevail over it to mandate the disclosure of State secrets. In *Almonte v Vasquez*, the Supreme Court of the Philippines explains the rationale of governmental privilege against disclosure as being, 'based upon public interest of such paramount importance as in and of

[170] The Law on Access to Information 2000 of Moldova provides in art 7(5) that '[n]o one can be punished … if releasing this information does not damage or cannot damage legitimate interests related to national security, or if the public interest for knowing the information is larger than the damage that can result from its dissemination'. However, this clause was not relied upon or discussed by the Court in *Guja v Moldova* (n 157).

[171] Eastern Division of the High Court of Denmark, 23 September 2005 <http://fe-ddis.dk/SiteCollectionDocuments/FE/Nyhedsarkiv/OSTRE_LANDSRET_PRESSEMEDDELELSE.pdf>. (Grevil was convicted of disclosing confidential information without authorization).

[172] Copenhagen City Court, 4 December 2006, unofficial English translation available at <http://www.psw.ugent.be/cms_global/uploads/publicaties/dv/CPH.Court.4.12.BerlingskeTidendeversie.doc> (acquitting the journalists involved).

[173] See Section IVA.

itself transcending the individual interests of a private citizen',[174] and as a consequence individuals cannot enforce their legal rights, including freedom of information. Viewed in this light, the extent to which the protection of certain State secrets is considered unnecessary or disproportionate by reference to an undefined and obscure public interest in disclosure will inevitably be diminished insofar as it must be balanced against a greater range of national security interests. Various contemporary factors facilitating the emergence of the modern 'national security state' will further contribute to national security discourse dominating and debilitating human rights discourse in many countries, through the legal protection of State secrets.

The idea that national security should, at least under certain circumstances, prevail over any other public interests is also reflected in the practice of certification by the authorized minister as conclusive evidence that the public interest in the non-disclosure of certain information on national security grounds outweighs the public interest in disclosing it. Conclusive certification is available in Belize, Ethiopia, Ireland, Jamaica, Malaysia, New Zealand, St Vincent and Grenadines, Trinidad and Tobago, and the UK.[175] Recently, the practice of conclusive certification has attracted debate because of its adoption and invocation in the context of counterterrorism.[176] Indeed, conclusive certification was adopted in Canada when the Canadian Parliament passed the Anti-Terrorism Act 2001, conferring upon the Attorney-General the power to issue confidentiality certificates which exclude national security-related information from the operation of the Access to Information Act 1982.[177]

A countervailing trend appears in countries where the public has made a conscious decision to insert an absolute public interest disclosure threshold or defence in legislation. Many Latin American countries fall within this category, with State secrets protection clauses recognizing overriding public interests such as human rights violations and crimes against humanity committed by public officials.[178] Such provisions arguably reflect the gravity and scale of the practice of disappearances and extrajudicial killings implemented by various regimes that were in power in many Latin American countries from the 1960s to the 1980s, sparking public anger and

[174] *Commissioner Jose T Almonte and Others v Conrado M Vasquez and Concerned Citizens*, Supreme Court of the Philippines, 23 May 1995 <http://www.lawphil.net/judjuris/juri1995/may1995/gr_95367_1995.html>.

[175] Freedom of Information Act 1994 (Belize) art 22(2); Proclamation on Freedom of the Mass Media and Access to Information 2008 (Ethiopia) art 35; Freedom of Information (Amendment) Act 2003 (Ireland) section 25(1)(a)(ii); Access to Information Act 2002 (Jamaica) section 23; Official Secrets Act 1972 (Malaysia) section 16A; Official Information Act 1982 (New Zealand) sections 6 and 7; Freedom of Information Act 2003 (St Vincent and Grenadines) section 10(2); Freedom of Information Act 1999 (Trinidad and Tobago) section 25(3); Freedom of Information Act 2001 (UK) section 24.

[176] See eg C Bell, The Freedom of Security: Governing Canada in the Age of Counter-Terrorism (University of British Columbia Press 2011) ch 2.

[177] Anti-Terrorism Act 2001 (Canada) sections 87, 103–4.

[178] See text (nn 100–103).

a struggle by family members and society in general to discover the fate of the victims.[179] Indeed, the Inter-American Court of Human Rights has held that in cases of human rights violations, national security cannot be relied upon to refuse access to information required for an investigation or court proceeding.[180] Relying on this regional jurisprudence and the emerging notion of the 'right to truth',[181] the UN Special Rapporteur has recently expressed his view that '[w]idespread secrecy justified on national security grounds is particularly problematic in the context of investigations of human rights violations because it may represent one of the main obstacles to the clarification of responsibilities and consequences of serious violations, ultimately becoming a barrier to the promotion of justice and reparation'.[182] Yet, as observed earlier in Section IVB, the idea that all human rights violations are public concerns that can always override national security interests is not universally accepted, and represents only a liberal interpretation of what is or is not considered necessary for the protection of national security. As long as human rights discourse on freedom of information allows for the balancing of interests, it is only through a legal expression of paramount societal values that each State can accept a definite limitation upon the public authorities in protecting its national security interests.

B. Balancing National Security and Government Accountability

Another fundamental issue arising from the operation of State secrets law concerns government accountability, in particular who is to make an assessment of what constitutes harm to national security, and whether there is a greater public interest nonetheless in the disclosure of the information. A broad incorporation of national security as an exception to freedom of information has been criticized for various reasons such as 'undermining the legitimacy of government actions, reducing accountability, hindering critical technological and scientific progress, interfering with the efficiency of the marketplace, and breeding paranoia'.[183] To the extent that national authorities themselves determine what is seriously damaging or jeopardizing the public interest, there is an inherent risk of abuse of State secrets law by suppressing political activists or deterring government

[179] See generally M Esparza, H R Huttenbach and D Feierstein (eds), *State Violence and Genocide in Latin America: The Cold War Years* (Routledge 2010); S Cardenas, *Human Rights in Latin America: A Politics of Terror and Hope* (University of Pennsylvania Press 2010).

[180] For example, *Gomes Lund and Others v Brazil*, Inter-American Court of Human Rights, 24 November 2010, Series C No 219, para 202; *Tiu Tojin v Guatemala*, Inter-American Court of Human Rights, 26 November 2008, Series C No 190, para 77; *Myrna Mack Chang v Guatemala*, Inter-American Court of Human Rights, 25 November 2003, Series C, No 101, para 180.

[181] For a discussion of the right to truth, see especially J Davis, *Seeking Human Rights Justice in Latin America: Truth, Extra-Territorial Courts, and the Process of Justice* (CUP 2014) ch 4.

[182] La Rue (n 153) para 57.

[183] Fuchs (n 50) 136–7. See also DE Pozen, 'Deep Secrecy' (2010) 62 StanLRev 257, 278–9.

officials from revealing government wrongdoing.[184] Also, serious public accountability concerns arise when the language of security from vaguely defined threats to national interests is used to distort security discourse and justify States' failure to implement their international legal obligations, particularly those which protect individuals and their human rights, as demonstrated by extrajudicial executions and forced disappearances.[185]

That 'national security' often serves as a cloak for illegitimate motives and demands for secrecy to conceal illegal conduct or wrongdoing is an enduring, fundamental problem associated with the development of the modern 'national security state'. This is one of the reasons why, as Arnold Wolfers observes, 'very high security aspirations tend to make a nation suspect of hiding more aggressive aims'.[186] Paul Chevigny goes further by pointing out that '[t]he problem with the "national security state" is that … it can lead to the repetition of irrational decisions'.[187] It has also been argued that with its broad discretion to control the dissemination of national security information, the executive may exercise its power to shape and distort public debate on foreign policy and national security matters.[188] The traditional view that information truly relating to national security is not a matter for public consumption does not remain unchallenged,[189] given that the notion of national security has started intruding on individuals' social lives through the expanded array of security threats and the changing nature of security-related information itself.

It is a generally accepted position that as Lord Simon of the UK House of Lords observed, 'courts of law must recognise their limitations for decision-making—that there are many matters on which the decision is more appropriately made by the collective wisdom of Parliament on the advice of an executive (itself collective in a system of cabinet government) briefed by officials who have investigated over a wide field of repercussions of the decision'.[190] The judiciary is generally considered ill-equipped to evaluate or 'second-guess' the national security significance of certain information.[191]

[184] For explanation of various barriers to effective accountability, see Chesterman (n 48) 78–82.

[185] Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, UN Doc A/67/275 (9 August 2012) para 110.

[186] A Wolfers, '"National Security" as an Ambiguous Symbol' (1952) 67 Political Science Quarterly 481, 488.

[187] PG Chevigny, 'Information, the Executive and the Politics of Information' in S Shetreet (ed), *Free Speech and National Security* (Martinus Nijhoff 1990) 130, 138.

[188] H Kitrosser, 'Secrecy and Separated Powers: Executive Privilege Revisited' (2007) 92 IowaLRev 489, 539–40; Anonymous, 'Keeping Secrets: Congress, the Courts, and National Security Information' (1990) 103 HarvLRev 906.

[189] cf SA Cohen, 'Freedom of Information and the Official Secrets Act' in JD McCamus (ed), *Freedom of Information: Canadian Perspectives* (Butterworths 1981) 152, 157.

[190] *D v National Society for the Prevention of Cruelty to Children* [1977] 1 All ER 589, 608–609.

[191] *Centre for International Environmental Law v Office of the US Trade Representative*, 718 F 3d 899 (DC Cir, 2013); *Meredith Larson v Department of State* (n 23) 865; *Leghaei v Director General of Security* (2007) 241 ALR 141, 147 (Brennan CJ); *A v Secretary of State for the Home Department* [2005] 2 AC 68 (House of Lords), 128 (Lord Nicholls).

This is because the assessment of national security concerns necessarily involves subjective judgement as to what is considered to be seriously damaging or jeopardizing the public interest.

At one end of the spectrum, the view can be adopted that '[t]hose who are responsible for the national security must be the sole judges of what the national security requires'.[192] This position makes perfect sense in source-based protection States such as Malaysia, where the majority view in the judiciary has been that '[i]f the originator or the owner of the document treats it and the information contained in it as an official secret and clearly marks it and keeps it as such, it is not open to anyone to regard it as otherwise'.[193] Similarly in the UK, Lord Diplock observed in *Council of Civil Service Unions v Minister for the Civil Service* that national security is the responsibility of the executive government and 'is par excellence a non-justiciable question'.[194] Bingham LJ of the UK Court of Appeal in *Attorney-General v Guardian Newspapers Ltd (No 2)*, however, commented that Lord Diplock's statement 'does not, I think, mean that even in this highly sensitive field the court will act on a mere assertion on behalf of the Government, but it does mean that where national security is in issue the court will readily acknowledge the obvious limitations on its own knowledge and expertise'.[195]

At the other end of the spectrum, courts may decide to intervene in assessing whether the disclosure 'is in fact' prejudicial to the State (therefore, the serious damage or consequence must be objectively proven), not whether it simply 'appears to be' prejudicial to the State.[196] This position is more likely to be taken in prejudice-based protection States, where it is possible for the judiciary to impose the burden on the government to prove that disclosure would prejudicially affect its national security.[197] As is the case in India, such a position may well become merely a 'rhetorical nod to the rule of law' in order to disguise judicial formalism and deference to the executive government's decision-making.[198] Nevertheless, the ICCPR's Human Rights Committee held that in the absence of any pertinent explanations, withholding information could not be deemed necessary for the protection of national security.[199] The Federal Constitutional Court of Germany, the Supreme Court of Israel, and the Constitutional Court of Guatemala have also adopted

[192] *The Zamora* [1916] 2 AC 77, 107 (Lord Parker).

[193] *Datuk Haji Dzulkifli bin Datuk Abdul Hamid v Public Prosecutor* [1981] 1 MLJ 112, 112 (Salleh Abbas FJ), cited with approval in *See Kok Kol @ See Liong Eng v Chong Kui Seng and Others* [2009] MLJU 1098, para 15; *Minister of Energy, Water and Communication & Anor v Malaysian Trade Union Congress & Others* [2013] 1 MLJ 61, 76–77 (Zaleha Zahari JCA).

[194] [1985] AC 374, 412.

[195] *Attorney-General v Guardian (No 2)* (n 159) 220.

[196] *Chandler v Director of Public Prosecution* [1964] AC 763, 811 (Lord Devlin).

[197] See text (nn 74–81).

[198] S Setty, 'Formalism and State Secrets' in D Cole, F Febbrini and A Vedaschi (eds), *Secrecy, National Security and the Vindication of Constitutional Law* (Edward Elgar 2013) 57, 69–70.

[199] *Nurbek Toktakunov v Krygyzstan* (n 20) para 7.7.

a similar position by requiring sufficient elaboration on the underlying reasons for sensitivity and the presentation of some proof.[200]

In Australia, the judiciary has indicated willingness to assess harm—albeit in a different legal context of information disclosure—where an interlocutory injunction is sought to restrain publication of information containing government secrets. In *Commonwealth of Australia v John Fairfax & Sons Ltd*, for example, Mason J of the High Court of Australia held:

> It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticise government action. Accordingly, the court will determine the government's claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected.[201]

The UK House of Lords in *Attorney-General v Guardian Newspapers (No 2)* cited this judgment with approval and held that the government must demonstrate that the public interest would suffer detriment if an injunction was not granted.[202] There is no denying that there are exceptional circumstances where national security concerns prompt courts to prevent publication or disclosure of information to protect an important public interest.[203] Yet, what is significant in these judgments is the indication that the courts will not simply accept the government's claim of confidentiality but require the government to establish harm to national security, and that the assessment of public interests is by no means an inherently non-justiciable issue.

The judicial position on the assessment of national security claims for State secrets protection will fall somewhere within this spectrum, influenced by many different factors such as the nature of the dispute (for example, whether it concerns a request for disclosure of State secrets or an interlocutory injunction to restrain publication of information containing State secrets), the extent and character of the material sought to be protected (for example, whether it concerns an ongoing operational activity or it is largely of historical significance), the judicial system (for example, to what extent the court is authorized to conduct judicial review), and the level of judicial activism or conservatism of individual judges.[204] However, with the growth of the

[200] BverfG, Case No 2 BvE 3/07, 17 June 2009, 124 BVerfGE 78, 134 (in relation to the constitutional right of Parliament to investigate and obtain information); *Ministry of Defense v Gisha Legal Center for Freedom of Movement*, Supreme Court of Israel, 19 December 2011, para 28; Advisory Opinion, Constitutional Court of Guatemala, 8 March 2005 (No 2819–2004).

[201] (1980) 147 CLR 39, 52; followed by majority in *Attorney-General (United Kingdom) v Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 45.

[202] [1990] 1 AC 109, 258 (Lord Keith), 267 (Lord Brightman), 270 (Lord Griffiths), 283 (Lord Goff).

[203] *Commonwealth v Fairfax* (n 159) 52; *Attorney-General v Jonathan Cape Ltd* [1976] 1 QB 752, 765 (Lord Widgery CJ).

[204] See *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services* [2008] ZACC 6, para 55 (Constitutional Court of South Africa).

modern 'national security state' and the technological advances in intelligence gathering and analysis for national security purposes, courts will find it increasingly difficult to challenge a government's claim to protect State secrets on the grounds of harm and public interest. This difficulty has already been compelling the judiciary into the realm of judicial deference—even in liberal democracies, particularly the US. This is evidenced by their acceptance of the 'mosaic theory', which has resulted in the evisceration of the judicial role in reviewing executive decisions as to what is necessary to protect national security,[205] whilst making national security claims increasingly speculative.[206]

Critics have argued that the judiciary should still perform a 'screening function' requiring the government to describe the specific basis for withholding information on each account,[207] not simply accepting speculative assertions. The European Court of Human Rights has indeed adopted an assertive position, stating that its supervisory jurisdiction is not limited to ascertaining whether the State exercised its discretion reasonably, carefully and in good faith, but it has capacity to review the decision that the government has taken pursuant to its margin of appreciation in the light of the case as a whole and to decide, moreover, whether 'they based their decisions on an acceptable assessment of the relevant facts'.[208] As discussed above in Section VA, however, the methodological rigour of the Court's assessment is challenged due to the ambiguity of 'public interest' and the inherent requirement of value judgement in assessing what is necessary and proportionate which, when combined with the expanded notion of national security, may well compel the Court to err on the side of caution against granting access to State secrets.

The same challenge will equally be posed to any form of independent public oversight mechanism. A public oversight mechanism by a parliamentary committee is often considered a major safeguard against the government's abuse of power,[209] and therefore has been promoted with the aim of ensuring transparency, efficiency and adequacy of State secrets decision-making.[210]

[205] For example, *Center for National Security Studies v US Department of Justice*, 331 F 3d 918, 932 (DC Cir, 2003); *North Jersey Media Group, Inc v Ashcroft*, 308 F 3d 198, 219 (3rd Cir, 2002).

[206] Pozen (n 49) 664–6.

[207] *Center for National Security Studies v US Department of Justice* (n 205) 951 (Tatel J dissenting); *Detroit Free Press v Ashcroft*, 303 F 3d 681, 708–709 (6th Cir, 2002). For discussion, see Pozen (n 49) 658–63; K Anderson, 'Is There Still a "Sound Legal Basis"?: The Freedom of Information Act in the Post-9/11 World' (2003) 64 OhioStLJ 1605, 1628–46.

[208] See eg *Stoll v Switzerland* (n 23) 1306–1307 para 101; *Guja v Moldova* (n 157) 550 para 69; *Grinberg v Russia* (n 150) 1001 para 27; *Steel and Morris v United Kingdom* (n 150) 433–434 para 87; *Hertel v Switzerland* (n 150) 570–571 para 46; cf *Jersild v Denmark* (n 150) 14 para 30 (although this case is cited as the first authority for this position, there is no mention of 'an acceptable assessment of the relevant facts' in this judgment).

[209] *Leander v Sweden* (n 23) 454–455 para 65.

[210] JNL Morrison, 'Political Supervision of Intelligence Services in the United Kingdom' in S Tsang (ed), *Intelligence and Human Rights in the Era of Global Terrorism* (Stanford University Press 2008) 41, 49–51; H Kitrosser, 'Congressional Oversight of National Security Activities:

Indeed, in one of the public inquiries initiated in the UK into the 'intelligence failure' in respect of the alleged weapons of mass destruction programmes in Iraq in the period leading up to a military action by the 'Coalition of the Willing' in 2003, the House of Commons Foreign Affairs Committee expressed its frustration at the lack of cooperation from the government for access to classified information as 'a failure of accountability to Parliament'. The Committee recommended that the Intelligence and Security Committee, which was a statutory body appointed by and directly answerable to the Prime Minister, be reconstituted as a parliamentary committee to enhance transparency and accountability of intelligence and security agencies.[211] As Nigel White observes, however, parliament is simply not independent or strong enough to scrutinize the actions of the executive in national security matters, given that most members of parliament, particularly if they are part of the majority that forms the government, would not be prepared to risk their position and challenge the government.[212]

An independent review of security assessment, for example, by former judicial officers or a panel comprising senior intelligence officers and judicial officers in their ex officio role, may well provide an alternative solution.[213] However, the inability of non-experts, and even intelligence experts, to precisely understand or assess the national security ramifications of disclosing certain information undermines the credibility of such mechanisms.[214] Moreover, even independent inquiries into the performance of intelligence agencies or any other government operations tend to steer away from thorny issues such as the adequacy of a decision to protect certain information as State secrets and its actual use in political decision-making. Thus, the independent inquiries in the UK, one led by Lord Hutton into the death of a former Ministry of Defence employee David Kelly,[215] and the other by Lord Butler into the performance of UK

Improving Information Funnels' (2008) 29 CardozoLRev 1049; HH Koh, *The National Security Constitution* (Yale University Press 1990) 163–4.

[211] House of Commons Foreign Affairs Committee, 'The Decision to Go to War in Iraq', Ninth Report of Session 2002–03, HC 813-I, vol 1 (3 July 2003) 49. The Intelligence and Security Committee itself subsequently published its own inquiry report with a narrow focus on the adequacy of intelligence material used: Intelligence and Security Committee, 'Iraq Weapons of Mass Destruction – Intelligence and Assessments' Cmnd 5972 (9 September 2003).

[212] ND White, *Democracy Goes to War: British Military Deployments under International Law* (OUP 2009) 280.

[213] For a brief discussion on the role and limitation of the Independent Reviewer of Adverse Security Assessments in the context of immigration status determination in Australia, see B Saul, 'Security and Fairness in Australian Public Law' in M Gloves (ed), *Modern Administrative Law in Australia: Concepts and Context* (CUP 2014) 93, 102.

[214] S Schulhofer, 'Oversight of National Security Secrecy in the United States' in D Cole, F Febbrini and A Vedaschi (eds), Secrecy, *National Security and the Vindication of Constitutional Law* (Edward Elgar 2013) 22, 27–8.

[215] Lord Hutton, 'Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly C.M.G.', HC 247 (28 January 2004).

intelligence regarding Iraqi weapons of mass destruction,[216] focused on the effectiveness of intelligence operation and institutional structure of intelligence agencies, though these led to the release of large amounts of classified material into the public domain.[217] Likewise, a similar commission of inquiry established in the US by Executive Order 13328 only addressed the causes of intelligence failure and the improvement of intelligence capabilities.[218] This is to a large extent due to the restriction on the terms of reference given to these independent inquiries, but the politicized nature of the process itself may well be another significant factor that deters independent reviewers from addressing the adequacy of national security assessment of classified material.

VI. CONCLUSION

As each nation transforms into a technologically complex information society, and consequently becomes increasingly vulnerable to many unidentifiable sources of hostile or disruptive activities, it will become more difficult to clearly separate genuine national security information from rogue national security information. The perceived need for stronger State secrets protection on national security grounds is increasingly shared by many States despite all the differences in their political orientation, legal system or socio-economic conditions. This is seen as a necessary evil in a rapidly developing digital age, notwithstanding efforts by human rights activists and organizations to promote best practice standards for national security exceptions to freedom of information, so as to clarify and restrict the extent to which the use of these exceptions can be justified. This article has shown that many State secrets laws that exist around the world, whether they are inherited from British colonial rule, or recently adopted as part of freedom of information law or as specialized legislation, are already well designed to accommodate contemporary national security concerns.

With the growth of the modern 'national security state', together with technological advances in intelligence gathering and analysis for national security purposes, traditional legal criteria such as a harm test and a public

[216] 'Review of Intelligence on Weapons of Mass Destruction', Report of a Committee of Privy Counsellors, HC 898 (14 July 2004) 93–117.

[217] For an analysis of these inquiry reports, see, RJ Aldrich, 'Whitehall and the Iraq War: The UK's Four Intelligence Inquiries' (2005) 16 Irish Studies in International Affairs 73. Another Committee of Privy Counsellors was established in 2009, led by Sir John Chilcot, with broad terms of reference which then-UK Prime Minister Gordon Brown described as 'unprecedented' and with access to all the information held by the government in relation to the military action in Iraq and its aftermath to the end of July 2009. As of February 2015, this Iraq Inquiry is still in progress and its impact upon the legal protection of State secrets on national security grounds remains to be seen. See its website at <http://www.iraqinquiry.org.uk>.

[218] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 'Report to the President of the United States' (31 March 2005) 157–196 <http://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf>.

interest test are becoming less effective in delimiting the scope of national security for State secrets protection. These changes also diminish the role that can be played by the judiciary or independent public oversight bodies, even in liberal democracies where an ideological commitment to the protection of individual liberties supposedly underpins the political and legal systems. The only exception will be those countries in which a public interest override is clearly guaranteed in legislation, without any need for balancing it with the significance of a national security interest. The absolute public interest override is thus considered a legal expression of paramount societal values that outweigh any other public interests, including national security. As Stewart J of the US Supreme Court observed, 'the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry—in an informed and critical public opinion which alone can here protect the values of democratic government'.[219] Recourse to such societal values as expressed by an informed citizenry can assist independent reviewers more effectively ensure that proper limits are placed upon State secrets protection on national security grounds.

[219] *New York Times Co v United States*, 403 US 713, 728 (1971).