Journal of Southeast Asian Human Rights, Vol. 9 Issue. 2 December 2025 pp. 304 – 338
doi: 10.19184/jseahr.v9i2.41171

Intelligence Surveillance, Counterterrorism, and the Right to Privacy in Indonesia and Canada

Amira Paripurna
Airlangga University, Indonesia
Email: amira@fh.unair.ac.id

Sébastien Lafrance
Tashkent State University of Law, Uzbekistan; Maqsut Narikbayev University, Kazakhstan; Ho Chi Minh City University of Law, Vietnam
Email: seblafrance1975@gmail.com

Masitoh Indriani
Airlangga University, Indonesia
Email: masitoh@fh.unair.ac.id

Abstract

This paper examines the regulation of intelligence surveillance technologies in Indonesia and Canada within the framework of counterterrorism law, focusing on how legal regimes seek to protect public security while safeguarding fundamental rights, particularly the right to privacy. Using a comparative legal approach, the article addresses three interrelated questions: how surveillance powers are regulated in each jurisdiction; what legal and institutional safeguards exist to supervise and constrain their use; and to what extent these regimes comply with international human rights standards governing communications surveillance and personal data collection. The study finds that although neither the Indonesian nor the Canadian Constitution explicitly enshrines the right to privacy, both legal systems incorporate privacy protection as an integral component of their counterterrorism frameworks. Significant differences nevertheless emerge in how security and rights are balanced. Indonesia's counterterrorism regime, primarily governed by its Anti-Terrorism Act, emphasizes preventive security and grants broad surveillance powers with limited statutory guidance on proportionality and excessiveness. Canada regulates surveillance mainly through its Criminal Code, embedding prior judicial authorization and post-facto review as mechanisms intended to align security measures with rights protection. When assessed against international human rights principles of legality, necessity, proportionality, and effective oversight, the article concludes that Canada's framework demonstrates a higher degree of formal compliance, while Indonesia's regime presents greater risks of disproportionate interference with privacy.

Keywords: *Surveillance technology, counter-terrorism, privacy rights, Indonesia, Canada*

I. INTRODUCTION

Counterterrorism policy inevitably operates at the intersection of security and fundamental rights. Measures designed to prevent terrorist violence are often justified by reference to the State's obligation to protect life and public order, yet those same measures may intrude upon individual freedoms, particularly the right to privacy. This inherent interdependence and tension between security and rights have become more pronounced as counterterrorism strategies increasingly rely on technology-driven surveillance. Surveillance is therefore not merely a technical tool, but a deeply normative practice that raises persistent questions about legality, proportionality, accountability, and democratic control.

The application of technology in surveillance techniques extends the ability of intelligence and law enforcement agencies to target terrorist activities on the Internet.[1] Technology-enabled intelligence surveillance has identified terrorist groups and intervened prior to an attack. For example, the arrest of Dian Yuli Novi in 2017—the first female suicide bomber of the Islamic State (IS) in Indonesia[2]--following the plot of suicide bombings at the Presidential Palace in Jakarta in 2016, demonstrated how intelligence gathered from multiple sources, including surveillance communications, community informants, and prison officials, was instrumental in the prevention of terrorism. In this context, intelligence played a significant role in counterterrorism efforts.

Despite being an important aspect of law enforcement and terrorism prevention, intelligence activities still face several challenges. For example, countering violent extremism through monitoring Internet activities may involve the surveillance and collection of information related to private citizens, which could interfere with the right to privacy of these individuals.[3] Intelligence surveillance focusing on the prevention and investigation of potential terrorist plots and conspiracies will often collect metadata as part of the efforts to identify terrorist networks.[4] Related public authorities usually rely on records generated by communications service providers to support their efforts in preventing, investigating, and prosecuting terrorism offences.

---

1 McGregor, "The Use of the Internet for Terrorist Purpose", (2012), online: *United Nations Office on Drugs and Crime Publication* <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>.

2 Charlie Campbell, "ISIS Unveiled: The Story Behind Indonesia's First Female Suicide Bomber", (3 March 2017), online: *TIME* <https://time.com/4689714/indonesia-isis-terrorism-jihad-extremism-dian-yulia-novi-fpi/>.

3 Giovanni Sartor & Andrea Loreggia, *The Impact of Pegasus on Fundamental Rights and Democratic Processes* (European Union, 2022), online: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

4 "E4J University Module Series: Counter-Terrorism", (2018), online: *United Nations Office on Drugs and Crime Publication* <https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/surveillance-and-interception.htm>.

The danger of the State's power to surveil first became a global concern in 2013 when a whistleblower from the United States National Security Agency (NSA) reported details of the international mass surveillance conducted by the governments of the United States, the United Kingdom, Australia, Canada, and New Zealand.[5] This surveillance includes acquiring customers' data from Google, recording and analysing telephone calls and text messages, as well as stealing encryption keys for mobile phone communications.[6] In response, the General Assembly of the United Nations created a resolution that called on all States to review their legislation, procedures, and practices governing communications surveillance, the collection of personal data, and the interception of personal communications.[7] In addition, the Human Rights Council adopted resolution[8] that required States to protect and comply with the right to privacy while countering terrorism in the context of digital communication.

Currently, at least seventy-five countries are actively using artificial intelligence technologies for surveillance purposes, including Indonesia and Canada,[9] which have both implemented facial recognition systems and smart policing.[10] Law enforcement authorities employ smart policing to develop strategies that prevent and respond to criminal acts by analysing data through algorithms.[11] Additionally, Indonesia has also utilised smart city platforms, which enable the government to enhance city management by leveraging data-gathering sensors from interconnected devices.[12]

Considering the risks associated with the use of intelligence technology, this paper aims to analyse and examine the application of intelligence surveillance technology as a counterterrorism measure in Indonesia and Canada. Both countries face terrorism threats[13] and struggle with this issue in a democratic context. Indonesia is the world's most

5 "Two Years After Snowden: Protecting Human Rights in an Age of Mass Surveillance", (2015), online: *Amnesty International* <amnesty.ch/de/themen/ueberwachung/edward-snowden/dok/2015/zwei-jahre-nach-den-snowden-enthuellungen-regierungen-halten-an-massenueberwachung-fest/two-years-after-snowden-protecting-human-rights-in-an-age-of-mass-surveillance-bericht-zur-massenueberwachung>.

6 *Ibid.*

7 *UN General Assembly Resolution A/RES/68/167, 2014.*

8 *UN Human Rights Council Resolutions 34/7, UN Doc A/HRC/34/7*, 2017.

9 Steven Feldstein, "The Global Expansion of AI Surveillance", (17 September 2019), online: *Carnegie Endowment for International Peace* <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847> at 25–27.

10 *Ibid.*

11 Feldstein, *supra* note 9 at 20.

12 *Ibid* at 17.

13 See e.g. in Indonesia: Indonesia Bombing: Worshippers Wounded in Makassar Church Attack", (28 March 2021), online: *BBC* <https://www.bbc.com/news/world-asia-56553790>; in Canada: Stewart Bell, "Suspect's alleged statements about ISIS led to terrorism charge over Toronto hammer attack: sources", (16 March 2020), online: <https://globalnews.ca/news/6661038/toronto-hammer-attack-by-isis-supporter/>.

populous Muslim-majority country, with a multicultural society.[14] The country's democratic transition followed more than three decades of authoritarian governance, and while democratic institutions have been consolidated since the Reformasi era, tensions remain between security-oriented State practices and rights-based constitutionalism. These tensions are especially visible in the regulation of intelligence surveillance and counterterrorism measures. On the other hand, Canada is a Western State with strong democratic traditions and a multicultural background.

In respect of the right to privacy, both countries have recognised this right in their constitutional law frameworks. Therefore, the comparison of counterterrorism legal frameworks that exist in both Indonesia and Canada will also consider their distinct backgrounds. A liberal democracy, like Canada for example, may seek, in certain circumstances, to restrict State actions in specific areas. This is because liberalism, as an element of liberal democracies, aims to protect against tyranny, which limits the State from interfering with the lives of society.[15] Meanwhile, an authoritarian government, which has been a significant part of Indonesia's history, rarely imposes domestic restrictions on government actions, meaning that the State has broad authority to regulate its citizens' lives. The comparison of these legal frameworks aims to provide a deeper understanding of their perspectives and compliance with international human rights standards, especially regarding the surveillance of communications, their interception, and the collection of personal data.

This paper addresses the regulation and oversight of intelligence surveillance in counterterrorism operations in Indonesia and Canada, with particular attention to its implications for the protection of the right to privacy. It is guided by three interconnected research questions. First, how do the legal frameworks in Indonesia and Canada regulate the use of intelligence surveillance technologies for counterterrorism purposes? Second, what legal and institutional safeguards exist in each country to monitor, constrain, and supervise law enforcement and intelligence authorities in order to prevent excessive or unlawful interference with the right to privacy? Third, to what extent do the surveillance regimes in both countries comply with international human rights standards governing communications surveillance, interception, and the collection of personal data. To address these questions, the paper adopts a comparative legal approach.

The paper first examines intelligence surveillance and counterterrorism in Indonesia. It begins by outlining Indonesia's legal framework on terrorism, then analyses the expansion and strengthening of intelligence surveillance mechanisms, and subsequently explores how counterterrorism policies intersect with human rights protection and democratic governance in the Indonesian context. It then turns to the

14 Imtiyaz Yusuf, ed, Multiculturalism in Asia - Peace and Harmony (Nakhorn Prathom: Mahidol University, 2018) at 130; Robert W Hefner, Civil Islam: Muslims and Democratization in Indonesia (Princeton: Princeton University Press, 2000) at 6; Herlambang P Wiratraman & Sébastien Lafrance, "Protecting Freedom of Expression in Multicultural Societies: Comparing Constitutionalism in Indonesia and Canada" (2021) 36:1 Yuridika.

15 Joan McGregor, "Liberalism and Democracy" (1988) 38:3 Philosophy East and West at 334.

Canadian experience, examining the country's counterterrorism legal framework, the regulation and practice of intelligence surveillance, and the role of constitutional principles and judicial oversight in safeguarding fundamental rights. Building on these analyses, the paper offers a comparative assessment that highlights key structural differences in oversight, accountability, and rights protection, while also identifying shared challenges faced by both countries in reconciling national security imperatives with the rule of law and international human rights obligations.

II. INTELLIGENCE SURVEILLANCE AND COUNTERTERRORISM IN INDONESIA

This section examines the development and regulation of intelligence surveillance within Indonesia's counterterrorism framework. Its primary purpose is to provide the national context necessary for understanding how surveillance powers have evolved in response to terrorism, how they are legally justified, and how they are constrained or insufficiently constrained by legal and institutional safeguards. By analysing Indonesia's experience, this section lays the groundwork for the comparative discussion in the subsequent section on Canada.

Following the terrorist attacks on the World Trade Centre on September 11, 2001, Indonesia became a battleground in the global war on terror.[16] The 2002 Bali bombings brought to light the existence of homegrown extremists within the country, leading to a united front against terrorism.[17] In response to these attacks and subsequent incidents by Islamist militants over the past 18 years, the Indonesian government has mainly implemented a criminal justice model in its counterterrorism measures.[18] Under this framework, terrorism is understood as a criminal offence, and the State has taken a reactive and coercive approach to counterterrorism. The Indonesian police's anti-terrorism unit has garnered praise for its success in combating terrorist attacks,[19] and the shifts from reactive to proactive intelligence-led policing is a crucial factor in this success.[20]

16 John Gershman, "Is southeast Asia the second front?", (1 October 2002), online: *Foreign Affairs* <https://www.foreignaffairs.com/articles/southeast-asia/2002-10-01/southeast-asia-second-front>; Andrew Tan, "Southeast Asia as the 'Second Front' in the War against Terrorism: Evaluating Threat and Responses" 15:2 Terrorism and Political Violence 2003 at 112.

17 Hannah Beech, "What Indonesia can teach the world about counterterrorism", (7 June 2010), online: *Time* <http://content.time.com/time/subscriber/article/0.33009.1992246.00.html>.

18 Kathrin Rucktäschel & Christoph Schuck, "Tracing Indonesia's Counterterrorism Measures Since the 2002 Bali Bombings", (4 September 2019), online: *The Diplomat* <https://thediplomat.com/2019/09/tracing-indonesias-counterterrorism-measures-since-the-2002-bali-bombings/>.

19 Adam Fenton & David Price, "Indonesia's New Legislation for Countering the Financing of Terrorism" (2014) 15:1 Australian Journal of Asian Law at 111.

20 Amira Paripurna, *The Use of Intelligence in Indonesian Counter-terrorism Policing* (PhD Dissertation, School of Law University of Washington, 2017) [unpublished] at 224–225.

There are several methods for gathering information through surveillance, including monitoring the Internet Protocol (IP) address of a computer used to send an email, tracking data from communication service providers, analysing bulk personal data such as a list of dialled phone numbers, and tracing a list of visited websites. These techniques typically rely on datasets containing information about a large number of people, which can be used to target a specific individual of interest. While surveillance has always been a critical aspect of law enforcement in counterterrorism,[21] it must be constrained to what is necessary to achieve a legitimate aim, such as the prevention or investigation of serious crimes, including terrorism.[22]

To address these issues, this paper first outlines Indonesia's legal framework on terrorism, focusing on the statutory basis for counterterrorism measures and the role of intelligence and law enforcement agencies. Then it analyses the strengthening of intelligence surveillance in Indonesia, including institutional developments, technological adoption, and the legal authorization of surveillance practices. Lastly it examines the relationship between counterterrorism, human rights, and democracy in Indonesia, assessing how surveillance practices are reconciled with constitutional principles, human rights obligations, and democratic governance.

1. Indonesia's Legal Framework on Terrorism

The 2002 Bali Bombings marked a significant turning point in the Indonesian government's fight against terrorism. In response to the attacks, the government passed Government Regulation in Lieu of Law (Perpu) No. 1/2002 on Antiterrorism and Perpu No.2/2002, which were later consolidated into Law No. 15/2003 (known as the AT Law 2003) and Law No. 16/2003. However, Law No. 16/2003 was later repealed in 2004 by the Constitutional Court due to its violation of the non-retroactive principle outlined in Article 28I of the 1945 Indonesian Constitution.[23] From a human-rights perspective, the Court affirmed that while terrorism may constitute an extraordinary crime, its exceptional character cannot justify retroactive criminalisation, as this would undermine legal certainty, foreseeability, and the rule of law, principles also reflected in Article 15 of the ICCPR. Normatively, although the decision constrained short-term prosecutorial flexibility in responding to a grave security threat, it represents a principled affirmation of constitutionalism and rights-based criminal justice, reinforcing the position that counterterrorism measures must be designed prospectively and remain consistent with fundamental human rights standards.

---

21 Barry Friedman, *Unwarranted: Policing Without Permission* (New York: Farrar, Straus and Giroux, 2017) at 9–10.

22 Ann Cavoukian, "Surveillance, Then and Now: Securing Privacy in Public Spaces" (2013) Information and Privacy Commissioner, online: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-surveillance.pdf> at 12.

23 *Judicial Review of Law Number 16 of 2003 Indonesian Constitutional Court Decision 013/PUU-I/2003*, Indonesian Constitutional Court at 70.

Prior to the enactment of the AT Law 2003, criminal offences that are now considered terrorism-related, such as premeditated murder or bodily injury, were prosecuted under existing laws like the Indonesian Criminal Code and the Emergency Law on the Possession of firearms and explosives.[24] However, these laws had inherent limitations in addressing the comprehensive nature of terrorism.[25] Thus, the Indonesian government recognised the need for a more comprehensive counterterrorism strategy that included repressive and preventive offenses, which could be achieved through the enactment of a special law specifically targeting terrorism.[26]

Several provisions of the AT Law 2003 were based on provisions found in Chapter XXIX of the Indonesian Criminal Code (hereinafter referred to as KUHP), which includes offences related to aviation safety and security.[27] However, the AT Law imposed harsher penalties compared to the existing penalties for aviation security offences under the KUHP.[28] Additionally, the AT Law did not introduce any new provisions to the Emergency Law on the Possession of Weapons and Explosives, which was enacted in 1951, but only increased the penalties for specific offences. As a special law, the AT Law 2003 introduced new provisions, including the criminalisation of terrorism financing and the implementation of criminal procedures that deviated from the existing KUHAP. These deviations were intended to create new mechanisms for the investigation and prosecution of terrorism offences.[29]

The Anti-Terrorism Law of 2003 marked a significant departure from ordinary criminal procedure by formally permitting the use of intelligence outputs within the law enforcement process. Intelligence reports were recognised as preliminary evidence at the pre-trial stage, reflecting the preventive orientation of counterterrorism operations. However, this incorporation of intelligence into criminal proceedings raised unresolved legal questions, particularly concerning the procedures by which intelligence is gathered and its status as admissible evidence at the trial stage under the Indonesian Criminal Procedure Code (KUHAP). Traditionally, intelligence reports function as internal security instruments designed to support prevention and early intervention, rather than as evidentiary material subjected to adversarial testing in court. In the counterterrorism context, however, intelligence reports may be relied upon at an early stage of the criminal

24 Topo Santoso, "Anti-Terrorism Legal Framework in Indonesia: Its Development and Challenges" (2013) 25:1 Mimbar Hukum at 93.

25 United Nations Office on Drugs and Crime, "Digest of Terrorist Cases", (2010), online: *United Nations Office on Drugs and Crime Publication* <https://www.unodc.org/documents/terrorism/Publications/Digest_of_Terrorist_Cases/English.pdf>

26 *Ibid.*

27 Simon Butt, "Anti-Terrorism Law and Criminal Process in Indonesia'" (2008) Islam and Modernity: Syari'ah, Terrorism and Governance in South-East Asia Background Papers, online: <https://law.unimelb.edu.au/__data/assets/pdf_file/0010/1546327/AntiTerrorismLawandProcessInIndonesia2.pdf> at 7–8.

28 *Ibid* at 6.

29 *Ibid.*

justice process, even prior to prosecution, blurring the boundary between preventive intelligence work and evidentiary standards in criminal adjudication.

It is important to note that the AT Law 2003 has been primarily used to combat Islamic extremist terrorism, specifically groups like Al-Qaeda, Jemaah Islamiyah, and Islamic State. For example, from 2003 until 2012, the law enforcement officers arrested 700 suspects of terrorism, and over 500 were imprisoned.[30] Court decisions indicate that all suspects were connected to either the militant Sunni Islamist Al-Qaeda group, the Southeast Asian militant Islamist organisation Jemaah Islamiyah, or the terrorist militant group Islamic State (hereinafter IS). After the Bali Bombings and the enactment of the AT Law 2003, the law enforcement agencies focusing on counterterrorism were able to reveal terrorist networks and their key figures. However, over time, the AT Law 2003 was deemed inadequate and failed to meet the needs of law enforcement in their efforts to proactively prevent terrorism. For example, this law did not regulate the mechanism for preventing incoming threats of foreign terrorism and or stopping the dissemination of radicalism and information about aiding terrorists on social media.[31] Consequently, the government sought to amend the law to give law enforcement officers broader authority to conduct pre-crime and counterterrorism activities.[32]

In 2018, the amendment to AT Law 2003 was approved by the legislature and became Anti-Terrorism Law No. 5 of 2018 (hereinafter referred to as AT Law 2018). The 2003 Anti-Terrorism Law did not provide a substantive definition of terrorism. Article 1(1) merely stated that a "terrorist crime" is any act that fulfils the elements of an offence under the Law, leaving the scope of the offence largely dependent on operational interpretation. This definitional ambiguity was subsequently addressed through legislative amendment. The AT Law 2018 articulates terrorism in explicit terms and incorporates motive as a constitutive element. Article 1(2) of the 2018 amendment defines terrorism as "an act which uses violence or threat of violence which causes a widespread atmosphere of terror or fear, which can cause mass victims, and/or creates damages or destruction to strategic vital object, environment, public facility, or international facility with a motive of ideology, politic, or security disturbance." This framework reflects an effort to strengthen legal certainty; however, it does not fully resolve the procedural tension between intelligence-led prevention and the requirements of criminal due process under KUHAP.

The AT Law 2018 has amended 10 articles, added 26 new provisions, and abolished 7 articles of the AT Law 2003. The AT Law 2018 contains several new provisions, including the criminalisation of 'preparatory acts of terrorism activity' (Article 10-15); it

30 Sri Lestari, "Ancaman Terorisme di Indonesia Masih Ada", (10 October 2012), online: *BBC News* <https://www.bbc.com/indonesia/laporan_khusus/2012/10/121010_lapsusterorism1>.

31 Fitriani et al, *The Current State of Terrorism in Indonesia: Vulnerable Groups, Networks, and Responses*, The CSIS Working Paper Series 2 (Jakarta: Centre for Strategic and International Studies, 2018) at 14.

32 Trias Palupi Kurnianingrum, "Arah Perubahan Undang-Undang Pemberantasan Tindak Pidana Terorisme" (2016) VIII:06 Info Singkat Hukum at 2.

extended the period of arrest (maximum of 14 days with an extension of 7 days) and detention (maximum of 120 days with possible extensions of 60 days, 20 days, and 60 days respectively) for suspects. It also expanded tapping and interception powers. It is worth noting that the AT Law 2018 empowers Indonesian law enforcement officers with additional capabilities and authority to implement preventive measures in countering terrorism. Besides granting extensive power to law enforcement, the AT Law 2018 focuses more on victims' rights (see Chapter concerning victims' rights (Article 35 A-B)). This law also provides special protection for victims of terrorism (Article 34). A new provision has also been adopted that requires law enforcement to comply with human rights standards, as well as another provision which penalises law enforcement officers who violate human rights standards during arrest and detention (Articles 25 and 28).

The Office of the United Nations High Commissioner for Human Rights (OHCHR) affirms that while states have a legitimate duty to prevent terrorism, counterterrorism measures must comply with non-derogable rights and fundamental due process principles, including legality, necessity, proportionality, judicial oversight, and effective remedies.[33] Surveillance, preventive criminalization, and prolonged detention pose heightened risks of abuse, particularly when exercised outside ordinary criminal procedure. Within the framework of the AT Law 2018, these developments raise serious concerns regarding arbitrary detention, the erosion of the presumption of innocence, and the emergence of potential "cycles of abuse." While the 2018 Anti-Terrorism Law formally incorporates human rights safeguards, the expansion of preventive powers risks remaining merely declaratory in the absence of stringent judicial control and effective independent oversight.

2. Strengthening Intelligence Surveillance in Indonesia

Terrorist threats and the rise of violent religious extremism in Indonesia are indeed worrying. Today, the government faces a host of urgent public policy issues, including cybercrime, national security concerns involving insurgencies and regional tensions, as well as omnipresent concerns about acts of terror. Unsurprisingly, the government is expected to develop or acquire various advanced surveillance capabilities.[34] The increasing proliferation of surveillance techniques currently considered by the government and law enforcement is far-reaching. The question emerges of whether the expansion of intelligence surveillance puts Indonesia's democratic society at risk, and whether this could result in a return authoritarian rule.

---

33 United Nations Office of the High Commissioner for Human Rights, Human Rights, Terrorism and Counter-Terrorism, Fact Sheet No. 32 (United Nations Office of the High Commissioner for Human Rights, 2008).

34 Matthew Carrieri et al, "Exploring Communications Surveillance in Indonesia", (25 October 2013), online: *The Citizen Lab* <https://citizenlab.ca/2013/10/igf-2013-exploring-communications-surveillance-indonesia/>.

Based on the AT Law 2018, mail intercepts and phone tapping are considered acceptable for methods for gathering intelligence. The AT Law permits investigators to use intelligence reports as evidence when conventional evidence is deemed insufficient (Article 26(2)), and allows investigators to intercept telephone conversations to obtain sensitive information (Article 31). The investigators have the authority to conduct communication surveillance of the terrorist suspect for a maximum of one year, and this period can be extended for one additional year (Article 31). In urgent circumstances, investigators are permitted to intercept the communication of a suspected terrorist without the permission of a district court chairperson (Article 31A). However, under the AT Law 2018 the term "urgent circumstances" is not elaborated. Further, Law No. 17 of 2011 on State Intelligence confers broad powers on authorities to intercept and surveil communications involving activities deemed to threaten national interests and national security, as stipulated in Articles 31, 32, and 34. The law also outlines punishments for persons found to have intentionally stolen, revealed, or leaked classified information (Articles 44 and 45).

Primary methods for gathering information against adversaries and terrorist organisations include electronic surveillance, covert investigations involving undercover agents and informants, and the creation of intelligence networks within the community.[35] Given recent developments, such as the increasing prevalence of "lone wolf" activities, the evolving nature of IS networks worldwide, and the growth of youth radicalism on college campuses,[36] the Indonesian police force has implemented new surveillance measures. These measures include the installation of surveillance cameras throughout the capital city[37] and the creation of a police cyber patrol that can provide early warnings regarding radicalism and terrorist activities on the internet.[38] Through cyber patrol, for

35 Amira Paripurna, "The Emergence of Proactive Intelligence Led Counterterrorism Policing and Surveillance in Post Suharto Indonesia" in Veronika Nagy & Klara Kerezsi, eds, *A Critical Approach to Police Science: New Perspective in Post Transitional Policing Studies* (Eleven, 2020) at 155; United Nations Office on Drugs and Crime, "Special Investigative Techniques and Intelligence Gathering", online: *United Nations Office on Drugs and Crime* <https://www.unodc.org/e4j/en/organized-crime/module-8/key-issues/special-investigative-techniques/intro.html>.

36 Kanupriya Kapoor, "Indonesia to Add Hundreds of Counterterrorism Police to Monitor IS", (29 December 2017), online: *Reuters* <https://uk.reuters.com/article/uk-indonesia-security/indonesia-to-add-hundreds-of-counter-terrorism-police-to-monitor-is-idUKKBN1EN0WO>.

37 Vela Andapita, "Smart City Relies on True 'Guardians': CCTV Cameras", (13 February 2019), online: *The Jakarta Post* <www.thejakartapost.com/news/2019/02/13/smart-city-relies-true-guardians-cctv-cameras.html>.

38 Heru Purwanto, "RI Police Initiates ASEAN Cyber Patrol", (19 September 2017), online: *Antara News* <https://en.antaranews.com/news/112698/ri-police-initiates-asean-cyber-patrol>; Akhdi Martin Pratama, "Polisi Giatkan 'Cyber Patrol' Hadapi Maraknya Berita 'Hoax'", (30 December 2016), online: *KOMPAS.com* <https://megapolitan.kompas.com/read/2016/12/30/16255681/polisi.giatkan.cyber.patrol.hadapi.maraknya.berita.hoax.>.

example, police may monitor private WhatsApp[39] and Telegram groups[40] if an investigation causes them to suspect the group or any of its members of terrorist activities.

Terrorists have increasingly turned to social media, encrypted communications, and the dark web to spread propaganda, recruit followers, and plan attacks, thereby shifting the fight against terrorism to cyberspace.[41] To address this, the Indonesian Ministry of Communications and Information, along with the Indonesian National Police, has launched the Cyber Drone 9 system to enhance their cyber patrol capabilities. This system utilises both artificial intelligence and human analysts to identify and verify negative content that has been detected automatically or reported by citizens or other agencies.[42] The system has detected over 22,000 instances of radical content on websites and social media platforms, which are reviewed by a team of 58 individuals operating 24 hours a day.[43]

Another new development in Indonesia regarding communication surveillance has been further included in Article 258 of the New Indonesian Penal Code, which classifies the act of illegal wiretapping as a crime that entails a maximum imprisonment of 10 years. This subsequently revokes Article 31 of Law No. 19 of 2016, which, contrary to Article 258 of the Indonesian Penal Code, does not clearly define what is classified as wiretapping. The latter, however, details the specific activities that constitute wiretapping, which encompass the act of listening, recording, diverting, altering, impeding, or noting the transmission of private electronic information or documents using a wireless network.[44]

---

39 Ariyani Yakti Widyastuti, "Halau Hoax, Polisi Gelar Patroli Siber Hingga ke Grup WhatsApp", (14 June 2019), online: *Tempo* <https://bisnis.tempo.co/read/1214686/halau-hoax-polisi-gelar-patroli-siber-hingga-ke-grup-whatsapp>.

40 "Telegram Blocks Terror Content After Indonesia Threatens Ban", (16 July 2017), online: *CNBC* <https://www.cnbc.com/2017/07/16/telegram-blocks-terror-content-after-indonesia-threatens-ban.html>.

41 Kapoor, *supra* note 36 at 36.

42 Chandni Vatvani, "In Indonesia, Extremists Finding Low-Tech Ways to Get Around High-Tech Blocks: Think Tank", (17 July 2018), online: Channel News Asia <https://www.channelnewsasia.com/news/asia/indonesia-extremists-low-tech-get-around-high-tech-10568864>; Indonesia and the Tech Giants vs Isis Supporters: Combating Violent Extremism Online, by Institute for Policy Analysis of Conflict (IPAC), 48 IPAC Report (Institute for Policy Analysis of Conflict (IPAC)) at 9–11.

42 Lazuardi Utama, "Mengenal Cyber Drone 9, Polisi Internet Indonesia" (3 January 2018), *VIVA.co.id*, online: https://www.viva.co.id/digital/992995-mengenal-cyber-drone-9-polisi-internet-indonesia.

44 *Indonesia and the Tech Giants vs Isis Supporters: Combating Violent Extremism Online*, IPAC Report No. 48 (Institute for Policy Analysis of Conflict (IPAC), 2018) at 9–11.

The Constitutional Court also addressed wiretapping in a separate decision.[45] Importantly, the Chief Justice of the Constitutional Court, Mahfud MD, stated that there is a need for a special law to regulate wiretapping and its procedures.[46] He added that information tapping is one of the activities of communication intelligence, and therefore, to avoid legal uncertainty, any government actions related to conducting surveillance must be regulated by law.[47] Building on this position, it can be argued that ensuring the enactment of laws and regulations consistent with the rule of law requires both ex ante and ex post assessments..[48] This means that before a law is implemented, it is necessary to examine whether the law is coherent and would actually address the social issue it is designed to target. Another relevant question in this context is whether this law adheres to constitutional principles and human rights. Additionally, the foreseen and unforeseen consequences of this law should be taken into consideration.

Indonesia has undergone a significant digital transformation, including the adoption of surveillance technology. Today, surveillance technology is reportedly developing in increasingly sophisticated ways, from visual-based technology to biological-based systems such as biometrics, and is used to monitor both public spaces and private life. For instance, the deployment of closed circuit television (CCTV) in public areas became a national trend after it was introduced in conjunction with electronic traffic fines[49] through formal collaboration between the Indonesian National Police and the Local Government.[50] The emergence of the Internet of Things (IoT) has made the situation more complex. According to Hartato, around 400 million IoT sensor devices will be installed by 2030 across various sectors.[51]

---

45 *Judicial Review of Law Number 11 of 2008 concerning Electronic Information and Transaction 2008 Indonesian Constitutional Court Decision 5/PUU-VIII/2010*, 2011 Indonesian Constitutional Court at 72.

46 *Ibid.*

47 *Ibid.*

48 Maertje van der Woude, *Governing through Crises? Civil Liberties under Pressure* (School of Law BINUS University, 2020).

49 Karina Tehusijarana, "Tito TV: Minister Wants Face-Recognizing Surveillance Cameras, Says it Will 'Comfort' Public", (29 November 2019), online: *The Jakarta Post* <https://www.thejakartapost.com/news/2019/11/28/tito-tv-minister-wants-face-recognizing-surveillance-cameras-says-it-will-comfort-public.html>; "Indonesia Plans 6000-Camera Public CCTV System For Jakarta", (1 July 2016), online: *SEN News* <https://sen.news/indonesia-plans-6000-camera-public-cctv-system-for-jakarta/>.

50 Inang Jalaludin Shofihara, "Cegah Terorisme, DPR Usul Wajibkan Pemasangan CCTV untuk Dapatkan IMB", (18 November 2019), online: *KOMPAS.com* <https://nasional.kompas.com/read/2019/11/18/16131121/cegah-terorisme-dpr-usul-wajibkan-pemasangan-cctv-untuk-dapatkan-imb>; Gega Ryani Cahya Kurnia B P, "Peran Kamera Pengawas Closed-Circuit Television (CCTV) dalam Kontra Terorisme" (2021) 9:4 Jurnal Lembaga Ketahanan Nasional Republik Indonesia at 101–102.

51 Pingit Aria Mutiara Fajrin, "Kominfo Terbitkan Regulasi Internet of Things Awal 2019", (14 November 2018), online: *Katadata* <https://katadata.co.id/pingitfajrin/digital/5e9a559813be4/kominfo-terbitkan-regulasi-internet-of-things-awal-2019>.

In practice, some measures taken by the government tend to compromise the value of privacy, as there is a factual and legal tension between the privacy of citizens and the protection of their safety. The presence of adequate legal instruments combined with technical measures and "social technology"[52] norms may be used to tackle such issues. However, dealing with this factual and legal tension is complex because the State may need to sacrifice or compromise fundamental rights and freedom of expression in cyberspace under certain scenarios.

The following section discusses the risks associated with enhancing surveillance technology as a counterterrorism measure. The discussion focuses on the issues that arises when surveillance technology is required for counterterrorism activities, while, at the same time, the government has the obligation to respect and fulfil the fundamental rights of citizens, particularly the right to privacy.

3. Counterterrorism and the Right to Privacy in Indonesia

The legal framework on privacy has been recognized since the Indonesian Penal Code introduced the notion of non-interference with personal property.[53] The right to privacy is not explicitly stipulated within the 1945 Constitution of the Republic of Indonesia. However, this right can be derived from Article 28G paragraph (1) as follows:

> "Every person shall have the right to protection of his/herself, family, honour, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right".

This formulation of Article 28G, paragraph (1) is derived from both Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (hereinafter referred to as the 'ICCPR'), which explicitly outline the right to privacy. The Indonesia Constitutional Court Decision Number 50/PUU-VI/2008 concerning Judicial Review of Information and Electronic Transactions Law, the Constitutional Court delineated the legal concept of the right to privacy as follows:[54]

---

52 C R Henderson, "The Scope of Social Technology" (1901) 6:4 American Journal of Sociology at 465 and 472 Henderson explains social technology as a system of conscious and purposeful organization in which every member finds it as a true place, and all factors in harmony cooperate to realize and increasing the quality of the 'health, wealth, beauty, knowledge, sociability, and rightness' desires. This meaning was then widened to include "administration as well as the determination of the norms which are to be applied in the administration."; Luther Lie Bernard, "Standards of Living and Planes of Living" (1928) 7:2 Social Forces at 190 and 192.

53 *Judicial Review of Law Number 11 of 2008 concerning Electronic Information and Transaction (2008) Indonesian Constitutional Court Decision 50/PUU-VI/2008*, 2009 Indonesian Constitutional Court at 46.

54 *Ibid* at 47.

> "No one may be disturbed by his personal affairs, his family, his household, or his correspondence, arbitrarily, nor may he violate his honor and his good name. Every person has the right to get legal protection against such disturbances or violations."

A degree of awareness towards personal data protection is further reflected in the recently enacted Law No. 27 of 2022 concerning the Protection of Personal Data (hereinafter, UU PDP). The formulation of such legislation demonstrates the government's recognition of the importance of data protection as a fundamental human right that must be fulfilled. This acknowledgment roots back to Article 28G (1) of the Indonesian 1945 Constitution, which guarantees the right to privacy for every individual. The goal of this provision is to increase the confidence of Indonesian society in providing their personal data without any worries of misuse through the implementation of a legal framework that offers ample protection for personal data.

However, several provisions within the UU PDP remain vague, especially those regulating Indonesia's government controls. As a result, privacy violations may be exacerbated, especially due to the government or private sector gaining control over personal data as a data processor. This imbalance can complicate the collection and preservation of evidence in court proceedings, even though law enforcement agencies may rely on strong forms of digital evidence, such as network logs. Therefore, clear and robust regulations on how and when data collected through the networks can be accessed, as well as by who, should be outlined. Under UU PDP, there is still no clear and established standard that distinguishes the obligations of the data processor and controller. This is evident in Article 52 of the UU PDP, which states that all obligations of the data processor stipulated under Articles 29, 31, 35, 36, 37, 38, and 39 shall also be borne by the data controller. On this matter, the UU PDP merely emphasises the subordinate nature of the data processor as it is expected to function under the instructions of the data controller. It only denotes the fundamental obligations that both a data controller and processor are subject to, *inter alia*, maintaining secrecy, protecting personal data, conducting supervision over such data, and preventing unauthorised access to personal data.[55]

The UU PDP further regulates the government's access to personal data. Prior to the enactment of UU PDP, the government issued the Ministry of Communication and Information Regulation No. 5 of 2020, which similarly provides the authority for the government to access an individual's personal data under the control of a Private Electronic System Operation. These provisions are prescribed in Article 21, which stipulates that a Private Electronic System Operator is mandated to provide access to law enforcement agencies for electronic data. This regulation has been criticized by several digital rights defenders, such as the Southeast Asia Freedom of Expression Network (hereinafter, SafeNET), which has contended that such a power given to the government to easily access an individual's data can potentially amount to violations of Article 12 of

55 *Government Explanation on the Bill of Data Protection* (2020).

the United Nations Declaration of Human Rights and Article 17 of the International Convention on Civil and Political Rights. It further asserted that the provisions did not consider the establishment of an independent body that would be tasked to oversee the access to personal data. Emphasis was placed on the existence of precedents showing the misuse of personal data by law enforcement. SafeNET also took note of how the three-part test would be implemented, which legitimizes interference with human rights if the measure is prescribed by law, pursues a legitimate aim, and is necessary for a democratic society, in the interests of national security, or for the prevention of disorder or crime. The findings presented by Amnesty International clearly show that Indonesia still faces significant challenges in ensuring effective supervision over the use of and access to personal data by state institutions. The 2024 Amnesty International Security Lab report revealed that various government agencies, including the Indonesian Police and National Cyber and Crypto Agency, have procured and potentially used surveillance technologies without a clear legal framework or public accountability mechanism. The absence of an independent authority that can monitor and control the government's activities in this area creates a high risk of misuse of personal data and excessive surveillance. SafeNet have also raises concerns that the current regulatory structure allows government access to personal data without sufficient procedural safeguards or judicial oversight.[56]

However, it should be noted that Article 22 regulates the procedures for granting access to law enforcement officials. This includes steps such as detailing the aim of accessing personal data, the period of time for which the data will be accessed, and highlighting the exigency nature of the request. Moreover, Article 23 of the Regulation further prescribes that the request shall be made in conjunction with a prior assessment of the interests of the supervision as well as the proportionality and the legality of the aspects that are referred to in Article 22. These provisions indicate that while access to personal data can be granted to the government, such activity is regulated by a developed and systematic procedural rule. Although the three-part test should be used in conjunction with these provisions, they signify efforts made by the government to mandate consideration of the proportionality and legality aspects of the measure.

Article 15 of the UU PDP prescribes that the rights of the subject of personal data may be derogated to uphold the government's interests in national security and law enforcement, execution of State functions, oversight of the financial sector, ensuring the stability of the financial sector, as well as facilitating research and data collection. The formulation of such an Article derives from the public interest principle, which allows the derogation of certain rights to uphold public security, sovereignty, and to eradicate criminal acts.[57] Article 10(1) allows data subjects to submit an objection or complaint over an action, such as profiling, that imposes legal consequences or has significantly impacted the rights of the subject concerned. The procedure to exercise such an exception,

55 Southeast Asia Freedom of Expression Network (SAFEnet), Policy Brief: Evaluating the Implementation of the Personal Data Protection Law in Indonesia (2023), online: https://safenet.or.id/.

57 *Academic Draft of the Bill of the Protection of Data Privacy*, at 37.

however, has not been clearly explicated, making it prone to misuse and abuse of an individual's right to privacy.

Exceptional clauses within the UU PDP lack a clear standard on its limitation and the requirement of reasonable precautions. Article 15 of the UU PDP, for instance, does not address the limitations and the extent of the exception provided. In comparison, Article 23 of the EU's General Data Protection Regulation and Articles 11 (1) and 11 (2) of the 108+ Convention prescribe that the use of the exceptional clause can be justified only if the measure taken is both necessary and proportionate. This entails the obligation to conduct a prior assessment to ensure that the extent of the means taken is not excessive in relation to the rights of the subjected individuals.[58] On the contrary, Article 15 of the UU PDP does not provide any restrictions, mechanisms, or guidelines on prior actions that shall be taken.[59] It merely allows the government to exercise such an exception for the public interests without any prior consideration. This may be easily taken advantage of, as the government can justify the actions as necessary, as they correlate with the preservation of public interests, but fails to consider whether the measures taken are proportionate in relation to the rights of the individual subject.

Similarly, Article 17 of UU PDP governs the installation of CCTVs, allowing them to be used for specific purposes such as safety, disaster prevention, and traffic management, and requires individuals in the area to be informed that CCTV is in use. As a general rule, CCTV may not be used to identify specific individuals. However, this prohibition is subject to an exception where identification is necessary to prevent a criminal act or to carry out law enforcement in accordance with applicable law. The mere recognition of such an exception, without clear limits or safeguards, is insufficient. While crime prevention and law enforcement are legitimate objectives, the government must also ensure that the measures adopted are proportionate to those aims. This requires an assessment of potential risks and the adoption of safeguards to prevent unjustified interference with the right to privacy arising from the use of CCTV. The rights of the individuals being subjected to surveillance shall be reconciled with the goals of law enforcement by first taking reasonable precautions prior to installing a CCTV system.[60]

The absence of clear precautionary regulation is further reflected in Article 20 of the UU PDP, which merely requires data controllers to identify a lawful basis for processing personal data. Such a basis shall encompass consent, the protection of the individual's private interests, the execution of tasks for the public interest, service, or the authority of the data controller based on the law, or, the fulfillment of interests by taking

---

58 *Studi Pendahuluan: Perbandingan Rancangan Undang-undang Perlindungan Data Pribadi dengan Konvensi Eropa 108+ dan GDPR*, by Sherly Haristya et al (Jakarta: Tifa Foundation, 2020).

59 Wahyudi Djafar, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan" Fakultas Hukum Universitas Gadjah Mada, online: <https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf> at 12.

60 *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties* (Washington, DC: The Constitution Project, 2006).

into account the aim, need, and balance between the data controller and the rights of the subjected individual. Although these factors convey rigid guidelines for a data controller, the article remains lacking in protections when compared to Article 6(4) of the GDPR.

Article 6(4) of the GDPR acknowledges the possibility that data may be processed for new purposes. The data controller must conduct a compatibility test when the data subject has not consented to the processing of personal data and the processing is not based on a legal obligation. For instance, it emphasizes that the nature of the personal data must be considered, which includes assessing whether it involves a high degree of sensitive information. In comparison to the provisions within the UU PDP, the GDPR's compatibility testing requires data controllers to conduct additional inspections to ensure the lawfulness of their data processing activity. This assessment reflects the use of good governance principles, particularly accountability, in further enhancing the protection of personal data. Although the UU PDP has incorporated this principle into its provisions, additional measures are still required to ensure the utmost protection of personal data.

The foregoing analysis demonstrates that Indonesia has made meaningful normative progress in recognizing privacy and personal data protection as components of fundamental rights, particularly through constitutional interpretation and the enactment of the Personal Data Protection Law (UU PDP). However, the regulatory framework governing intelligence surveillance and access to personal data remains fragmented, exception-heavy, and insufficiently constrained by clear necessity and proportionality. While procedural requirements exist for government access to personal data, key provisions especially those permitting derogations in the name of public interest, national security, and law enforcement lack clearly articulated limits, authorization mechanisms, and independent oversight. This creates structural vulnerabilities that may enable excessive surveillance practices and weaken effective remedies for rights holders. The Indonesian approach thus reveals an enduring tension between security-oriented governance and rights-based democratic accountability, particularly in the absence of robust precautionary and review mechanisms. This tension provides an important point of comparison with Canada, where surveillance powers are more explicitly embedded within judicial authorization frameworks and constitutional jurisprudence. The following sections therefore examine the use of intelligence surveillance as a counterterrorism measure in Canada.

III. INTELLIGENCE SURVEILLANCE AND COUNTERTERRORISM IN CANADA

In 2004, Professor Sossin posed what the authors regard as the central question for evaluating Canada's counter-terrorism measures, namely how the exercise of executive power in the name of national security can be effectively overseen, limited, and supervised so that it remains consistent with the rule of law and the fundamental values

underpinning Canadian society"[61] Keeping in mind that technology has made significant strides since this question was posed, it will serve as the underlying focus throughout the analysis of Canada's counterterrorism measures, along with an analysis of the varied implications of specific uses and applications of AI.[62]

1. Canada's Legal Framework on Terrorism

Canada had no official anti-terrorism legislation until the passing of the Anti-terrorism Act in 2001.[63] The act defines terrorism as acts, within or outside of Canada, that are taken or threatened for political, religious or ideological purposes and which threaten the public or national security by killing, seriously harming or endangering a person, causing substantial property damage that is likely to seriously harm people or by interfering with or disrupting an essential service, facility or system.[64] The Anti-terrorism Act of 2015, also known as Bill C-51, created the Security of Canada Information Sharing Act and the Secure Air Travel Act, and amended several existing acts, including the Canadian Security Intelligence Service Act, the Criminal Code, and the Immigration and Refugee Protection Act. Under the Criminal Code, a terrorist activity is defined as an action that takes place either in or outside Canada, committed in whole or in part for a political, religious or ideological *purpose, objective or cause*, and intended to intimidate the public 'with regard to its security, including its economic security' or compelling people, governments or domestic or international organizations to do or to refrain from doing any act' whether those targets are in or outside of Canada.

According to research by Roach, the Supreme Court of Canada has stressed the importance of requiring proof of terrorist purposes and has read broadly defined terrorism offences to exclude conduct that creates only a negligible risk of harm.[65] With respect to the concept of 'terrorist activity', Douglas wrote, "Canada ... defines terrorist activity to include activities falling within a number of specified offences that implement Canada's obligations under terrorism conventions. ... . [it] includes conspiracies, threats, attempts, being an accessory after the fact, and counselling in relation to terrorist

61 "The Views of Canadian Scholars on The Impact of the Anti-Terrorism Act" (2004) Department of Justice Canada at 71.

62 Aviv Gaon & Ian Stedman, "A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada" (2019) 56:4 Alberta Law Review at 1165.

63 Kristen N Leppington, *Bill C-36: The Creation of Canada's 2001 Anti-Terrorism Act* (Master Thesis in Political Science, Laval University, 2011) [unpublished] at 2; Alex Conte, *Human Rights in the Prevention and Punishment of Terrorism* (Berlin: Springer Berlin Heidelberg, 2010) at 164.

64 Faisal Bhabha, "Tracking Terrorists' or Solidifying Stereotypes – Canada's Anti-Terrorism Act in Light of the Charter's Equality Guarantee'" (2003) 16:95 Windsor Review of Legal and Social Issues at 110–111.

65 Kent Roach, "Be Careful What You Wish For? Terrorism Prosecutions in Post-9/11 Canada" (2014) 40:99 Queen's LJ at 101.

activities."[66] A terrorist activity also "requires proof of *motive* as an essential element of a crime, something that is generally not necessary in criminal law."[67] Indeed, Justice Dickson of the Supreme Court of Canada wrote in *United States of America v. Dynar*, "It does not matter to society, in its efforts to secure social peace and order, what an accused's motive was, but only what the accused intended to do."[68] Justice Dickson further clarified, "Normally, motivation is irrelevant for intention."[69] This may be explained by the fact that "[t]errorism ... is a highly political ... activity"[70] and is also "highly motivated by an ideology"[71], which "acts of violence ... target civilians in the pursuit of political or ideological aims."[72] Roach observed, "Canada borrowed a political or religious motive requirement from British law as a means to distinguish terrorism from other crimes".[73] In addition, it must be noted, "Canada did not simply copy the British legislation, but took a more restrained approach."[74] It must also be noted that "[d]espite the prolific use of this concept, 'terrorism' is not an unequivocal and unanimously accepted concept in the field of criminal law."[75] Generally speaking, isolated "two different approaches ...: either a specific definition has been implemented into national law (as in the UK's [Terrorism Act] 2000) or a 'scheduled offence' approach has been followed."[76]

For those who would fear an all-encompassing or an inappropriate application of the definition of terrorism in Canada, let us mention that according to Douglas: "The Canadian, New Zealand, and Australian definitions [provide] that in certain circumstances, behaviour that would otherwise constitute terrorism will not do so if the

66 Roger Douglas, *Law, Liberty, and the Pursuit of Terrorism* (Michigan: University of Michigan Press, 2014) at 50–51.

67 Kent Roach, 'Did September 11 Change Everything - Struggling to Preserve Canadian Values in the Face of Terrorism', (2002) 47 *McGill LJ 893*, 903 (italics added).

68 *United States of America v Dynar, [1997] 2 SCR 462*, at para 81.

69 *Ibid* at para 79. Citing 'The Lords and Impossible Attempts, or Quis Custodiet Ipsos Custodes?', [1986] Cambridge L.J. 33, at 78.

70 David M Paciocco, "Constitutional Casualties of September 11: Limiting the Legacy of the Anti-Terrorism Act" (2002) 16 The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference at 186 Now judge at the Court of Appeal for Ontario; Mariona Llobet Anglí, "What does 'terrorism' mean" in Aniceto Masferrer & Clive Walker, eds, *Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of State* (Gloucestershire: Edward Elgar, 2013) at 17–36.

71 Michael Freeman, *Freedom or Security: The Consequences for Democracies Using Emergency Powers to Fight Terror. Praeger* (Westport: Praeger, 2003) at 30.

72 United Nations Office of the High Commissioner for Human Rights, *supra* note 33 at 5-6.

73 Kent Roach, "Counter-Terrorism In and Outside Canada and in and Outside the Anti-Terrorism Act" (2012) 16:2 Review of Constitutional Studies/Revue d'études constitutionnelles at 247.

74 *Ibid* at 246. For example, "The Canadian offences are broad, but do not go quite as far as British offences that apply to the possession of items and training that may only be peripherally linked to terrorism", at 249.

75 Aniceto Masferrer & Clive Walker, eds, *Counter-Terrorism, Human Rights and The Rule df Law: Crossing Legal Boundaries in Defence of State* (United Kingdom: Gloucestershire, 2013) at 18.

76 *Ibid* at 87–105.

act constitutes advocacy, protest, dissent, or industrial action. In Canada, an act that falls within one or more of these categories and involves disruption to an essential service does not constitute terrorism *unless* it is intended to cause serious harm, endanger a life, or endanger the health or safety of the population."[77] As this last author also aptly observed:[78]

> "Definitions have rarely given rise to litigation, and insofar as courts have considered the meaning and validity of definitions, they have generally agreed with the government. The only exception is ***R v Khawaja,*** a Canadian case where a defendant charged with terrorism offences argued that the motivation requirement represented an unconstitutional interference with freedom of political and religious expression."

Mohammad Momin Khawaja was the first person charged and convicted of terrorism offences established under the *Anti-terrorism Act* 2001. The case went before the Supreme Court of Canada, which concluded that section 83.18 is not grossly disproportionate nor overbroad in relation to the objective of prosecuting and, in particular, of preventing terrorism.[79] Before Khawaja was rendered in 2012, the definition of terrorist activity given in the 2002 case of *Suresh v. Canada* departed from the *Anti-terrorism Act* definition because it did not require proof of political or religious motive.

The literature and jurisprudence discussed above demonstrate that Canadian terrorism law has developed along a carefully delimited path that seeks to reconcile preventive security objectives with core principles of criminal legality. Although terrorism offences are drafted broadly and encompass preparatory conduct, courts have emphasized purposive interpretation, motive requirements, and harm thresholds as limiting devices. These doctrinal features function to prevent the concept of terrorism from collapsing into ordinary criminality or from being applied to conduct that lacks a genuine nexus to political or ideological violence. In this sense, Canadian law reflects a conscious effort to preserve conceptual coherence and proportionality in an area of criminal law that is otherwise prone to expansion under conditions of perceived existential threat. The evolution from Suresh to Khawaja highlights the dynamic and contested nature of terrorism definitions, particularly with respect to motive and preventive rationales. This tension underscores the importance of continued scrutiny of how terrorism offences are interpreted and applied, especially as they form the legal foundation for broader state powers, including surveillance, preventive detention, and other exceptional security measures

77 Douglas, *supra* note 75 at 54 (italics added).

78 *Ibid* at 58.

79 ***R v Khawaja, 2012 SCC 69, [2012] 3 SCR 555***, 2012 at para 63, in fine; see also Conte (n 73), 170. For a more recent discussion of the overbreadth characters of a provision connected to a terrorism offence, see e.g. Canada (Attorney General) v. Driver, 2016 MBPC 3, paras. 35-44.

2. Intelligence Surveillance in Canada

Following the September 11 terrorist attack on the United States, "[w]ho would contest the necessity of electronic surveillance to combat biker gangs, transnational mafias, or Al-Qaeda? ... there is even greater justification for more intrusive state conduct and extraordinary police powers when the security of the nation is at risk."[80]; "What better way for the Canadian government to fight terrorism than through the employment of sophisticated technology to eavesdrop on those that they suspect of planning terrorist activity?"[81] Even though 'September 11' may still be fresh in our memory, it is not new that intelligence gathering has an important place in police work in Canada. Decades ago, the Ouimet Committee in its 1969 report stated, "One of the most important aspects of police work in the field of crime prevention and the detection and apprehension of offenders involves the gathering of information with respect to intended crimes and the organisation of criminal groups."[82] Most people will agree that "[t]he advance of science and technology is inexorable"[83], and then the investigative methods to gather intelligence must adapt accordingly.

Feldstein commented, "tracking tools play a vital role in preventing terrorism [b]ut technology has changed the nature of how governments carry out surveillance and what they choose to monitor."[84] The same applies to terrorists: they "use modem communication tools ... Al Qaeda elements may communicate by e-mail or through the use of Internet websites."[85] However, it must be noted that after the terrorist attack on the United States in 2001, "Canadian surveillance legislation has remained largely unchanged, and there have been no relevant changes to the surveillance powers of the Canadian Security Intelligence Service."[86] This may be because "Canada's national security agencies already had broad surveillance powers." In a nutshell, "Communications surveillance in national security investigations is typically conducted by the Royal Canadian Mounted Police ('RCMP')"[87] but Three entities are responsible for national security in Canada: the police, including the RCMP, the Canadian Security Intelligence Service ('CSIS') established in 1984, and the Communications Security Establishment Canada ('CSEC') established after World War II and transferred to the Department of National Defence in 1975.

---

80 Penney, *supra* note 71 at 263.

81 Yoni Rahamim, "Wiretapping and Electronic Surveillance in Canada: The Present State of the Law and Challenges to the Employment of Sophisticated and Intrusive Technology in Law Enforcement" (2004) 18 Windsor Rev Legal & Soc Issues 87 at 102–103.

82 Stanley A Cohen, "Invasion of Privacy: Police and Electronic Surveillance in Canada" (1982) 27:4 McGill Law Journal at 667.

83 *Ibid* at 651.

84 Feldstein, *supra* note 9.

85 Wayne N Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy" (2006) 43:3 Alberta Law Review at 783.

86 Douglas, *supra* note 75 at 77.

87 Penney, *supra* note 71 at 253.

The police including the RCMP, CSIS and CSEC "may conduct surveillance of private, domestic communications and activities when they have reasonable grounds to believe that such surveillance will reveal evidence of a broad range of criminal offences, including all terrorism-related offences."[88] For example, "the Canadian Security Intelligence Service ... is empowered to gather information concerning activities that give reasonable cause to suspect that they may endanger the security of Canada ... The information must be gathered under a judicial search warrant"[89]; "the requirement of "reasonable and probable grounds" as a condition precedent to most police actions ... is the mechanism whereby the state insures that official action will not be arbitrary."[90] In short, "[i]n almost all cases, prior judicial authorization is still required before electronic surveillance or communications interception can be conducted by Canadian authorities."[91] Also, the Supreme Court of Canada stated in *R. v. Araujo* that State agents may also have to show that there is "no other reasonable alternative method of investigation"[92] before obtaining an authorization to intercept electronic communications. This is known as the "investigative necessity" requirement"[93], which "can be demonstrated in numerous ways, for example, by showing that alternative methods, such as the use of physical surveillance, informants, undercover agents, and ordinary search warrants, would likely be dangerous or ineffective."[94] However, as noted in *R. v. Desjardins*, "given the difficulties associated with investigating and prosecuting criminal organizations and terrorism, the investigative necessity requirement is not applicable for these offences".[95] Some authors contend that "allowing police to conduct communications surveillance in terrorism investigations without establishing investigative necessity ... should be found to violate section 8 of the *Charter* because they infringe substantially on the privacy of innocent Canadians, especially those of Muslim or Arab background, while doing little to advance national security."[96] Since then, "the courts have considered whether investigative necessity is only a statutory requirement or whether it is also a constitutional requirement".[97] In *R. v. Largie*, the Court of Appeal for Ontario stated, "Nowhere does the Court characterise investigative necessity as a constitutional

88 *Ibid* at 248–249.

89 Emanuel Gross, "The Struggle of a Democracy against Terrorism - Protection of Human Rights: The Right to Privacy versus the National Interest - the Proper Balance" (2004) 37:1 Cornell International Law Journal at 79–80; *Canadian Security Intelligence Service Act, RSC 1985, c C-23*, ss 12 and 21; *Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re), [2019] 2 FCR 359*, ss 12 and 21.

90 A. Cohen, *supra* note 92 at 63.

91 Wispinski, *supra* note 70 at 8–9. Besides, "the sole exception to this is when "private communication" is intercepted by the Communications Security Establishment (CSE), in which case prior authorization from the Minister of National Defence is required. There are many safeguards contained in the provisions authorizing CSE interceptions that are designed to limit when such interceptions can be authorized and how the intercepted information may be used once captured".

92 *R v Araujo, [2000] 2 SCR 992*, at para 29 in fine and 35.

93 Penney, *supra* note 71 at 250.

94 *Ibid* at 257.

95 *R v Desjardins, 2014 QCCS 6712*, at para 11.

96 Penney, *supra* note 71 at 252.

97 *R. v. Desjardins, 2014 QCCS 6712*, *supra* note 105 at para 16.

requirement, or as anything other than statutory pre-condition."[98] The same court in *R. v. Lucas* reached the same conclusion four years later.[99] In addition, the deciding judge in *R. v. Desjardins* concluded that it does not violate s. 8 of the Charter.[100]

Penney wrote, "[i]n response to terrorist attacks, many nations have passed laws broadening the surveillance capacities of law enforcement and national security agencies. Some have argued that these laws unduly diminish the liberty, privacy, and equality interests of non-terrorists".[101] Let us examine more closely in the next section some of the Canadian fundamental rights provided by the *Canadian Charter of Rights and Freedoms*[102] ("Charter"), enacted in 1982 and part of the Canadian constitution, which may need to be considered with respect to terrorism criminal offences.

Taken together, this body of scholarship and jurisprudence reveals a consistent trajectory in Canadian national security law in which technological change and the post-9/11 security environment have intensified the perceived need for electronic surveillance, yet Canada has largely relied on pre-existing institutional and legal frameworks rather than radically expanding formal surveillance powers. Surveillance activities conducted by the RCMP, CSIS, and CSEC remain, in principle, constrained by requirements of reasonable grounds and prior judicial authorization, reflecting a longstanding commitment to guarding against arbitrary state action. At the same time, courts have shown considerable deference in terrorism and organized crime cases by limiting the applicability of the investigative necessity requirement, characterizing it as a statutory rather than constitutional safeguard and rejecting claims that its relaxation violates section 8 of the Charter. This judicial approach underscores an enduring tension between national security imperatives and individual privacy rights, one that has become more pronounced as surveillance technologies grow increasingly intrusive and as counter-terrorism rationales continue to justify exceptional investigative measures.

3. Counterterrorism and The Right to Privacy in Canada

According to the United Nations Office on Drugs and Crime,[103] several experts describe the integration of intelligence activities with the criminal justice system as a fundamental problem in dealing with terrorism. The division of counter-terrorism intelligence collection along geographical and functional lines between ministries, the desire to protect sensitive sources and methods, and concerns about protecting civil liberties create

98 *R v Largie, 2010 ONCA 548*, at para 46, cited in *R. v. Desjardins*, *Ibid* at para 25.

99 *R v Lucas, 2014 ONCA 561*, at para 101, leave to appeal to SCC dismissed, no. 35974 (January 22, 2015).

100 *R. v. Desjardins, 2014 QCCS 6712*, *supra* note 105 at para 42.

101 *Ibid* at 248.

102 *Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being schedule B the Canada Act 1982 (UK) 1982*, c 1.

103 *Supra* note 26 at 70.

inherent difficulties in coordinating inquiries and prosecutions while protecting legally recognised rights.

With respect to privacy rights, the United Nations Office of the High Commissioner for Human Rights observes that some States have significantly extended their surveillance powers in recent years. This may give way to the use of powerful technologies for collecting and sharing detailed personal information by law enforcement, potentially leading to an erosion of privacy. Many governments have been deploying CCTV to monitor public spaces, promoting the use of national identification cards embedded with biometric identifiers, and accessing personal information held in private sector databases.[104] Conte encapsulated the tension that then exists between human rights, in general, and security in the context of combatting terrorism:[105] Debates on counter-terrorism and human rights are often polarized, with some viewing counter-terrorism as an unjustified expansion of state power and others treating human rights as secondary to security, raising the question of whether effective counter-terrorism can be reconciled with democratic principles and human rights.Canada is widely regarded as one of the world's leading democracies, due to its systems and rules designed to strengthen and protect democratic values and institutions.[106] Thus, comparing Indonesia with Canada in terms of their ability to balance national security with protection of human rights can provide valuable insights.

According to Rahamim, while the *Anti-terrorist Act* granted expanded powers to the [law enforcement] of Canada in the context of surveillance and interception of private communications, it also respected the integrity of Canadian Charter rights.[107] Therefore, the Canadian example could be valuable for Indonesia. However, according to Cockfield' Canada's promotion of new technologies by police and intelligence officials to locate, track and arrest suspects has been accompanied by legislative changes that dilute traditional safeguards against State searches.

In Canada, privacy as a fundamental right is protected by section 8 of the *Canadian Charter of Rights and Freedoms*. Privacy can be divided into categories that include personal privacy[108], territorial privacy[109] and informational privacy[110] The fundamental right to privacy also serves as a safeguard against unreasonable search and seizure.[111] For an

104 Arthur J Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" 40:1 UBC Law Review 2007 at 41.

105 Conte, *supra* note 65 at 282.

106 United Nations Office on Drugs and Crime, *supra* note 26 at 1152.

107 Rahamim, *supra* note 91 at 102–103.

108 *R v Stillman, [1997] 1 SCR 607*; *R v Golden, [2001] 3 SCR 679*; *R v Saeed, [2016] 1 SCR 518*.

109 *R v Edwards, [1996] 1 SCR 128*; *R v Feeney, [1997] 2 SCR 13*; *R v White, 2015 ONCA 508*; *R v Saciragic, 2017 ONCA 91*.

110 *R v Tessling, [2004] 3 SRC 432*; *R v Morelli, [2010] 1 SCR 253*; *R v Cole, [2012] 3 SCR 34*; *R v Marakah, [2017] 2 SCR 608*; *R v Reeves, [2018] 3 SCR 531*; *R v Dyment, [1988] 2 SCR 417*, at para 19.

111 When it is found to be unreasonable by a court, the evidence gathered may potentially be excluded pursuant to section 24(2) Charter.

action to constitute a reasonable search or seizure, the impacted individual must have a reasonable expectation of privacy in the information that the State has accessed.[112] With respect to electronic surveillance, the Supreme Court of Canada in *R. v. Duarte* stated that its "very efficacy ... is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private."[113] However, like all *Charter* rights, the right to privacy is not absolute, but rather protects a reasonable expectation of privacy[114] to be determined on the totality of circumstances.[115] The reasonable expectation of privacy must give way to the State's legitimate law enforcement interest in appropriate circumstances.[116] Reasonable expectation of privacy applies to intelligence surveillance and gathering, but has proved to be much more complicated, especially with the development of new technology.[117] Indeed, Canada's legal privacy framework has struggled to address the unique issues raised by many new technologies.[118] For example, the Supreme Court's section 8 jurisprudence pulls in opposing directions. On the one hand, it suggests that since communications surveillance is such a grave and pernicious threat to privacy, it should not be used unless truly necessary. On the other hand, jurisprudence reflects the concern that, because terrorism constitutes a grave and diffuse threat to security, national security surveillance should not be conditioned on the existence of reasonable ground.[119]

Further, equality is also protected as a fundamental right by section 15 of the Charter. It is a guarantee of non-discrimination, setting essential human dignity as its defining standard.[120] Some authors contend that the *Anti-terrorism Act* discriminates on the basis of race, religion, colour and ethnic or national origin, specifically targeting Muslims.[121] They also raise concerns that the political climate has, since September 2001, become ardently Islamophobic.[122] A judge of the Ontario Superior Court also took judicial notice in *R. v. Odle* that "racial stereotypes and racial bias exist in Canadian

112 *Hunter et al v Southam Inc, [1984] 2 SCR 145*, at 150–160; *Goodwin v British Colombia (Superintendent of Motor Vehicle), [2015] 3 SCR 250*, at para 55.

113 *R v Duarte, [1990] 1 SCR 30*; *R v Wong, [1990] 3 SCR 36*.

114 It was first outlined by the Supreme Court of Canada in *Hunter et al. v. Southam Inc.* (n 124).

115 *R. v. Edwards, [1996] 1 SCR 128*, *supra* note 121 at paras 31 & 45 (5); *R. v. Reeves, [2018] 3 SCR 531*, *supra* note 122 at para 12.

116 Mathew Johnson, "Privacy in the Balance - Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8" (2012) 58:3 Criminal Law Quarterly at 444–445.

117 *Ibid*.

118 Johnson, *supra* note 128; Zaia Reem, "Awakening Section 8 in Wakeling: Legal Implications on Wiretaps, Intercepts, Intelligence Sharing and Beyond" (2017) 50:1 UBC Law Review at 208: "Whether the doctrinal section 8 test is sufficient in the face of developing technology is a question that frequently occupies jurisprudential thinking and scholastic thought."

119 Penney, *supra* note 71 at 251.

120 Bhabha, *supra* note 68 at 135.

121 *Ibid* at 98.

122 *Ibid* at 117; *Elmasry and Habib v Roger's Publishing and MacQueen (No 4), 2008 BCHRT 378*, at para 89; John Boccabella, "Profiling the Anti-Terrorism Act: Dangerous and Discriminatory in the Fight Against Terrorism" (2023) 9:1 Appeal: Review of Current Law and Law Reform at 17.

society."[123] However, the Canadian judicial system and prosecutors are meant to serve as a safeguard against discrimination by all law enforcement agencies enforcement in Canada. An example of the court serving as a safeguard is given by the decision rendered by the Federal Court of Canada, where it recommended "a comprehensive external review [of Canadian Security Intelligence Service that] must address more fundamental concerns relating to the prioritisation of the rule of law as a foundational principle in all [Canadian Security Intelligence Service'] decision-making."[124]

IV. CONCLUSION

The legal definition of terrorism has greatly evolved in Canada and Indonesia. Both countries have adopted a similar definition of terrorism, considering the motive of the perpetrators of terrorism offences. However, some issues remain, as both countries have been criticized for the lack of clarity in certain aspects of their definitions.

In both countries, authority is given to investigators to intercept phone conversations or other types of communication of individuals who are suspected of preparing, planning, and conducting any acts of terrorism. Contrary to Canada, which governs surveillance methods under its Criminal Code and not by means of special legislation, Indonesia regulates surveillance methods specifically under its Anti-Terrorism Act. The authors argue that Indonesia's legal framework on surveillance still lacks clear limitations as to when surveillance is deemed excessive and threatens violation of the right to privacy. In Canada, the legal requirements for obtaining a search warrant, issued by a court to use surveillance methods, serve as a safety net to protect, to a certain extent, against potential breaches of fundamental rights, even if this does not provide flawless protection in all circumstances. Breaches may still be possible in that context, and they may then be challenged in court.

Under the Indonesian and Canadian Constitutions, the right to privacy is not expressly stipulated. In terms of their respective approaches to the use of surveillance technology in addressing terrorism, Indonesia places emphasis on its national security, which may make tilt the balance of justice in a way that may compromise the right to privacy of suspected individuals. Canada, on the other hand, has a robust jurisprudence on the right to privacy, which addresses the legal requirements that apply in the context of surveillance methods. While national security remains a priority, the authors argue that Canada is more inclined to strike a balance between national security and the right to privacy in the context of surveillance and terrorism offenses.

---

123 *R v Odle, 2020 ONSC 3991*, at para 53, see also the list of the relevant Canadian jurisprudence regarding the "systemic racism against Indigenous people within the Canadian criminal justice system" at para 54, and "[t]he prevalence of anti-Black racism in the criminal justice system and the overrepresentation of African Canadians in ... jails" at para 55.

124 *Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re), 2020 FC 616, 310*, ss 12 and 21.

Measured against international human rights standards on communications surveillance, especially the requirements of legality, necessity, proportionality, and effective oversight, Canada's surveillance framework exhibits a relatively strong level of formal compliance, largely attributable to robust judicial authorization mechanisms and well-developed privacy jurisprudence. Indonesia's framework, by contrast, raises greater concerns under international human rights law, as broad preventive powers and limited supervisory mechanisms risk enabling disproportionate interferences with the right to privacy.

BIBLIOGRAPHY

Amnesty International, "Two Years After Snowden: Protecting Human Rights in an Age of Mass Surveillance", (2015), online: *Amnesty International* <amnesty.ch/de/themen/ueberwachung/edward-snowden/dok/2015/zwei-jahre-nach-den-snowden-enthuellungen-regierungen-halten-an-massenueberwachung-fest/two-years-after-snowden-protecting-human-rights-in-an-age-of-mass-surveillance-bericht-zur-massenueberwachung>.

A Cohen, Stanley, "Invasion of Privacy: Police and Electronic Surveillance in Canada" (1982) 27:4 McGill Law Journal.

Andapita, Vela, "Smart City Relies on True 'Guardians': CCTV Cameras", (13 February 2019), online: *The Jakarta Post* <www.thejakartapost.com/news/2019/02/13/smart-city-relies-true-guardians-cctv-cameras.html>.

Aria Mutiara Fajrin, Pingit, "Kominfo Terbitkan Regulasi Internet of Things Awal 2019", (14 November 2018), online: *Katadata* <https://katadata.co.id/pingitfajrin/digital/5e9a559813be4/kominfo-terbitkan-regulasi-internet-of-things-awal-2019>.

BBC, "Indonesia Bombing: Worshippers Wounded in Makassar Church Attack", (28 March 2021), online: *BBC* <https://www.bbc.com/news/world-asia-56553790>.

Beech, Hannah, "What Indonesia can teach the world about counterterrorism", (7 June 2010), online: *Time* <http://content.time.com/time/subscriber/article/0.33009.1992246.00.html>.

Bell, Stewart, "Suspect's alleged statements about ISIS led to terrorism charge over Toronto hammer attack: sources", (16 March 2020), online: <https://globalnews.ca/news/6661038/toronto-hammer-attack-by-isis-supporter/>.

Bhabha, Faisal, "Tracking Terrorists' or Solidifying Stereotypes – Canada's Anti-Terrorism Act in Light of the Charter's Equality Guarantee'" (2003) 16:95 Windsor Review of Legal and Social Issues.

Boccabella, John, "Profiling the Anti-Terrorism Act: Dangerous and Discriminatory in the Fight Against Terrorism" (2023) 9:1 Appeal: Review of Current Law and Law Reform.

Butt, Simon, "Anti-Terrorism Law and Criminal Process in Indonesia'" (2008) Islam and Modernity: Syari'ah, Terrorism and Governance in South-East Asia Background Papers, online: <https://law.unimelb.edu.au/__data/assets/pdf_file/0010/1546327/AntiTerrorismLawandProcessInIndonesia2.pdf>.

Campbell, Charlie, "ISIS Unveiled: The Story Behind Indonesia's First Female Suicide Bomber", (3 March 2017), online: *TIME* <https://time.com/4689714/indonesia-isis-terrorism-jihad-extremism-dian-yulia-novi-fpi/>.

Carrieri, Matthew et al, "Exploring Communications Surveillance in Indonesia", (25 October 2013), online: *The Citizen Lab* <https://citizenlab.ca/2013/10/igf-2013-exploring-communications-surveillance-indonesia/>.

Cavoukian, Ann, "Surveillance, Then and Now: Securing Privacy in Public Spaces" (2013) Information and Privacy Commissioner, online: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-surveillance.pdf>.

CNBC, "Telegram Blocks Terror Content After Indonesia Threatens Ban", (16 July 2017), online: CNBC <https://www.cnbc.com/2017/07/16/telegram-blocks-terror-content-after-indonesia-threatens-ban.html>.

Conte, Alex, *Human Rights in the Prevention and Punishment of Terrorism* (Berlin: Springer Berlin Heidelberg, 2010).

Department of Justice Canada, "The Views of Canadian Scholars on The Impact of the Anti-Terrorism Act" (2004) Department of Justice Canada.

Djafar, Wahyudi, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan" Fakultas Hukum Universitas Gadjah Mada, online: <https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>.

Douglas, Roger, *Law, Liberty, and the Pursuit of Terrorism* (Michigan: University of Michigan Press, 2014).

European Data Protection Supervisor, "Necessity & Proportionality", online: *European Data Protection Supervisor* <https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en>.

Feldstein, Steven, "The Global Expansion of AI Surveillance", (17 September 2019), online: *Carnegie Endowment for International Peace* <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>.

Fenton, Adam & David Price, "Indonesia's New Legislation for Countering the Financing of Terrorism" (2014) 15:1 Australian Journal of Asian Law.

Fitriani et al, *The Current State of Terrorism in Indonesia: Vulnerable Groups, Networks, and Responses*, The CSIS Working Paper Series 2 (Jakarta: Centre for Strategic and International Studies, 2018).

Fournier, Louis, *F.L.Q.: The Anatomy of an Underground Movement* (Toronto: NC Press, 1984).

Freeman, Michael, *Freedom or Security: The Consequences for Democracies Using Emergency Powers to Fight Terror. Praeger* (Westport: Praeger, 2003).

Friedman, Barry, *Unwarranted: Policing Without Permission* (New York: Farrar, Straus and Giroux, 2017).

Gaon, Aviv & Ian Stedman, "A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada" (2019) 56:4 Alberta Law Review.

Gershman, John, "Is southeast Asia the second front?", (1 October 2002), online: *Foreign Affairs* <https://www.foreignaffairs.com/articles/southeast-asia/2002-10-01/southeast-asia-second-front>.

Gross, Emanuel, "The Struggle of a Democracy against Terrorism - Protection of Human Rights: The Right to Privacy versus the National Interest - the Proper Balance" (2004) 37:1 Cornell International Law Journal.

Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties (Washington, DC: The Constitution Project, 2006).

Haristya, Sherly et al, *Studi Pendahuluan: Perbandingan Rancangan Undang-undang Perlindungan Data Pribadi dengan Konvensi Eropa 108+ dan GDPR*, by Sherly Haristya et al (Jakarta: Tifa Foundation, 2020).

Indonesia and the Tech Giants vs Isis Supporters: Combating Violent Extremism Online, IPAC Report No. 48 (Institute for Policy Analysis of Conflict (IPAC), 2018).

Institute for Policy Analysis of Conflict (IPAC), *Indonesia and the Tech Giants vs Isis Supporters: Combating Violent Extremism Online*, by Institute for Policy Analysis of Conflict (IPAC), 48 IPAC Report (Institute for Policy Analysis of Conflict (IPAC)).

Institute for Policy Research and Advocacy (ELSAM) & Privacy International, *The Right to Privacy in the Indonesia*, by Institute for Policy Research and Advocacy (ELSAM) & Privacy International, Stakeholder Report Universal Periodic Review 27th Session – Indonesia (Institute for Policy Research and Advocacy (ELSAM) and Privacy International, 2016).

Jalaludin Shofihara, Inang, "Cegah Terorisme, DPR Usul Wajibkan Pemasangan CCTV untuk Dapatkan IMB", (18 November 2019), online: *KOMPAS.com* <https://nasional.kompas.com/read/2019/11/18/16131121/cegah-terorisme-dpr-usul-wajibkan-pemasangan-cctv-untuk-dapatkan-imb>.

J Cockfield, Arthur, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" 40:1 UBC Law Review 2007.

J Daniels, Ronald, Kent Roach & Patrick Macklem, *The Security of Freedom: Essays on Canadian Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001).

Johnson, Mathew, "Privacy in the Balance - Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8" (2012) 58:3 Criminal Law Quarterly.

Kapoor, Kanupriya, "Indonesia to Add Hundreds of Counterterrorism Police to Monitor IS", (29 December 2017), online: *Reuters* <https://uk.reuters.com/article/uk-indonesia-security/indonesia-to-add-hundreds-of-counter-terrorism-police-to-monitor-is-idUKKBN1EN0WO>.

Kurnianingrum, Trias Palupi, "Arah Perubahan Undang-Undang Pemberantasan Tindak Pidana Terorisme" (2016) VIII:06 Info Singkat Hukum.

Lestari, Sri, "Ancaman Terorisme di Indonesia Masih Ada", (10 October 2012), online: *BBC News* <https://www.bbc.com/indonesia/laporan_khusus/2012/10/121010_lapsusterorism1>.

Lie Bernard, Luther, "Standards of Living and Planes of Living" (1928) 7:2 Social Forces.

Llobet Anglí, Mariona, "What does 'terrorism' mean" in Aniceto Masferrer & Clive Walker, eds, *Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of State* (Gloucestershire: Edward Elgar, 2013).

Martin Pratama, Akhdi, "Polisi Giatkan 'Cyber Patrol' Hadapi Maraknya Berita 'Hoax'", (30 December 2016), online: *KOMPAS.com* <https://megapolitan.kompas.com/read/2016/12/30/16255681/polisi.giatkan.cyber.patrol.hadapi.maraknya.berita.hoax.>.

Masferrer, Aniceto & Clive Walker, eds, *Counter-Terrorism, Human Rights and The Rule df Law: Crossing Legal Boundaries in Defence of State* (United Kingdom: Gloucestershire, 2013).

McGregor, "The Use of the Internet for Terrorist Purpose", (2012), online: *United Nations Office on Drugs and Crime Publication* <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>.

McGregor, Joan, "Liberalism and Democracy" (1988) 38:3 Philosophy East and West.

M Paciocco, David, "Constitutional Casualties of September 11: Limiting the Legacy of the Anti-Terrorism Act" (2002) 16 The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference.

N Leppington, Kristen, *Bill C-36: The Creation of Canada's 2001 Anti-Terrorism Act* (Master Thesis in Political Science, Laval University, 2011).

N Renke, Wayne, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy" (2006) 43:3 Alberta Law Review.

Paripurna, Amira, *The Use of Intelligence in Indonesian Counter-terrorism Policing* (PhD Dissertation, School of Law University of Washington, 2017) [unpublished].

——, "The Emergence of Proactive Intelligence Led Counterterrorism Policing and Surveillance in Post Suharto Indonesia" in Veronika Nagy & Klara Kerezsi, eds, *A Critical Approach to Police Science: New Perspective in Post Transitional Policing Studies* (Eleven, 2020).

——, Masitoh Indriani & Ekawestri Prajwalita Widiati, "Implementation of Resolution No. 4/2016 of the ICPO-INTERPOL Concerning Biometric Data Sharing: Between Countermeasures Against Terrorist Foreign Fighters (FTFS) and Protection of the Privacy of Indonesian Citizens" (2018) 5:1 Brawijaya Law Journal.

Penney, Steven, "National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits" 48:2 Osgoode Hall Law Journal 2010.

Purwanto, Heru, "RI Police Initiates ASEAN Cyber Patrol", (19 September 2017), online: *Antara News* <https://en.antaranews.com/news/112698/ri-police-initiates-asean-cyber-patrol>.

P Wiratraman, Herlambang & Sébastien Lafrance, "Protecting Freedom of Expression in Multicultural Societies: Comparing Constitutionalism in Indonesia and Canada" (2021) 36:1 Yuridika.

Sartor, Giovanni & Andrea Loreggia. *The Impact of Pegasus on Fundamental Rights and Democratic Processes*. European Union, 2022. Online: European Parliament <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf>.

SEN News, "Indonesia Plans 6000-Camera Public CCTV System For Jakarta", (1 July 2016), online: *SEN News* <https://sen.news/indonesia-plans-6000-camera-public-cctv-system-for-jakarta/>.

Quan Nguyen, Van et al, "Legal and Social Challenges Posed by the Social Credit System in China" (2020) 14:5 International Journal of Innovation, Creativity and Change.

Ratcliffe (ed), Jerry, *Strategic Thinking in Criminal Intelligence*, 1st edition ed (Sydney: The Federation Press).

R Henderson, C, "The Scope of Social Technology" (1901) 6:4 American Journal of Sociology.

Rahamim, Yoni, "Wiretapping and Electronic Surveillance in Canada: The Present State of the Law and Challenges to the Employment of Sophisticated and Intrusive Technology in Law Enforcement" (2004) 18 Windsor Rev Legal & Soc Issues 87.

Reem, Zaia, "Awakening Section 8 in Wakeling: Legal Implications on Wiretaps, Intercepts, Intelligence Sharing and Beyond" (2017) 50:1 UBC Law Review.

Roach, Kent, "Be Careful What You Wish For? Terrorism Prosecutions in Post-9/11 Canada" (2014) 40:99 Queen's LJ.

——, "Counter-Terrorism in and Outside Canada and in and Outside the Anti-Terrorism Act" (2012) 16:2 Review of Constitutional Studies/Revue d'études constitutionnelles.

Rucktäschel, Kathrin & Christoph Schuck, "Tracing Indonesia's Counterterrorism Measures Since the 2002 Bali Bombings", (4 September 2019), online: *The Diplomat* <https://thediplomat.com/2019/09/tracing-indonesias-counterterrorism-measures-since-the-2002-bali-bombings/>.

Ryani Cahya Kurnia B P, Gega, "Peran Kamera Pengawas Closed-Circuit Television (CCTV) dalam Kontra Terorisme" (2021) 9:4 Jurnal Lembaga Ketahanan Nasional Republik Indonesia 100–116.

Santoso, Topo, "Anti-Terrorism Legal Framework in Indonesia: Its Development and Challenges" (2013) 25:1 Mimbar Hukum.

Southeast Asia Freedom of Expression Network (SAFEnet). *Policy Brief: Evaluating the Implementation of the Personal Data Protection Law in Indonesia*. 2023. Online: <https://safenet.or.id/>.

Tan, Andrew, "Southeast Asia as the 'Second Front' in the War against Terrorism: Evaluating Threat and Responses" 15:2 Terrorism and Political Violence 2003.

Tehusijarana, Karina, "Tito TV: Minister Wants Face-Recognizing Surveillance Cameras, Says it Will 'Comfort' Public", (29 November 2019), online: *The Jakarta Post* <https://www.thejakartapost.com/news/2019/11/28/tito-tv-minister-wants-face-recognizing-surveillance-cameras-says-it-will-comfort-public.html>.

United Nations Office on Drugs and Crime, "Digest of Terrorist Cases", (2010), online: *United Nations Office on Drugs and Crime Publication* <https://www.unodc.org/documents/terrorism/Publications/Digest_of_Terrorist_Cases/English.pdf>.

UNODC, "E4J University Module Series: Counter-Terrorism", (2018), online: *United Nations Office on Drugs and Crime Publication*

<https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/surveillance-and-interception.htm>.

Utama, Lazuardi. "Mengenal Cyber Drone 9, Polisi Internet Indonesia". *VIVA.co.id* (3 January 2018). Online: <https://www.viva.co.id/digital/992995-mengenal-cyber-drone-9-polisi-internet-indonesia>.

——, "Special Investigative Techniques and Intelligence Gathering", online: *United Nations Office on Drugs and Crime* <https://www.unodc.org/e4j/en/organized-crime/module-8/key-issues/special-investigative-techniques/intro.html>.

Vatvani, Chandni, "In Indonesia, Extremists Finding Low-Tech Ways to Get Around High-Tech Blocks: Think Tank", (17 July 2018), online: *Channel News Asia* <https://www.channelnewsasia.com/news/asia/indonesia-extremists-low-tech-get-around-high-tech-10568864>.

Webb, Maureen, "Essential Liberty or a Little Temporary Safety - The Review of the Canadian Anti-terrorism Act" (2005) 53 51 Crim LQ.

Wesley Pue, W, "The War on Terror: Constitutional Governance in a State of Permanent Warfare" (2003) 41:2 & 3 Osgoode Hall Law Journal, online: <http://digitalcommons.osgoode.yorku.ca/ohlj/vol41/iss2/6>.

W Hefner, Robert, *Civil Islam: Muslims and Democratization in Indonesia* (Princeton: Princeton University Press, 2000).

Whitaker, Reg, "Keeping Up with the Neighbours: Canadian Responses to 9/11 in Historical and Comparative Context" (2003) 41:2/3 Osgoode Hall Law Journal.

Wispinski, Jennifer, *The USA Patriot Act and Canada's Anti-Terrorism Act: Key Differences in Legislative Approach* (The Library of Parliament of Canada, 2006).

Woude, Maertje van der, *Governing through Crises? Civil Liberties under Pressure* (School of Law BINUS University, 2020).

Yakti Widyastuti, Ariyani, "Halau Hoax, Polisi Gelar Patroli Siber Hingga ke Grup WhatsApp", (14 June 2019), online: *Tempo* <https://bisnis.tempo.co/read/1214686/halau-hoax-polisi-gelar-patroli-siber-hingga-ke-grup-whatsapp>.

Yusuf, Imtiyaz, ed, *Multiculturalism in Asia - Peace and Harmony* (Nakhorn Prathom: Mahidol University, 2018).

Acknowledgments

The author(s) gratefully acknowledges Auralia Rizki Putri for her careful research assistance and support provided in her capacity as a research assistant at the Faculty of Law.

This work was prepared separately from this author's employment responsibilities at the Public Prosecution Service of Canada. The views, opinions and conclusions expressed herein are personal to this author and should not be construed as those of the Public Prosecution Service of Canada or the Canadian federal Crown.

Amira Paripurna holds a doctoral degree (Ph.D.) from the University of Washington School of Law and a Master of Laws (LLM) on International Human Rights Law and Criminal Justice System at Utrecht University. She serves as an Assistant Professor in the Criminal Law Department at Universitas Airlangga's Faculty of Law and as Head of the university's Center for Anti-Corruption and Criminal Law Policy (CACCP). Her research focuses on policing, intelligence, counterterrorism, and human rights within criminal law and justice frameworks.

Sébastien Lafrance Sébastien Lafrance, Ph.D. h.c., LL.M., LL.B., B.Sc., Cert. (Chinese), Cert. (Turkish), has been a Crown Counsel (Prosecutor) for the Public Prosecution Service of Canada for more than thirteen years. He is an Honorary Professor at Tashkent State University of Law, Uzbekistan; an Adjunct Assistant Professor at Maqsut Narikbayev University, Kazakhstan; an Adjunct Professor at Universitas Airlangga, Indonesia; an Adjunct Lecturer at Ho Chi Minh City University of Law, Vietnam; and he was a Visiting Professor in 2023 at Jindal Global Law School, India. He has published a book, book chapters and articles in Australia, Brazil, Canada, France, India, Indonesia, Netherlands, the United Kingdom and Vietnam (in English, French and Vietnamese) on criminal law, constitutional law, public international law, civil law, competition law, artificial intelligence and the law, international trade law, energy law, and also labour law, one of which was awarded a national prize in Canada. This work was prepared separately from this author's employment responsibilities at the Public Prosecution Service of Canada. The views, opinions and conclusions expressed herein are personal to this author and should not be construed as those of the Public Prosecution Service of Canada or the Canadian federal Crown.

Masitoh Indriani is an academic staff member at the Department of International Law, Faculty of Law, Universitas Airlangga. Her academic focus lies in international law, privacy and data protection. She obtained her Bachelor of Laws (S.H.) from the Faculty of Law, Universitas Airlangga, and pursued her postgraduate studies at the School of Law, University of Leeds, United Kingdom. Masitoh has particular expertise in privacy and data protection issues, cybersecurity, and the development of legal and regulatory frameworks related to law and digitalization. In addition to teaching, she is actively engaged in research, academic publications, and opinion writing for national media. She

also frequently participates in academic forums, particularly those addressing data protection and legal challenges in the digital era.