

Submission in response to the Call for Input – Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism

1 September 2025

Professor Ben Saul, Special Rapporteur on Counter-Terrorism and Human Rights

By email only: hrc-sr-ct@un.org

Contact: Timothy Roberts

President, NSW Young Lawyers

Jessica Lighton

Submissions Lead, NSW Young Lawyers

Claudia Robinson

Human Rights Sub-Committee Chair, NSW Young Lawyers

Contributors: Claudia Robinson and Caity Suchanow.

The NSW Young Lawyers Human Rights Sub-Committee (**Sub-Committee**) makes the following submission in response to the Call for Input – Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism by the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism.

NSW Young Lawyers

NSW Young Lawyers is a Committee of the Law Society of New South Wales that represents the Law Society and its members on issues and opportunities arising in relation to young lawyers i.e. those within their first five years of practice or up to 36 years of age. Through its 12 sub-committees, each dedicated to a substantive area of law, NSW Young Lawyers supports practitioners in their professional and career development by giving them the opportunity to expand their knowledge, advance their career and contribute to the profession and community.

The Sub-Committee comprises a group of volunteers and subscribers interested in human rights law, including lawyers working in academia, for government, private and NGO sectors and other areas of practice that intersect with human rights law, as well as barristers and law students. The objectives of the Sub-Committee are to raise awareness about human rights issues and provide education to the legal profession and wider community about human rights and their application under both domestic and international law. Members of the Sub-Committee share a commitment to effectively promoting and protecting human rights and to examining legal avenues for doing so. The Sub-Committee takes a keen interest in providing comments and feedback on legal and policy issues that relate to human rights law and its development and support.

Summary of Recommendations

1. Adopt binding treaties and national legislation to regulate the use of AI in counter-terrorism, specifically including:
 - a. Prohibition on decisions made by AI without meaningful human oversight in the counter-terrorism context;
 - b. Mandatory Human Rights Impact Assessments before deploying AI for use in counter-terrorism, focusing on the human rights to privacy, non-discrimination, life, and due process; and
 - c. Clear accountability frameworks, assigning responsibility for rights violations in cross-border intelligence cooperation to both state and non-state actors.
2. Establish independent oversight mechanisms, both domestically in Australia and internationally, to review decisions that authorise the use of AI in counter-terrorism operations and provide redress where human rights have been violated.
3. Adopt multilateral standards for the use and exchange of AI-generated counter-terrorism data, with explicit safeguards for privacy and data protection.

Background on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism

Artificial intelligence (“AI”) is the capability of machines to perform tasks associated with human learning, reasoning, problem-solving, perception, and decision-making. In the counter-terrorism context, AI can enhance a State’s security capabilities by processing and rapidly analysing vast volumes of information.¹ There are recorded benefits to the use of AI in countering terrorism. For example, in the United States of America, the military employs AI to analyse drone surveillance data to detect terrorist movements and anticipate potential future movements.² Similarly, researchers at

¹ Serena Bianchi et al, “Artificial Intelligence to Counter Cyber-Terrorism” *Proceedings of the International Conference on Cybersecurity and Cybercrime* Vol. X (2023), 15.

² Boaz Ganor, “Artificial or Human: A New Era of Counterterrorism Intelligence?” *Studies in Conflict & Terrorism* (2019), 2.

the Computing Research Institute in Qatar analysed more than three million tweets over a three-month period and developed an AI algorithm that was able to detect Islamic State of Iraq and Syria (“ISIS”) opponents or supporters of ISIS with an 87% accuracy, and even predicted potential future recruits of ISIS.³

However, the application of AI in countering terrorism raises profound human rights concerns. The use of AI in counter-terrorism frequently involves surveillance overreach, inherent algorithmic bias, and a lack of transparency or accountability. Legal AI scholars caution that predictive uses of AI in this context are often ineffective, risky and inappropriate. Terrorism is not a regularly occurring event; attacks are relatively rare, and each case is highly context-specific. As a result, the limited datasets available can produce errors, over-generalisation, and false positives. Compounding these risks, there is no universally agreed definition of a “terrorist” or “terrorism”, which increases the likelihood of discrimination and human rights violations. While AI can enhance security by processing large datasets and identifying potential threats, its deployment also creates significant risks of overreach, bias, and human rights violations.

How does the use of artificial intelligence (AI) in countering terrorism affect human rights? Which rights are impacted? Which specific applications of AI in efforts to counter terrorism pose the greatest risks to human rights?

The use of artificial intelligence (AI) in counter-terrorism has profound implications for the protection and enjoyment of human rights. While States emphasise AI’s utility in preventing threats and enhancing national security, its application often occurs in ways that lack transparency, proportionality, and accountability. This creates a tension between legitimate security aims and international human rights obligations. The risks are particularly acute in relation to the rights to privacy, non-discrimination, the right to life and security, due process, and freedom from refoulement.

Right to Privacy

³ Boaz Ganor, “Artificial or Human: A New Era of Counterterrorism Intelligence?” *Studies in Conflict & Terrorism* (2019), 2.

An individual's right to privacy is one of the most directly impacted rights. AI enables mass surveillance and monitoring of individuals and groups. AI algorithms can analyse large amounts of data from social media, CCTV cameras, travel records, communications, and other sources to identify patterns and potential threats. Such large-scale data processing often occurs without adequate consent, human oversight, or proportionality, raising serious concerns regarding an individual's right to privacy. However, such approaches are often disproportionate, indefinite in scope, and highly susceptible to "function creep," where information gathered for one purpose is subsequently repurposed for broader surveillance activities. Individuals are rarely informed that their data is collected, nor given the opportunity to challenge its use. This undermines the internationally protected right to privacy under Article 17 of the International Convention on Civil and Political Rights ("ICCPR").

In Australia, the recently enacted Privacy and Other Legislation Amendment Bill 2024 (Cth) amended the Privacy Act 1988 (Cth) by introducing a statutory tort for serious invasions of privacy, enabling individuals to seek remedies for intrusions against their privacy. However, broad exemptions for intelligence and law enforcement agencies were also introduced, preventing any meaningful oversight when AI is utilised to counter terrorism, as this would be exclusively conducted by intelligence and law enforcement agencies. There is, to date, no public record of this new tort being invoked in a counter-terrorism or AI surveillance context, highlighting the absence of effective accountability mechanisms for individuals impacted by such practices.

Right to Non-Discrimination and Equality Before the Law

AI in counter-terrorism also poses a significant risk to the right to equality before the law and the right to non-discrimination. Algorithmic systems are only as neutral as the datasets on which they are trained. Where data reflects societal or institutional biases, these biases are reproduced and magnified in AI outputs. This is particularly concerning in the counter-terrorism context, where minority communities, such as ethnic, religious, and political minorities, are disproportionately subjected to profiling, surveillance, and policing. Predictive policing tools and AI-enabled facial recognition systems have repeatedly demonstrated higher error rates when applied to racial minorities, increasing the risk of wrongful suspicion, detention, or violence. Such discriminatory practices would undermine Articles 2 and 26 of the ICCPR, which guarantee equality before the law

and protection from discrimination. The use of AI in this manner also risks exacerbating marginalisation, distrust of state institutions, and social fragmentation, which may in fact undermine counter-terrorism objectives.

Right to Life and Security

The right to life and security is also impacted through the deployment of AI in military counter-terrorism operations. AI targeting systems, which are sometimes utilised in counter-terrorism operations by States, raises grave concerns if human control, accountability, and verification are insufficient. Additionally, the speed and complexity of AI decision-making may compromise adherence to the principles of distinction and proportionality under international humanitarian law. Failures in system accuracy or oversight could lead to the unlawful killing of civilians or misidentification of lawful targets. This raises serious concerns under Article 6 of the ICCPR, which protects the inherent right to life, and under Article 9, which prohibits arbitrary deprivation of liberty and security. States cannot and should not outsource these obligations to machines; human accountability and meaningful oversight remain indispensable safeguards.

Right to Due Process

The right to due process is also threatened by the overuse of AI models. AI is increasingly used to generate watchlists, conduct automated risk assessments, and determine outcomes in border security and migration management. Individuals may be denied entry, detained, or restricted in their movement on the basis of opaque algorithmic determinations, often without notification, explanation, or an opportunity to challenge the decision. Such practices undermine Article 14 of the ICCPR, which guarantees the right to a fair trial, Article 12, which protects freedom of movement, and Article 9, which safeguards against arbitrary detention. AI systems deployed in migration and asylum processes further raise the risk of breaches of the principle of non-refoulement under Article 33 of the Refugee Convention, as flawed risk assessments may wrongfully deny protection to legitimate asylum seekers. AI-powered watchlists and automated decisions in relation to border security and risk assessments may result in individuals being denied freedom of movement, detained, or restricted without notice or an opportunity to challenge the decision.

In light of these impacts, it is clear that the use of AI in counter-terrorism must be subject to far greater transparency, proportionality, and accountability than it is currently the case. States should ensure that AI systems are accompanied by robust safeguards, including independent and adequate human oversight.

Do existing guidelines, legislation and regulatory mechanisms currently in place prove effective in ensuring humans exercise meaningful oversight over the use of artificial intelligence in operations countering terrorism? In addition to existing international initiatives to regulate and govern AI, is there a need for any dedicated mechanism(s) relating to AI in counter-terrorism specifically?

International Guidelines

Existing guidelines in the international sphere around the responsible use of AI in countering terrorism are haphazard, contain many exemptions, are largely not legally binding, and often contain few remedies. As a result, “meaningful human oversight” is often overlooked by States that use AI in their counter-terrorism operations. The most relevant international agreement on counter-terrorism, the UN Global Counter-Terrorism Strategy,⁴ repeatedly affirms that counter-terrorism measures must respect human rights and the rule of law, but it does not prescribe concrete oversight architectures, audit duties, or redress pathways for AI-enabled practices; States retain wide discretion and the Strategy functions as a political commitment rather than a legally binding standard. Other UN initiatives, such as the UN Guiding Principles on Business and Human Rights⁵ and the Office of the High Commissioner for Human Rights’ recommendations on AI,⁶ set out general principles of accountability and transparency but stop short of requiring meaningful oversight in the specific context of counter-terrorism. This absence of enforceable international law leaves a significant regulatory gap, enabling governments to justify intrusive or discriminatory AI-driven surveillance and targeting under the broad and often vaguely defined mandate of “national security.”

⁴ UN General Assembly, *The United Nations Global Counter-Terrorism Strategy*, GA Res 60/288, UN GAOR, 60th sess, 72nd plen mtg, Agenda Item 46, UN Doc A/RES/60/288 (8 September 2006)

⁵ UN Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*, UN Doc A/HRC/17/31 (21 March 2011).

⁶ Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/48/31 (13 September 2021).

Consequently, millions of people may be subjected to human rights violations without effective safeguards or remedies, underscoring the urgent need for a dedicated mechanism to govern AI in counter-terrorism.

Australia-Specific Guidelines

Australia does not have any specific guidelines, legislation, or regulatory mechanisms that ensure meaningful human oversight in the use of AI to counter terrorism. Current regulation in this area consists primarily of voluntary AI ethics principles and some broader protections under the *Privacy Act 1988* (Cth); however, neither of these are tailored to the unique risks and responsibilities of utilising AI to counter terrorism.

The risks of inadequate oversight in Australia are illustrated by the Robodebt Scandal. In 2015, the Australian government announced the implementation of a new automated debt recovery scheme to recover debt owed to the Australian Social Security network, Centrelink. The scheme was given the name “**Robodebt**” by the public and media. The automated decision-making in debt recovery, absent any human checks, led to widespread errors, unlawful debts, and significant harm to vulnerable people.⁷ Although Robodebt was not a counter-terrorism programme, it demonstrates the harm that can occur when AI tools are utilised without proper oversight and when the onus is placed onto the individual to disprove the AI tool, as was the case with the Robodebt scheme.⁸ The risk of harm in counter-terrorism operations is even higher where automated decisions can restrict a person’s liberty, movement, and expression.

Existing international and domestic frameworks do not effectively ensure meaningful human oversight of AI in counter-terrorism operations. Australia, as well as the international sphere, requires specific, binding mechanisms to uphold human rights and ensure effective human oversight while countering terrorism with AI use.

⁷ Kai-Ti Kao, “From Robodebt to Responsible AI: Sociotechnical Imaginaries of AI in Australia” (2024) 10:3 *Communication Research and Practice* 387, 392.

⁸ Ibid.

What are the implications of cross-jurisdictional sharing of information arising from counter-terrorism efforts that exploit AI systems and their capabilities?

There is a very real need for States to coordinate counter-terrorism efforts, as the President of the European Commission highlighted that terrorists are not confined to state borders and counter-terrorism efforts would be at a significant disadvantage if operating in isolation.⁹ Cross-jurisdictional sharing of information generated through AI-enhanced counter-terrorism efforts has an array of implications. It can offer significant operational benefits, improved threat detection, faster data fusion, and cross-border coordination.¹⁰ However, it also raises profound human rights risks that must be addressed.

Firstly, privacy and data protection concerns are significant risks. AI-enabled surveillance systems often hinge on sensitive personal data. When such data is shared across borders, sometimes under minimal transparency or oversight, privacy rights can be severely undermined.¹¹ The rules and regulations on data protection vary among States, despite initiatives to standardise the management of information and data.¹² This makes cross-border cooperation difficult; without robust legal frameworks or independent oversight, individuals may face surveillance or restrictions without due process.¹³

Secondly, risks of discrimination and bias are amplified. AI systems used in predictive policing or threat scoring often rely on historical or heterogeneous data, making them susceptible to algorithmic

⁹ Privacy International, 'Unregulated Intelligence Sharing Poses Risks to Human Rights and to the Democratic Rule of Law' (21 November 2018) < [Unregulated intelligence sharing poses substantive risks to human rights and to the democratic rule of law | Privacy International](#) >

¹⁰ Europol, *AI and policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement* (Europol Innovation Lab Observatory Report, Publications Office of the European Union, Luxembourg, January 2025) ISBN 978-92-95236-35-6.

¹¹ United Nations, *Report of the Special Rapporteur on Contemporary forms of slavery, including its causes and consequences, Note by Secretary-General, UNGA, 78th Sess., Agenda item 73(b), UN Doc A/78/161* (12 July 2023), pg. 17, [42]. <[A/78/161](#)>.

¹² United Nations, *Report of the Special Rapporteur on Contemporary forms of slavery, including its causes and consequences, Note by Secretary-General, UNGA, 78th Sess., Agenda item 73(b), UN Doc A/78/161* (12 July 2023), pg. 17, [42]. <[A/78/161](#)>.

¹³ United Nations, *Report of the Special Rapporteur on Contemporary forms of slavery, including its causes and consequences, Note by Secretary-General, UNGA, 78th Sess., Agenda item 73(b), UN Doc A/78/161* (12 July 2023), pg. 17, [42]. <[A/78/161](#)>.

bias.¹⁴ When shared across jurisdictions, these biases can disproportionately affect marginalised groups beyond their original context, resulting in transnational profiling and wrongful targeting.¹⁵

Thirdly, accountability and oversight become highly complex in a cross-border environment. When data flows involve multiple jurisdictions with differing legal standards, tracing responsibility for rights violations can be difficult.¹⁶ The European Union has been considered a leader in digital rights, taking a precautionary approach to the use of AI, and there are strict obligations for ‘high-risk’ systems.¹⁷ However, the United States has taken a more innovation-driven approach, which varies depending on jurisdiction and industry.¹⁸ It is these types of disparities that cause friction in the sharing of information. This opacity weakens both oversight and remedy mechanisms, increasing the risk that unlawful or disproportionate acts go unchecked.¹⁹ Additionally, the unregulated space of intelligence sharing poses many risks, allowing governments to exchange information with little independent oversight.²⁰

Finally, sovereignty and normative divergence present further challenges. States have different approaches to data privacy, human rights, and counter-terrorism, making harmonised governance difficult. These disparities can erode democratic norms and enable authoritarian misuse of data shared in the name of security.²¹ Additionally, projects such as Project Nimbus, which involved Amazon and Google, have raised a range of concerns. This project, which was predominantly for

¹⁴ Jade Briend, ‘*The EU’s AI Act: Implications on Justice and Counter-Terrorism*’ (10 march 2025) Global Network on Extremism and Technology <[The EU’s AI Act: Implications on Justice and Counter-Terrorism – GNET](#)>.

¹⁵ Andrea Bianchi and Anna Greipl, *States’ Prevention of Terrorism and the Rule of Law: Challenging the ‘Magic’ of Artificial Intelligence (AI)*, International Centre for Counter-Terrorism, 17 November 2022. <[States’ Prevention of Terrorism and the Rule of Law: Challenging the ‘magic’ of Artificial Intelligence \(AI\) | International Centre for Counter-Terrorism - ICCT](#)>.

¹⁶ Oluwagbade, Elizabeth. (2025). *Accountability Without Borders: Cross-Jurisdictional Challenges in Regulating AI-Driven Decisions*, [2]- [3.3].

¹⁷ Oluwagbade, Elizabeth. (2025). *Accountability Without Borders: Cross-Jurisdictional Challenges in Regulating AI-Driven Decisions*, [2.1].

¹⁸ Oluwagbade, Elizabeth. (2025). *Accountability Without Borders: Cross-Jurisdictional Challenges in Regulating AI-Driven Decisions*, [2.2].

¹⁹ Oluwagbade, Elizabeth. (2025). *Accountability Without Borders: Cross-Jurisdictional Challenges in Regulating AI-Driven Decisions*, [2]- [3.3].

²⁰ Privacy International, ‘Unregulated Intelligence Sharing Poses Risks to Human Rights and to the Democratic Rule of Law’ (21 November 2018) <[Unregulated intelligence sharing poses substantive risks to human rights and to the democratic rule of law | Privacy International](#)>.

²¹ Jade Briend, ‘*The EU’s AI Act: Implications on Justice and Counter-Terrorism*’ (10 march 2025) Global Network on Extremism and Technology <[The EU’s AI Act: Implications on Justice and Counter-Terrorism – GNET](#)>.

providing cloud services to Israel, raised ethical concerns among employees due to its potential use in digital surveillance in Palestinian territories, exacerbating systemic discrimination.²²

To reduce the human-rights risks associated with cross-jurisdictional AI-driven information sharing, States and international bodies should mitigate these risks by:

- a. Adopting multilateral standards that regulate the use and exchange of AI-generated counter terrorism data, with explicit safeguards for privacy and data protection.
- b. Guaranteeing transparency and independent oversight, including the publication of data-sharing agreements and the involvement of Human Rights monitoring bodies.
- c. Developing harmonised human rights-based norms encouraging mutual recognition of minimum standards for lawful data use, regardless of divergent national counter-terrorism policies.
- d. Establishing and embedding accountability frameworks, making clear which actors, state or non-state, are responsible for rights violations in cross-border intelligence cooperation.

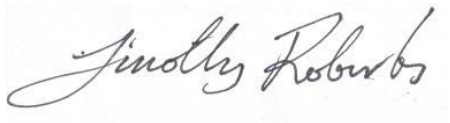
While cross-jurisdictional AI-enabled information-sharing is a potent tool in counter-terrorism, it must be carefully regulated to uphold human-rights principles across borders.

²² J. Bhuihan and B. Montgomery, 'A Betrayal: Google Workers protests Israeli military contract at vigil for ex-intern killed in airstrike', the Guardian, 1 December 2023.

Concluding Comments

NSW Young Lawyers and the Sub-Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions, please contact the undersigned at your convenience.

Contact:



Timothy Roberts

President

NSW Young Lawyers

Email: president@younglawyers.com.au

Alternate Contact:



Jessica Lighton

Submissions Lead

NSW Young Lawyers

Email: submissions.YL@lawsociety.com.au

Alternate Contact:



Claudia Robinson

Human Rights Sub-Committee Chair

NSW Young Lawyers

Email: hrsexecutive@gmail.com

Alternate Contact:



Caity Suchanow

International Law Sub-Committee Chair

NSW Young Lawyers

Email: nswylinternationalallawexec@gmail.com