GLOBAL CENTER
ON COOPERATIVE SECURITY

POLICY BRIEF

Human Rights Implications of the Use of New and Emerging Technologies in the National Security Space

By Annabelle Bonnefont
March 2024

Integrating new and emerging technologies, such as electronic surveillance, drones, unmanned aerial systems, biometrics, metadata analysis, artificial intelligence, and monitoring of online communications and social media, has become pivotal to modern national security strategies. Artificial intelligence (AI), in particular, has emerged as a cornerstone of innovation, revolutionizing how nations approach national security, counterterrorism, and public safety. Its ubiquity extends far beyond mere surveillance or data analysis; AI is now an indispensable tool across a spectrum of technologies, from electronic surveillance systems to unmanned aerial vehicles and biometric identification methods. While these technologies offer significant assistance to national security efforts, their use raises profound concerns about potential human rights violations, privacy violations, and the erosion of civil liberties, necessitating a careful examination of their implications. We not only have been witnessing the exploitation of new technologies by terrorist groups around the world to coordinate attacks, spread propaganda, and recruit new members, but we also must contend with states' use and misuse of these same tools under the auspices of national security. Striking a balance between national security imperatives and safeguarding individual rights and due process requires careful legislative, ethical, and technological considerations.

The International Covenant on Civil and Political Rights (ICCPR), adopted by the United Nations General Assembly in 1966, is a key international human rights treaty. Notable for its emphasis on civil and political liberties, the ICCPR outlines fundamental rights such as freedom of expression, religion, and assembly, as well as safeguards against arbitrary detention and torture. It remains a treaty of paramount importance, given its extensive ratification and comprehensive coverage of civil and political rights. While more than 170 UN member states have ratified the ICCPR—meaning that they have consented to be bound by the treaty—there are a few notable exceptions, such as China and Saudi Arabia. This policy brief will primarily reference the ICCPR as a framework for analyzing and addressing human rights concerns, acknowledging its place within the larger context of international human rights law.

Among the pivotal articles of the ICCPR, Article 17 protects individuals against the arbitrary interference with their privacy; Article 18 safeguards the freedom of thought, conscience, and religion; and Article 9 enshrines a person's

right to liberty and security. However, there are some narrow exceptions. Article 4 allows for certain rights to be restricted during a "public emergency threatening the life of the nation," but such derogations must be strictly necessary, proportionate, and temporary. The Article does not define what constitutes such emergencies, or their duration. Article 18 of the ICCPR also allows for exceptions to the freedom to manifest one's religion or beliefs under paragraph 3 in cases where it's necessary to "protect public safety."[1] The interpretation and application of these exceptions require vigilance to prevent government overreach.

In practice, the right to privacy, freedom of movement, and freedom of expression protected under the ICCPR are the rights that are often the first to be sacrificed in the name of protecting a state and its citizens. Exploiting ambiguities around national security concerns, authorities around the world engage in increased surveillance measures, impose restrictions on movement, censor free speech, and conduct systematic monitoring and data collection. Derogations that should be temporary under the ICCPR often serve as a pretext for prolonged and disproportionate infringements on civil liberties. This exploitation of Article 4 undermines the very principles the ICCPR seeks to uphold, stifling opposition voices, human rights defenders, journalists, and civil society actors, and thereby undermining democratic principles and human rights.

The rise and rapid expansion of new technologies and the exponential development of AI have only intensified the precarious balance between state sovereignty and individual rights. This policy brief examines the intricate human rights landscape related to the use of new and emerging technologies as part of efforts related to national security, counterterrorism, violent extremism, and public safety. It provides an overview of how different technologies are deployed in the context of national security and underscores the risks they present to human rights and fundamental freedoms protected in the ICCPR and echoed in domestic legislation. Drawing on national examples and case law, the brief concludes with reflections on areas in need of reform and highlights existing mitigation mechanisms that pursue a more equitable balance between national security imperatives and fundamental human rights.

CASE STUDIES ON THE INTERSECTION OF HUMAN RIGHTS AND NEW TECHNOLOGIES IN THE CONTEXT OF NATIONAL SECURITY

Through case studies and the examination of case law, this section aims to unravel the complexities surrounding the use of new and emerging technologies and offer insights into the delicate balance required to preserve both national security and the fundamental rights that form the cornerstone of democratic societies. It focuses on electronic surveillance, drones, metadata, biometrics, online communications, internet, and social media, including AI-powered technologies, and delves into how these technologies intersect with existing legal frameworks regarding privacy rights, freedom of movement, and due process rights.

ELECTRONIC SURVEILLANCE

Electronic surveillance is a broad term that covers any type of analog and digital information gathering. It encompasses both traditional wiretapping and monitoring of emails, social media profiles, digital cloud storage, drones or unmanned aerial systems, and the use of physical electronic trackers. Today, governments leverage AI-driven surveillance technologies to enhance their intelligence-gathering capabilities. This includes monitoring communications, tracking online activities, and utilizing facial recognition technologies to identify potential threats.

1 United Nations, "International Covenant on Civil and Political Rights," Office of the United Nations High Commissioner for Human Rights, accessed 28 January 2024, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

New and emerging technologies have reshaped the landscape of electronic surveillance, becoming powerful tools in the national security space. As AI continues to advance rapidly, it introduces unprecedented capabilities and complexities into surveillance, intelligence gathering, and counterterrorism efforts. However, the use of these technologies has a considerable impact on human rights, especially on the right to privacy as protected under Article 17 of the ICCPR. A spate of revelations[2] shows that such tools are being used to spy on politicians, journalists, human rights activists, lawyers, and ordinary citizens who pose no national security threat.[3] In addition, the mass utilization of AI-driven technologies like facial recognition risks erroneous and discriminatory identifications. The exponential deployment of AI for surveillance in public spaces raises concerns about the arbitrary monitoring of individuals, potentially infringing on their right to privacy.

The *Harun Causevic Case* in Australia (see box 1) provides a clear example of tensions over when electronic surveillance tactics can be deployed. Under Australian law, control orders (COs) grant the authority to electronically monitor suspects to "prevent the provision of support for or the facilitation of either a terrorist act or the engagement in a hostile activity in a foreign country."[4] COs are issued by a court following applications by the Australian Federal Police or the Australian Security Intelligence Organisation based on national security concerns and the need to prevent individuals from engaging in terrorist activities or supporting such activities. Since the enactment of the 2015 Counter-Terrorism Legislation Amendment Act (No 1) Bill (Cth), courts have been granted the authority to issue COs for the comprehensive surveillance and monitoring of individuals, enabling law enforcement agencies to conduct searches, intercept communications, and deploy surveillance equipment without demonstrating evidence of a potential terrorist threat or intelligence indicating terrorist activity.

Box 1. Case law: *R v. Causevic* [2016] VSC 321

Eighteen year-old Harun Causevic was arrested for an alleged connection to a planned terrorist attack on Melbourne Anzac Day in 2015.[a] He was released due to a lack of evidence after spending more than four months in a maximum-security prison. Subsequently, a CO required him to wear a GPS tracker.[b] Causevic faced restrictions on where he could worship and live, had a curfew implemented, saw his contact with friends and family limited, and experienced communications monitoring. The CO was criticized for infringing on his freedom of movement, expression, and privacy as protected under Articles 12, 17, and 19 of the ICCPR. Without sufficient evidence to bring a criminal case for his alleged terrorism connection, it was argued that the case did not qualify under the national security exemption provided for in paragraph 3 of Article 12.[c]

After nine months, a Federal Judge ultimately ordered the removal of Causevic's GPS tracker, citing a lack of evidence that Causevic was associated with terrorist activity. This case sparked discussions about counterterrorism measures and the legal process in Australia. Recognizing the

2 "The Pegasus Project," Forbidden Stories, https://forbiddenstories.org/case/the-pegasus-project.

3 Fionnuala Ní Aoláin and Adriana Edmeades Jones, "Spyware Out of the Shadows: The Need for a New International Regulatory Approach," Just Security, 16 May 2023, https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/#:~:text=Since%20the%20worldwide%20media%20investigation,human%20rights%20activists%2C%20lawyers%2C%20and.

4 Law Council of Australia, "Review of Police Stop, Search and Seizure Powers, the Control Order Regime and the Preventative Detention Order Regime to the Parliamentary Joint Committee of Intelligence and Security (PJCIS)," 3 November 2017, p. 4, https://lawcouncil.au/publicassets/7d6b1b91-a2c2-e711-93fb-005056be13b5/3365%20-%20PJCIS%20Stop%20Seach%20Seize%20COs%20and%20PDOs.pdf.

facts of the Causevic case and the danger of implementing such broad powers of surveillance, a review by the Law Council of Australia in 2017 proposed updates to the 2015 Counter-Terrorism Legislation Amendment Act (No 1) Bill (Cth), recommending narrower language that focused on acts that are "likely" rather than "capable" of occurring and, in those instances, where a "rational inference" can be drawn.[d] While some modifications have been made to the criteria for COs, the practice continues to be under scrutiny by civil society, the Australia Human Rights Commission, and the Law Council of Australia.[e]

a Law Council of Australia, "Review of Police Stop, Search and Seizure Powers, the Control Order Regime and the Preventative Detention Order Regime to the Parliamentary Joint Committee of Intelligence and Security (PJCIS)," 3 November 2017, p. 10, https://lawcouncil.au/publicassets/7d6b1b91-a2c2-e711-93fb-005056be13b5/3365%20-%20PJCIS%20Stop%20Seach%20Seize%20COs%20and%20PDOs.pdf..

b Tammy Mills, "Tracking Device Removed from Former Anzac Day Terror Plot Accused Harun Causevic," *The Age*, 9 July 2016, https://www.theage.com.au/national/victoria/tracking-device-removed-from-former-anzac-day-terror-plot-accused-harun-causevic-20160708-gq1m7l.html.

c Paragraph 3 of the article specifies that "The rights mentioned above shall not be subject to any restrictions except those that are deemed necessary to safeguard national security."

d Law Council of Australia, "Review of Police Stop, Search and Seizure Powers," p. 15.

e See generally, submissions made to the Parliament of Australia can be found at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofAFPPowers/Submissions, including the Australian Human Rights Commission Review of Australian Federal Police Powers dated 10 September 2020, and the Law Council of Australia Review of Federal Police Powers dated 17 September 2020.

In the United States,[5] numerous legal battles have shaped the contours of permissible surveillance activities. The United States established the Foreign Intelligence Surveillance Act (FISA) in 1978 to bring statutory order to electronic surveillance for law enforcement purposes to prevent abuse.[6] Following the events of 9/11, the Patriot Act notably broadened FISA's authority, allowing federal agents to conduct electronic surveillance without warrants on individuals considered "agents for foreign powers," under the guise of gathering foreign intelligence. This expansion has sparked debate about the potential for privacy violations, ultimately resulting in litigation over the constitutionality of warrantless surveillance under FISA (see box 2).

Attempts have been made to pull back the reigns on the FISA surveillance programs. For example, a 2022 Executive Order by President Joseph Biden imposed "limits on the conduct of signals intelligence collection by executive agencies, and also includes a redress mechanism under which individuals may seek review of alleged violations of, among other things, the US Constitution, FISA, or Executive Orders 12333 or 14086."[7] However, the broad contours of the program have remained intact. In December 2023, President Biden signed a reauthorization of the controversial program. The provision had been "slipped" into the yearly defense budget authorization bill, which funded not only U.S. government operations but also provided assistance for Ukraine and Israel.[8] Among others, a group of 20 US civil society organizations and think tanks decried the reauthorization, expressing their opposition to its inclusion in the defense bill without "robust debate," calling it a "blatant disregard for the civil liberties of the American people."[9]

5 The United States has not ratified the International Covenant on Civil and Political Rights (ICCPR), indicating a divergence in its stance on certain international human rights agreements.

6 See Edward Liu, "Reauthorization of Title VII of the Foreign Intelligence Surveillance Act," Congressional Research Service, 17 March 2023, pp. 4–5, https://crsreports.congress.gov/product/pdf/R/R47477 (it's one of several laws governing electronic surveillance for law enforcement purposes in the United States, the others being the Electronic Communications Privacy Act [ECPA] and Executive Orders 12333 and 14086). FISA works in conjunction with and is modified by all of the other laws, and as with the ECPA, can override it.

7 Liu, "Reauthorization of Title VII of the Foreign Intelligence Surveillance Act," pp. 7–8.

8 Tami Luhby, "Here's What's in the $886 Billion Defense Bill," CNN, 14 December 2023, https://www.cnn.com/2023/12/13/politics/ndaa-defense-bill-what-is/index.html.

9 Brennan Center for Justice, "Coalition Letter Urges Congressional Leaders to Keep Reauthorization of Section 702 Out of NDAA," 21 November 2023, https://www.brennancenter.org/our-work/research-reports/coalition-letter-urges-congressional-leaders-keep-reauthorization-section.

Box 2. Case law: *United States v. Muhtorov,* 20 F.4th 558, 581 (10th Cir. 2021)

In 2007, the United States National Security Agency (NSA) conducted warrantless surveillance on Jamshid Muhtorov, a legal U.S. permanent resident, capturing his emails and roughly 39,000 audio recordings before charging him in 2012 with providing material support to a designated foreign terrorist organization, the Islamic Jihad Union.[a] The government alleged that Muhtorov communicated with members of the organization, expressing his support and willingness to join them in their fight. Mr. Muhtorov's defense challenged the constitutionality of the surveillance methods used to gather evidence against him, arguing that they violated his Fourth Amendment rights guaranteeing the right to due process and protection from unreasonable searches and seizures.

Mr. Muhtorov was the first person ever to receive notice from the government that Section 702 had been used to spy on his communications. In a split decision in December 2021, the Tenth Circuit court of appeals ruled against Mr. Muhtorov, arguing that protecting the nation from foreign threats outweighed the due process concerns raised.[b]

A second point of tension emerges when governments cite national security concerns to conceal information about surveillance programs and procedures. In some instances (see Box 3), governments have denied individuals subject to surveillance access to the alleged evidence that would to be used against them in a criminal proceeding. The denials are made on the grounds of state security but effectively hinder citizens from challenging government intrusion. The outcome is the inclusion of innocent individuals and groups as surveillance targets, including legitimate civil society organizations, whose basic rights are violated despite the absence of any evidence linking them to terrorist activities.

a Summary of *United States v. Muhtorov*, ACLU, https://www.aclu.org/cases/us-v-muhtorov.
b *United States v. Muhtorov*.

Box 3. Case law: *Al-Haramain Islamic Foundation v. U.S. Treasury,* 660 F.3d 1019 (9th Cir. 2011)

In the *Al-Haramain Islamic Foundation v. Treasury* Case, the U.S. Treasury Department designated the Al-Haramain Islamic Foundation ("AHIF") as a supporter of terrorism in 2004 and froze its assets.[a] Lawyers for AHIF requested documentation to show why the organization was suspected to have terrorist ties.[b] The Office of Foreign Assets Control (OFAC) complied, and the response included a document marked top secret. It contained "a logbook of intercepted phone calls between the charity's lawyers in Washington DC and its clients in Saudi Arabia."[c] The subsequent lawsuit filed in 2006 asserts that the government intercepted conversations without a court order and thus, without probable cause—a requirement to obtain a FISA warrant.[d] The government response to this lawsuit was to demand that all copies of the logbook, a key piece of evidence in the case, be returned, asserting state secret privilege.[e] The District Judge tried to

balance the government's concerns with the constitutional rights of AHIF, but the government refused, citing the fact that the court should not be considering the legality of the NSA surveillance. The plaintiffs thus won the case by default.[f]

Electronic surveillance tactics are amplified through the deployment of other emerging technologies such as artificial intelligence. Protections for the right to privacy, freedom of assembly, freedom of association, and freedom of expression are weakened when surveillance is conducted by AI or other software programs monitored by nongovernmental parties. For example, third-party contractors engaged by the U.S. government are not subject to Freedom of Information Act (FOIA) requests, leaving their methods cloaked in secrecy (see box 4).

a *Al-Haramain Islamic Foundation v. Treasury*, 660 F.3d 1019 (9th Cir. 2011).
b Susan Herman, *Taking Liberties: The War on Terror and the Erosion of Democracy* (Oxford: Oxford University Press, 2011), pp. 180–84.
c Philip Shenon, "Lawyers Fear Monitoring in Cases on Terrorism," *New York Times*, 28 April 2008, https://www.nytimes.com/2008/04/28/us/28lawyers.html.
d Carol D. Leonnig and Mary Beth Sheridan, "Saudi Group Alleges Wiretapping by U.S.," NBC News, 2 March 2006, https://www.nbcnews.com/id/wbna11631768.
e Shenon, "Lawyers Fear Monitoring in Cases on Terrorism."
f Herman, *Taking Liberties*, p. 183.

Box 4. Case Study: ZeroFOX and the Department of Homeland Security

In 2016, two civil rights groups filed a Freedom of Information Act (FOIA) request to obtain information about the monitoring of Baltimore protestors by the Department of Homeland Security and its contractor ZeroFOX.[a] The request stemmed from various instances of government-funded surveillance of protests related to the Black Lives Matter movement, including government monitoring of protestors' social media accounts in Ferguson, Missouri; the Chicago Police Department's use of technology to eavesdrop on local protests; and monitoring of the aforementioned Baltimore protestors by ZeroFOX and the Department of Homeland Security.

ZeroFOX, which makes software that monitors social media accounts and other internet channels for potential cybersecurity threats, provided a 22-page report that evaluated Twitter and other social media platforms for potential cyber security threats and made recommendations to the Department of Homeland Security for securing information. On the fourth page, the report says that ZeroFOX recorded 19 "threats mitigated," and tallied up 340 real and fake social media accounts monitored. A section identifying "Threat Actors" included information about national Black Lives Matter protest leaders and local grassroots collectives that were using Twitter as a means of organizing and advocating against police brutality. These were labelled in the report as, "Threat Type: Physical."

The FOIA request yielded no results, as third-party contractors remain exempt from FOIA requests, preserving the veil of secrecy surrounding their surveillance methods. This outcome underscores the challenges of transparency and oversight when it comes to the activities of third-party contractors in surveillance and monitoring.

a Stephen Babcock, "ZeroFOX under Fire for Social Media 'Threat Actors' Report during Baltimore Riots—Technical.Ly Baltimore," Technically Baltimore, 4 August 2015, https://technical.ly/baltimore/2015/08/04/zerofox-fire-social-media-threat-actors-report-baltimore-riots.

THE USE OF DRONES

The increasing prevalence of drones or unmanned aerial systems (UAS) and AI-enabled drone operations in counterterrorism surveillance and local policing efforts have raised significant concerns. This is primarily due to the potential for arbitrary or unlawful interference with one's right to privacy, as underscored in Article 17 of the ICCPR. Today, drones are commercially available, relatively inexpensive, and can be operated via remote control or autonomously. Information technologies embedded in drones perform various data processing activities, including data collection, recording, organization, storage, and the combing of collected data sets. Depending on the quality of the data, it may be possible to identify individuals directly or indirectly.

The deployment of drones in counterterrorism surveillance and targeted intelligence operations raises serious concerns, particularly related to the collection of personal data and the monitoring of individuals without their consent (see Box 5). While both the U.S. Constitution and the ICCPR recognize the need to derogate the right to privacy in times of emergency or national security threats, the interpretation of this provision related to the use of drones to maintain public order remains unclear. For example, a recent report from the ACLU highlights the quick spread of policing via drones across the United States without a legal infrastructure in place to prevent abuse.[10] The lack of accountability regarding the use of drones will likely follow the same pattern that policing in general has followed over the last 20 years—becoming increasingly militarized and lacking important safeguards.[11]

Box 5. Case law: *Weber and Saravia v. Germany,* no. 54934/00, § 114, 29 June 2006; *Vissy v. Hungary,* no. 37138/14, § 54, ECHR 2016

Case law, such as the European Court of Human Rights' rulings in cases like *Weber and Saravia v. Germany* and *Szabo and Vissy v. Hungary,*[a] underscore the importance of safeguards against indiscriminate or disproportionate surveillance measures. These decisions ascertain that surveillance activities must be subject to effective oversight, judicial review, and proportionality assessments to ensure compliance with human rights standards.

In *Weber and Saravia v. Germany,* the applicants challenged the legality of Germany's data retention laws, which required telecommunications companies to retain the metadata of their customers' communications for a specified period. The applicants argued that this mass data retention violated their right to privacy under Article 8 of the European Convention on Human Rights (ECHR). *Vissy v. Hungary* concerned the legality of Hungary's legislation allowing for mass surveillance and data retention. The applicant alleged that Hungary's laws violated his rights to privacy and freedom of expression under Articles 8 and 10 of the ECHR.

In both cases, the court ruled in favor of the applicants, finding that Germany's and Hungary's data retention laws violated Articles 8 and 10 of the ECHR. The court held that the legislation failed to strike a fair balance between the legitimate aims of law enforcement and the protection of individuals' privacy rights.

a *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 114, 29 June 2006; *Szabó and Vissy v. Hungary*, No. 37138/14, § 54, ECHR 2016.

10 See generally, Jay Stanley, "Eye in the Sky Policing Needs Strict Limits," ACLU, 27 July 2023, https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits.

11 See Radley Balko, *Rise of the Warrior Cop: The Militarization of America's Police Forces* (New York: PublicAffairs, 2023).

UN Special Rapporteur on the right to privacy Joseph Cannataci has highlighted the need for clear legal frameworks and accountability mechanisms to regulate the use of drones in surveillance operations. In his reports to the UN General Assembly, Cannataci has emphasized the potential risks posed by mass surveillance technologies, including drones, to privacy rights and called for greater transparency, oversight, and accountability in their use.

The previous UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, also stressed the lack of human rights protections and enforcement regarding the use of drones, citing the fact that while there have been "attempts over the past decade to urge States to agree, adopt and abide by consistent standards" on the use of drones, very little progress has been made.[12] The incorporation of AI technology adds another layer of complexity to this endeavor. AI-driven drones can operate autonomously, raising concerns about accountability and transparency in decision-making processes. To create accountability, civil society actors around the world have been calling for comprehensive legislation on the use of drones domestically and in international conflicts, as well as for counterterrorism purposes. The rapid pace of technological advancement, particularly in AI, requires the continuous monitoring and adaptation of regulatory frameworks. Without proactive measures to address the intersection of AI and drone technology, there's a risk of falling behind in safeguarding privacy rights, human rights, and accountability in surveillance and counterterrorism efforts.

METADATA

Metadata is data about data—the information around a message (such as when, how, and where it was produced) without the content of the message itself.[13] It can be considered a sister to electronic surveillance, which directly targets the actual content of messages. Metadata has proven to be a useful tool for law enforcement in the post 9/11 world, often becoming the centerpiece of a counterterrorism investigation. With bulk metadata, government analysts can predict things like an individual's location in the immediate future, but also their locations months and years ahead of time.[14]

The use of metadata to effectively conduct mass surveillance raises concerns about the erosion of privacy rights and the chilling effect on free expression and association, as individuals may self-censor out of fear of being monitored or targeted for their political beliefs or affiliations. The method of metadata collection and storage raises further privacy concerns, as the data is repeatedly searched to identify patterns. While some argue that metadata is an essential tool for national security, Article 17 of the ICCPR addresses potential "unlawful" or "arbitrary" interference with individuals' "privacy, family, home or correspondence," prompting ongoing debates about the balance between security and individual rights. The growing reliance on private-sector technology firms poses further challenges related to accountability and transparency, blurring the lines between public and private entities in the pursuit of national security objectives.

In the United States, the government's collection of metadata began in 2006, when the Foreign Intelligence Service Court (FISC) authorized the collection of bulk telephony metadata under section 215 of the Patriot

12 Fionnuala Ní Aoláin, "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counterterrorism and Countering and Preventing Violent Extremism," 1 March 2023, p. 10, https://www.ohchr.org/en/documents/thematic-reports/ahrc5239-human-rights-implications-development-use-and-transfer-new.

13 International Committee of the Red Cross (ICRC) and Privacy International, "The Humanitarian Metadata Problem: 'Doing No Harm' in the Digital Era," 11 December 2018, p. 11, https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era.

14 Adam Sadilek and John Krumm, "Far Out: Predicting Long-Term Human Mobility," vol. 26, no. 1, Twenty-Sixth AAAI Conference on Artificial Intelligence, 2012, https://ojs.aaai.org/index.php/AAAI/article/view/8212.

Act.[15] This allowed U.S. intelligence authorities to collect petabytes of metadata information "relevant" to counterterrorism over 20 years, giving the government extensive information about those under monitoring.[16] The leak of classified documents by Edward Snowden revealed the extent of these measures, which included collecting information "indiscriminately and in bulk—regardless of whether [an individual] was suspected of any wrongdoing" (see Box 6).[17]

The United States is not alone in the collection of metadata for law enforcement purposes. In 2014, Australia updated its telecommunication interception laws to establish a mandatory metadata retention system in order to enhance the powers available to security agencies to combat "home grown terrorism and Australians who participate in terrorist activities overseas."[18] The program involves the collection and storage of data by telecommunications companies and

Box 6. Case law: The Snowden case

Edward Snowden is a former NSA contractor who leaked classified documents to journalists in 2013. The documents exposed the extensive scope of NSA surveillance programs, including the bulk collection of metadata from telecommunications and internet communications, and gave rise to concerns about privacy and violations of civil liberties. To avoid prosecution, Snowden fled the United States and sought asylum in Russia.

Snowden's disclosures sparked public outcry and led to policy reforms, such as the USA Freedom Act in 2015, which aimed to reform certain surveillance practices. The Act put restrictions on the bulk collection of data, requiring a "specific selection term" that "specifically identifies a person, account, address, or personal device in a way that limits the scope of information sought to the greatest extent reasonably practicable."[a] The Act also aims to ensure that information collected by the government for surveillance purposes was "appropriately focused and targeted,"[b] meaning that it was collected with specific purposes in mind and not gathered indiscriminately.

The notoriety of the Snowden case helped draw attention to the importance of the right to privacy as enshrined in international human rights instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

a Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, 6 June 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
b Ibid.

15 Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of The USA Patriot Act, 127 Harv. L. Rev. 1871, 2014, https://harvardlawreview.org/print/vol-127/administration-white-paper-bulk-collection-of-telephony-metadata.
16 Don Rassler, "Commentary: Data, AI, and the Future of US Counterterrorism: Building an Action Plan," Combating Terrorism Center at West Point, October 2021, https://ctc.westpoint.edu/commentary-data-ai-and-the-future-of-u-s-counterterrorism-building-an-action-plan.
17 Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, 6 June 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
18 Transcript of joint press conference: Parliament House, Canberra: 5 August 2014: New Counter-Terrorism Measures for a Safer Australia; Racial Discrimination Act; Malaysia Airlines Flight MH17; baby Gammy, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/3320720/upload_binary/3320720.pdf;fileType=application%2Fpdf#search=%22media/pressrel/3320720%22.

internet service providers for two years and makes that data available to government agencies upon request.[19]

The Benbrika case (see Box 7) highlighted the use of intercepted communications and metadata as evidence in counterterrorism prosecutions and raised questions about the balance between national security concerns and civil liberties, particularly regarding the use of surveillance and intelligence-gathering techniques in counterterrorism efforts.

Concerns about who can access data are not limited to domestic authorities. Data from one country is often readily shared with others in the name of counter-terrorism cooperation. For example, in its 2020 data strategy, the U.S. Defense Department "recognizes that data is a strategic asset that must be operationalized to provide a lethal and effective Joint Force" consisting of a network of allies and partners.[20] The Snowden revelations also underscored the extensive cooperation and intelligence-sharing among intelligence agencies of the Five Eyes partners—the United States, the United Kingdom, New Zealand, Canada, and Australia.[21]

The fact that each country has its own privacy standards complicates how data is shared, protected, and utilized. For example, the Australian government cannot guarantee to its citizens that the United States will adopt the same strict standards employed by Australian agencies in the exchange and storage of their metadata.[22] Per former Special Rapporteur Fionnuala Ní Aoláin, "global counter-terrorism cooperation rhetoric

Box 7. Case law: *R. v. Benbrika & Ors,* (Ruling No 20) [2008] VSC 80, 20 March 2008

Abdul Nacer Benbrika was the alleged leader of a group of men accused of plotting terrorist attacks in Melbourne, Australia. The group's activities came to the attention of Australian authorities, who conducted extensive surveillance and monitoring of their communications.

During the trial, prosecutors presented evidence obtained through surveillance, including intercepted phone calls, emails, and other communications. Metadata, such as information about the timing and duration of communications, was likely used to establish connections between the defendants and their alleged activities. The prosecution's reliance on surveillance evidence in the Benbrika case raised questions about the balance between national security imperatives and civil liberties. The case prompted discussions about the appropriate limits on government surveillance powers and the need for robust oversight mechanisms to prevent abuses.

While Abdul Nacer Benbrika and five of his associates were found guilty, concerns were raised regarding the lack of balance between the need to protect national security interests with the defendant's right to a fair trial, particularly when it involves classified intelligence sources or methods. This case highlighted the importance of establishing procedures for handling classified information in legal proceedings while safeguarding defendants' rights.

19 Rick Sarre, "Metadata Retention as a Means of Combatting Terrorism and Organized Crime: A Perspective from Australia," *Asian Journal of Criminology*, DOI 10.1007/s11417-017-9256-7, September 2017, pp. 2-6, https://www.researchgate.net/profile/Rick-Sarre/publication/318911383_Metadata_Retention_as_a_Means_of_Combatting_Terrorism_and_Organised_Crime_A_Perspective_from_Australia/links/59aff4afaca272037079125f/Metadata-Retention-as-a-Means-of-Combatting-Terrorism-and-Organised-Crime-A-Perspective-from-Australia.pdf.

20 Rassler, "Data, AI, and the Future of US Counterterrorism."

21 Sarre, "Metadata Retention as a Means of Combatting Terrorism."

22 Ibid. p. 6.

is defined by a rhetorical illusion that all states value privacy equally; do not misuse information to target individuals outside the rule of law; and that information practices including integrity, anonymity, destruction as appropriate are rule of law based."[23]

Cooperation and data sharing between governments also raises questions as to how and when states may be liable under national and international law for their surveillance activities, which may have an impact far beyond their own borders. One issue is the extent to which states can be "extraterritorially" accountable for their human rights violations overseas, e.g., the surveillance of private communications in other countries.

BIOMETRICS

Governments around the world are increasingly investing in biometric and facial recognition technologies (FRTs) to bolster their counterterrorism and national security capabilities. The collection of biometric and other data has been elevated in the UN Security Council as a critical means to combat terrorism, and member states have been called on to share and pool their data.[24] Biometric data consists of uniquely identifying biological characteristics like iris patterns, a person's gait, voice recognition, or fingerprints.[25] It is further defined by the European Union as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person."[26] Biometrics are commonly used in everyday life: mobile phones with facial scan technology and voice recognition, and smartwatches that can track heart rate, temperature, blood pressure, blood oxygen, etc. With the rapid expansion of AI, governments, the private sector, and other actors now have the capacity to analyze biometric data such as facial recognition, fingerprints, and iris scans with unprecedented accuracy and speed.

The advent of biometric systems—enhanced by AI—has sparked apprehension concerning their potential misuse and violation of ICCPR articles, notably Article 17, which safeguards the right to privacy, and Article 9, which protects against arbitrary detention. These concerns are underscored by concrete instances of abuse. For instance, biometric systems powered by AI such as facial recognition systems, while touted for their efficiency, have been found to exhibit biases, perpetuating discrimination against marginalized communities, which contravenes Article 26 of the ICCPR on ensuring equality before the law. Inaccurate identifications stemming from flawed algorithms or inadequate training data have led to wrongful detentions, a violation of Article 9 of the ICCPR. Moreover, the susceptibility of biometric data to breaches and spoofing techniques jeopardizes individuals' privacy rights as enshrined in Article 17 of the ICCPR. With the increasing use of this technology in everyday life, states will need to keep pace with regulations and human rights implications for its use by the public and private sectors.

Case studies from various countries reveal a trend of implementing biometric systems and FRTs in public spaces, airports, and other critical infrastructure, ostensibly to identify and track potential threats (see Box 8–10).

23 Ibid. pp. 18–19.

24 United Nations, "CTED Analytical Brief: Biometrics and Counterterrorism," UNSC CTED, 2020-2021, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf. See also UNSC Counter-Terrorism Committee, "CTC Holds Open Briefing on the Work of CTED with Member States of South and South-East Asia Pursuant to Security Council Resolution 2395, 2017," https://www.un.org/securitycouncil/ctc/news/ctc-holds-open-briefing-work-cted-member-states-south-and-south-east-asia-pursuant-security.

25 Katja Lindskov Jacobsen, *Biometric Data Flows and Unintended Consequences of Counterterrorism*, International Review of the Red Cross (2021), pp. 619–52, https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-02/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916.pdf.

26 Ibid., citing European Union, General Data Protection Regulation, Regulation (EU) 2016/679, 27 April 2016, OJ L 119, 4.5.2016, pp. 1–88, Art. 4(14).

Box 8. Case study: The National Facial Biometric Matching Capability

In September 2015, Australia unveiled a new biometric counterterrorism tool, the National Facial Biometric Matching Capability.[a] The tool is meant to be utilized by Commonwealth agencies as an image-based verification to help establish identity for law enforcement.[b] However, during the COVID pandemic, it was used as a "police check" to ensure that anyone diagnosed with COVID remained at home or in quarantine.[c] This expanded use of the tool raised significant privacy and civil liberties concerns among the Australian public. The government's utilization of biometric data for public health enforcement without sufficient safeguards and oversight prompted calls for legislative action to address these concerns.

In early December 2023, Australia passed the Identity Verification Services Bill to provide safeguards, oversight, and transparency over the use of the tool, including by requiring express consent and requiring the government to comply with privacy laws and obligations to protect personal data.[d]

a Parliament of Australia, "New $18.5 Million Biometrics Tool to Put a Face to Crime," 9 September 2015, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4064462%22.
b Ibid.
c Jessica Mudditt, "The Nation Where Your 'Faceprint' Is Already Being Tracked," BBC.com, 23 June 2022, https://www.bbc.com/future/article/20220616-the-nation-where-your-faceprint-is-already-being-tracked.
d The Hon Mark Dreyfus KC MP, "Delivering Strong Safeguards for Identity Verification Services," 7 December 2023, https://ministers.ag.gov.au/media-centre/delivering-strong-safeguards-identity-verification-services-07-12-2023#:~:text=Parliament%20has%20today%20passed%20legislation,to%20identity%20fraud%20and%20theft.

Box 9. Case study: United States, Secure Electronic Enrollment Kit (SEEK)

As part of the "global war on terror," the United States collected biometric data of the populations in Afghanistan and Iraq—not just the data of suspected criminals, but also of "citizens who have never been accused of any wrongdoing."[a] Per the U.S. Army, biometric data is used as an identification tool to help identify adversaries who disguise their identities through name changes and changes to their physical appearance.[b] In the field, American soldiers would use the Secure Electronic Enrollment Kit (SEEK) to scan an individual's biometrics and compare it to the information already stored to identify them.[c] Biometric data was gathered through a variety of methods, including from detainees and local residents applying for government jobs, military positions, or to work at American installations.[d] Fingerprint data could also be lifted from defused bombs or debris after a blast to help identify perpetrators.[e]

In 2007, human rights organizations estimated that the database of biometric information collected in Iraq contained approximately 750,000 records, including fingerprints, photographs, and iris scans.[f] By 2019, the U.S. military had gathered biometric data from 7.4 million people.[g] A likely contributor to this increased volume of data were humanitarian organizations that were encouraged to use biometrics in conjunction with aid delivery, resulting in a system where aid became conditional on giving up personal biometric information.[h] This kind of conditional

transaction raises questions of informed consent and implications of refusal[i] and may contradict the humanitarian principles of neutrality and impartiality.

a Krisztina Huszti-Orban and Fionnuala Ní Aoláin, "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?," Human Rights Center, University of Minnesota, 2020, p. 7, https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf.
b Jacob Kohrs, "Army Unveils New Army Biometric Program Directive," Army News Service, 15 November 2022, https://www.army.mil/article/262016/army_unveils_new_army_biometric_program_directive.
c Martin Zwanenburg, "Know Thy Enemy, The Use of Biometrics in Military Operations and International Humanitarian Law," *International Law Studies* vol. 97, 2021, p. 1405, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2986&context=ils.
d Katja Lindsokov Jacobsen, "Biometric Data Flows and Unintended Consequences of Counterterrorism," International Review of the Red Cross, no. 916–917 (2022), pp. 619–52, https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916.
e Ibid.
f Ibid. p. 6.
g Ibid.
h Huszti-Orban and Aolain, "Use of Biometric Data to Identify Terrorists," p. 7.
i Ibid., citing Dragana Kaurin, "Data Protection and Digital Agency for Refugees," World Refugee Council Research Paper no. 12, Center for International Governance Innovation, 15 May 2019, https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

Box 10. Case study: United Nations' use of biometrics

The United Nations has been using biometric data tools in Afghanistan since 2002, when the United Nations High Commissioner for Refugees (UNHCR) implemented mandatory iris scans for Afghan refugees[a] and continues to use it as a tool for identification, notably in Somalia. In some cases, the United Nations has engaged contractors to access the more isolated areas of Somalia, which enabled them to bypass some UN security regulations.[b]

The United Nations also implemented Security Council Resolution 2396, which imposes a binding obligation to develop biometric capabilities without a requirement to share the compiled data.[c] Unfortunately, this resolution fails to address any international law or human rights implications of biometrics and data sharing.[d] The omission of specific directives on human rights law in the resolution does not signal that states' obligations under the ICCPR can be ignored, as there is still an expectation that states will take measures to protect basic rights. But the lack of attention given to basic freedoms as defined by the ICCPR in this resolution—although implied—signals that there is no appetite among the member nations to implement specific regulations addressing these issues, as there is a benefit to having the flexibility to search, store, and utilize the data as needed.

a Jacobsen, "Biometric Data Flows and Unintended Consequences of Counterterrorism," 627.
b Ibid., p. 631.
c Huszti-Orban and Aoláin, "Use of Biometric Data to Identify Terrorists," p. 11.
d Ibid.

There have been indications of troubling biometric surveillance practices in relation to civil liberties and due process rights. For example, the Federal Bureau of Investigation (FBI) notably claimed that it does not need to demonstrate probable cause of criminal activity before employing FRTs, raising significant questions about unchecked government surveillance.[27] FBI witnesses in another hearing were unable to confirm whether the agency fulfills its constitutional obligations to inform criminal defendants when the technology identifies them.[28]

The FBI also has a history of utilizing biometric data to monitor civil society groups, ranging from racial justice movements to environmental activists. This raises serious concerns about the targeting of dissent and legitimate protest activities.[29] Similarly, investigations into climate justice activists, including 350.org and the Standing Rock water protectors, under the guise of national security highlight the misuse of surveillance powers to suppress political dissent and silence voices advocating for social and environmental justice.[30] The DOJ has refused Freedom of Information Act requests regarding its use of facial recognition and other biometric surveillance technologies (see Box 12). Failure to notify individuals subjected to facial recognition technology in criminal cases represents a fundamental breach of due process rights.

In addition to the impact on civil liberties, numerous studies underscore the challenges with biometric technology itself, including bias in programming, error rates, fraud, software issues, false matches, data breaches, and data poisoning. AI and machine learning algorithms can exacerbate this issue if not carefully designed and monitored. FRTs can be vulnerable to spoofing—where an individual uses a prosthetic or other device to hide their features—and is also susceptible to environmental conditions such as lighting.[31] Fingerprinting is the least reliable type of biometric surveillance and has the highest rate of error.[32] Two samples of the same person's index finger could produce anomalies due to issues such as cuts on the person's finger, whether their hands are dry, temperature, humidity, and how the person places their finger on the sensor.[33] A peer-reviewed study conducted by researchers at the Massachusetts Institute of Technology revealed that facial recognition technology has the potential to misclassify the faces of dark-skinned women up to 35 percent of the time.[34] Another study found that "emotion recognition" software tended to depict Black men as exhibiting higher levels of anger and contempt compared to their white counterparts,[35] while other researchers discovered that facial surveillance algorithms exhibit discriminatory behavior against transgender and gender nonconforming individuals.[36]

Further challenges emerge when exploring algorithmic "training data." While AI plays a crucial role in reducing error rates through continuous learning and adaptation, inadequate training data or insufficient algorithm refinement can result in higher error rates.

27 Neema Singh Guliani, "The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database," ACLU, 10 June 2019, https://www.aclum.org/en/publications/fbi-has-access-over-640-million-photos-us-through-its-facial-recognition-database.

28 Kade Crockford, "The FBI is Tracking Our Faces in Secret. We're Suing," ACLU, 31 October 2019, https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing.

29 Chip Gibbons, "Still Spying on Dissent: The Enduring Problem of FBI First Amendment Abuse," Defending Rights and Dissent, 2019, https://www.rightsanddissent.org/fbi-spying.

30 Alice Speri, "The FBI Spends a Lot of Time Spying on Black Americans," The Intercept, 29 October 2019, https://theintercept.com/2019/10/29/fbi-surveillance-black-activists.

31 "Biometrics: Friend or Foe of Privacy?" Privacy International, 13 December 2013, https://privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy.

32 Ibid.

33 Zwanenburg, "Know Thy Enemy," p. 1409.

34 See MIT's Gender Shades Project, https://www.media.mit.edu/projects/gender-shades/overview.

35 Lauren Rhue, "Racial Influence on Automated Perceptions of Emotions," SSRN, 9 November 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.

36 Matthew Gault, "Facial Recognition Software Regularly Misgenders Trans People," Vice.com, 19 February 2019, https://www.vice.com/en/article/7xnwed/facial-recognition-software-regularly-misgenders-trans-people.

Even where discrimination is not intended, indirect discrimination can result from policies, practices, or criteria, which, while not intentionally discriminatory, disproportionately disadvantage certain groups based on characteristics such as race or ethnicity.[37] The former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism raised concerns about "inaccurate/discriminatory algorithmic decision-making"[38] or, as researcher Tarcízio Silva called it, "algorithmic racism," which cites the fact that "development of algorithmic technologies feeds on social history to offer alleged artificial intelligence"[39] and does not take into consideration the variety of nuances that human bodies have.

Despite the normalization of biometric technology in everyday life, accountability remains an issue. Former Special Rapporteur Fionnuala Ní Aoláin has expressed concerns about the collection of biometric data, as well as the retention period of that data, and the non-disclosure of any data-sharing agreements between agencies of different nations.[40] These are the same concerns raised by a number of humanitarian organizations with regard to all biometric data-gathering programs (see Box 12–13).

Box 12. Case law: *ACLU v. Department of Justice* - FOIA Lawsuit (ongoing)

The FOIA is a federal law that allows for the full or partial disclosure of previously unreleased information and documents controlled by the U.S. government. It aims to promote transparency by enabling individuals to request access to government records. However, agencies can withhold information under specific exemptions outlined in the FOIA, such as those concerning national security or personal privacy.

In May 2018, the American Civil Liberties Union (ACLU) filed a Request Under the Freedom of Information Act against the Department of Justice, the Drug Enforcement Administration, and the FBI, seeking disclosure of documents related to the DOJ's use of facial recognition and other biometric surveillance technologies. In their request, the ACLU argued that the DOJ was not sufficiently transparent about its use of facial recognition technology, which raised significant concerns regarding privacy, civil liberties, and potential biases. The ACLU sought to obtain information about the DOJ's policies, procedures, and practices related to facial recognition technology, as well as any agreements or collaborations with other agencies.[a]

The outcome of the case could have significant implications for government transparency, the regulation of facial recognition technology, and the protection of civil liberties. It underscores the ongoing debate over the balance between security and privacy in the digital age and highlights the importance of robust oversight mechanisms to ensure accountability and safeguard fundamental rights.

a *ACLU v. DOJ* - FOIA Request on Social Media Surveillance: Freedom of Information Act Request for Records on Federal Agencies' Monitoring of Social Media, 24 May 2018, https://www.aclu.org/legal-document/aclu-v-doj-foia-request-social-media-surveillance.

37 E. Tendayi Achiume, "Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis," Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 18 June 2020, p. 3.

38 Kelley Sayler, "Biometric Technologies and Global Security," Congressional Research Service, 30 January 2023, https://crsreports.congress.gov/product/pdf/IF/IF11783.

39 Daiane Batista and Tarcízio Silva: "Algorithmic Racism Is a Kind of Update of Structural Racism," Fiocruz Strategic Studies Center, 30 March 2023, https://cee.fiocruz.br/?q=Tarcizio-Silva-O-racismo-algoritmico-e-uma-especie-de-atualizacao-do-racismo-estrutural.

40 Aoláin, "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counterterrorism and Countering and Preventing Violent Extremism."

Box 13. Case study: UN's Countering Terrorist Travel Programme

The United Nations Countering Terrorist Travel ("CT Travel") Programme is an initiative of the United Nations Office of Counter-Terrorism (UNOCT). Its objective is to assist beneficiary Member States with building their capabilities to use the Advance Passenger Information (API) and Passenger Name Record (PNR) data of known and suspected terrorists and criminals and enhance international information exchange, in accordance with Security Council resolutions 2178 (2014), 2396 (2017), and 2482 (2019), international standards, and recommended practices and human rights principles.[a] The CT Travel programme's goal is to enhance border security measures through the deployment of cutting-edge technologies such as biometric identification systems, advanced screening procedures, and real-time data-sharing platforms, with the goTravel Software Solution at its core. This biometric identification system uses biometric data such as fingerprints, facial recognition, and iris scans to accurately identify and verify individuals crossing borders.

The lack of regulation around data collection and retention, non-disclosure agreements, and oversight for the CT Travel Programme raises concerns about the potential for misuse.[b] The extensive use of biometric data and advanced surveillance technologies raises legitimate fears about potential infringements on individuals' privacy. Critics emphasize the risks associated with the United Nations embracing and disseminating specific technologies without adequate consideration for human rights safeguards. Such actions by the United Nations could inadvertently contribute to a global landscape where technological advancements are wielded without proper ethical oversight, potentially undermining fundamental freedoms and rights. The broad authority granted to border security agencies under the program could also lead to overreach and abuse, resulting in discriminatory profiling and unwarranted surveillance. Furthermore, the lack of transparency and accountability mechanisms within the program exacerbates these concerns, making it difficult to assess the extent to which human rights are safeguarded in its implementation.

In a Position Paper on the United Nations CT Travel Programme and the goTravel Software Solution, the former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism called for an independent audit of the program, which is a remedy that could be applied across a spectrum of data collection programs.[c] An independent auditor could ensure compliance with ICCPR standards of the right to privacy, freedom of expression, and, in the case of this specific UN program, the freedom of movement.

a UN Countering Terrorist Travel Programme, https://www.un.org/cttravel.
b Ibid.
c Position Paper of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism Fionnuala Ní Aoláin on the United Nations Countering Terrorist Travel ("CT Travel") Programme and the goTravel Software Solution, 30 October 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf.

INTERNET AND SOCIAL MEDIA

The rapid proliferation of social media use worldwide has ushered in an era where digital platforms serve as arenas for communication, activism, and information dissemination. Over 70 percent of U.S. adults are estimated to have used social media in 2021, versus 5 percent in 2005.[41] A 2022 Australian estimate found that 82.7 percent of the population had active social media accounts.[42] Due to the escalating use of social media by people of all ages and demographics, it has also become a tool for law enforcement to disseminate information. For example, social media was used by law enforcement to communicate with the public immediately after the Boston Marathon bombing[43] and in the investigation and identification of many of the January 6th perpetrators by the U.S. Government.[44]

However, alongside the benefits of communication, there exists a pervasive concern regarding the potential abuses of social media surveillance and censorship. These abuses encompass violations of privacy rights, the targeting of specific groups, misinterpretation of content, government overreach, and censorship of dissenting voices. Such practices not only undermine fundamental human rights principles but also raise significant legal and ethical questions. In the context of international human rights standards, these abuses intersect with the principles outlined in the ICCPR, particularly Articles 17 on the Right to Privacy, 19 on Freedom of Expression, and 22 on Freedom of Association.

While social media platforms and the internet have been tools used to fuel far-right radicalization in the West,[45] they have also been serving as vast sources of information for intelligence agencies.[46] AI-powered tools can sift through enormous amounts of data, extracting valuable insights, patterns, and trends that can aid in identifying potential threats, monitoring adversarial activities, and understanding public sentiment. Today, law enforcement's monitoring of social media remains largely unregulated and activists, journalists, protestors, and human rights organizations have all been surveilled by law enforcement via social media. Per the Brennan Center, "[l]aw enforcement can, with little effort, learn the personal beliefs, location and associations of large swaths of the population and actively track their online activities without having to justify whom they're watching, or why."[47]

Box 14. Case study: Australia, Surveillance Legislation Bill, 2021

Australia enacted the Surveillance Legislation Amendment (Identify and Disrupt) Bill in 2021, granting the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) the authority to obtain data disruption warrants,[a] network activity warrants,[b] and account takeover warrants.[c] In the first year of implementation (2021), these warrants were applied at least six times,[d] with three additional warrants sought and granted in 2022–2023 for child

41 Kristin Finklea, "Law Enforcement and Technology: Using Social Media," Congressional Research Service, 11 January 2022, p. 1, https://crsreports.congress.gov/product/pdf/R/R47008.

42 Australian Human Rights Commission, "Social Media: A Tool for Foreign Interference," 2 August 2023, https://humanrights.gov.au/about/news/social-media-tool-foreign-interference.

43 Finklea, "Law Enforcement and Technology: Using Social Media," p. 2.

44 Ibid., p. 1.

45 Global Internet Forum for Counter Terrorism, APRWG White Paper: Extremism Research Horizons, January to June 2021, https://gifct.org/wp-content/uploads/2021/07/GIFCT-APRWG-WhitePaper.pdf.

46 Ibid.

47 Gabriella Sanchez and Rachel Levinson-Waldman, "Police Monitoring Chills Activism," Brennan Center for Justice at New York University School of Law, 18 November 2022, https://www.brennancenter.org/our-work/analysis-opinion/police-social-media-monitoring-chills-activism.

abuse offenses.[e] The warrants target serious offenses such as drug crimes, weapons offenses, money laundering, and criminal association.[f] Law enforcement argues that the warrants are necessary due to the inadequacy of previous methods in addressing threats from the "dark web" and artificial intelligence.[g] However, concerns have been raised about the potential misuse of surveillance powers and its impact on privacy. The Office of the Australian Information Commissioner (OAIC) notes that while the bill requires magistrates to consider privacy in account takeover warrants, no such requirement exists for data disruption and network activity warrants, potentially allowing law enforcement to gather significant information without adequate privacy safeguards.[h]

a Per the Australian Government, Department of Home Affairs page, "Allow the disruption of data through modification and deletion of data to frustrate the commission of serious offences, such as the distribution of child abuse material." See https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-act-2021.

b Ibid. ("Allow the collection of intelligence on serious criminal activity carried out by criminal networks operating online.")

c Ibid. ("Allow the control of a person's online account to gather evidence about criminal activity to further a criminal investigation.")

d Ry Crozier, "AFP, ACIC Continue to Use Account Takeover, Network Activity Powers," IT News, 24 November 24 2023, https://www.itnews.com.au/news/afp-acic-continue-to-use-account-takeover-network-activity-powers-602702.

e Australian Government, Transparency Portal, Annex D: Account Takeover Warrants Annual Report 2022-23, https://www.transparency.gov.au/publications/attorney-general-s/australian-federal-police/australian-federal-police-annual-report-2022-23/annexes/annex-d%3A-account-takeover-warrants-annual-report-2022%E2%80%9323.

f Crozier, "AFP, ACIC Continue to Use Account Takeover, Network Activity Powers."

g James Jin King and Jumana Abu-Khalaf, "Facebook or Twitter Posts Can Now Be Quietly Modified by the Government under New Surveillance Laws," The Conversation, 6 September 2021, https://theconversation.com/facebook-or-twitter-posts-can-now-be-quietly-modified-by-the-government-under-new-surveillance-laws-167263.

h Ibid.

When an account holder's social media profile is open to the public, the use of social media for surveillance purposes does not necessarily violate expectations of privacy. However, it does open the door for government officials as well as their private contractors to review the content of posts, location of posters, and make its interpretations about the poster's intent. The Human Rights Law Centre argues that increased surveillance creates a chilling effect on interactions between whistleblowers and journalists.[48] In the context of social media platforms, companies like Meta have established procedures for law enforcement requests, citing compliance with international standards.[49] However, over the years, contractors in software development have increasingly taken on government surveillance responsibilities, particularly in counterterrorism efforts. In 2015, ZeroFOX, a U.S.-based company, was contracted to monitor social media and internet channels for cybersecurity threats (See Box 4). They surveilled the social media accounts of protestors in Baltimore, identifying 19 "threat actors," including two Black Lives Matter leaders deemed a "physical threat."[50]

Post-9/11, Muslim individuals and groups were frequently targeted. The Al-Husseyen case is a stark reminder of the impact of social media monitoring and online surveillance on civil society and the potential misinterpretation of social media posts (see box 14), illustrating the clear prioritization of national

48 Human Rights Law Centre, "Insufficient Safeguards in New Surveillance Law," 25 August 2011, https://www.hrlc.org.au/news/2021/8/25/insufficient-safeguards-in-new-surveillance-law.

49 Meta Privacy Policy, https://www.facebook.com/privacy/policy/?annotations[0]=10.ex.1-WhenWeRespondTo.

50 Stephen Babcock, "ZeroFOX under Fire for Social Media 'Threat Actors' Report during Baltimore Riots—Technical. Ly Baltimore," Technically Baltimore, 4 August 2015, https://technical.ly/baltimore/2015/08/04/zerofox-fire-social-media-threat-actors-report-baltimore-riots.

Box 15. Case law: *United States v. Al Hussayen,* 3:03cr48 (D. Idaho 2004)

In February 2003, Sami Omar Al-Hussayen, a Saudi national, was arrested by the FBI in Moscow, Idaho. Al-Hussayen was a graduate student at the University of Idaho and was accused of supporting terrorism through activities on social media platforms that promoted jihad and supported groups like Hamas. The government alleged that he used his skills in computer programming to maintain these websites, provide technical support, and recruit members for extremist organizations.

Al-Hussayen faced charges under the USA PATRIOT Act, including allegations of visa fraud, making false statements to the government, and conspiracy to support terrorism. His trial began in February 2004 and lasted for several months. During the trial, the prosecution presented evidence including emails, website postings, and financial transactions linking Al-Hussayen to terrorist activities.

The defense argued that Al-Hussayen's activities were protected by the First Amendment right to free speech and that he was not directly involved in any violent acts. They maintained that he was merely exercising his right to express political and religious opinions. Despite arrests and extensive monitoring, the government found no evidence of links to terrorism, charging Al-Hussayen with immigration fraud instead.

security over individual rights. The impact of that case on civil society within the Muslim community ranged from a decrease in charitable giving to organizations being completely shut down, highlighting the prioritization of national security over fundamental freedoms.[51]

Another aspect of social media is the censorship imposed by the platforms themselves—at times under government influence or due to misinterpretation or the excessively narrow application of laws. Platforms like Facebook, Twitter (now X), and YouTube impose terms of service as a contract between users and the platform, prohibiting content such as hate speech, terrorist material, nudity, and harassment. While these restrictions are within their rights as private corporations, their content moderation methods face criticism. Each company sets its own standards, leading to mass takedowns that disproportionately affect marginalized groups. Over the years, there have been multiple instances where Facebook erroneously deleted news articles and suspended the accounts of journalists and human rights activists, including at least 35 accounts belonging to Syrian journalists in the spring of 2020 and the accounts of 52 Palestinian activists in a single day in May 2020.[52]

The censorship of dissenting voices on social media poses a significant threat to free expression and democratic discourse. As platforms increasingly wield power over the flow of information, there is growing concern that certain viewpoints are being suppressed or silenced altogether. Recently, we have seen the ongoing censorship of Palestinian voices on Meta-owned platforms, particularly Instagram and Facebook. A Human Rights Watch report[53] highlights the systematic suppression of Palestinian content, including accounts, posts, and hashtags, by Meta, despite its stated

51 *United States v. Al Hussayen*, 3:03cr48 (D. Idaho 2004).
52 Ibid.
53 Human Rights Watch, "Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook," 20 December 2023, https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and.

commitment to free expression. Through detailed analysis and case studies, the report calls for Meta to uphold its responsibilities to respect freedom of expression and to address the discriminatory practices that undermine Palestinian voices on its platforms.

THE WAY FORWARD: REFORM AND MITIGATION

This section reflects on the avenues that exist to pursue a more equitable balance between national security imperatives and fundamental human rights with regard to the use of new and emerging technologies in the national security space. It proposes a variety of reform and mitigation measures that pursue structural change while empowering individuals and organizations to protect themselves from invasive surveillance, monitoring, and data collection. In most cases, the onus falls on members of civil society to lead these efforts—often at great risk to personal safety and security.

LEGAL AND POLICY DEVELOPMENT

Comprehensive legislative reform is needed to meaningfully address the use of new technologies in the context of national security and counterterrorism measures and to ensure the appropriate balance between public safety and the protection of civil liberties.

As a critical normative body, the United Nations can play an important role in establishing universal protections in line with its Charter and international law. There are opportunities to improve the verbiage of Security Council Resolutions and to develop guidance for member states to shape their practical implementation. For example, Security Council Resolution 2178 (2014) mandates member states to develop watch lists and databases for counterterrorism cooperation related to foreign terrorist fighters (FTFs). Resolution 2396 (2017) further urges states to strengthen border control, criminal justice, and information-sharing systems related to FTFs. Both resolutions would benefit from further clarity regarding data retention and sharing procedures, the establishment of consent requirements for data gathering, and recourse measures for data gathering without probable cause. In parallel, the UN Counter-Terrorism Committee Executive Directorate (CTED) should persist in identifying legal shortcomings and human rights concerns within national counterterrorism laws and policies, while UNOCT and other UN technical assistance providers should be more vigilant about the normative implications of its programming efforts.

Domestic legislation must clarify and reinforce due process protections to guide when, how, and for how long specific technologies can be deployed by government authorities during public emergencies or in pursuit of public safety. Transparent and routine reauthorization processes are critical to ensuring robust debate and that measures remain proportionate and necessary. Harmonization around the protocols for deployment and training on the limitations of new technologies, such as failure rates and inherent biases, are important to ensure that the use of new technologies remains consistent with international law. Applying consent requirements to data gathering and recourse for data gathering without probable cause would contribute to establishing clear boundaries and preventing the abuse of individuals' civil rights. The regulation of third-party contractors working on behalf of governments is also required to ensure that the same protections apply for surveillance, data collection, content moderation, and other practices.

The legal and regulatory framework for private sector actors also demands the recalibration of data collection, retention, and sharing practices. The current approach affords the private sector disproportionate responsibility for ensuring ethical data practices. In some cases, lawmakers lack the technical capacity to identify data-related concerns and craft regulations that safeguard human rights. In others, governments are willfully reluctant to establish protections, as law enforcement and intelligence agencies could benefit from accessing privately held data for their own security and surveillance efforts.

To be effective, policy frameworks must be crafted through meaningful and equitable collaboration between government, civil society, and technology companies. Doing so ensures a clear, comprehensive,

practical, and transparent framework consistent with international human rights law and data protection and privacy measures. Sustained dialogue and evaluation of policy implementation are also important to ensure that the legal and regulatory frameworks achieve their intended purposes and remain reflective of and appropriate to the dynamic technological landscape.

OVERSIGHT AND ACCOUNTABILITY

The swift evolution and expansion of technology, coupled with the exponential growth and increasing sophistication of artificial intelligence, is currently outpacing regulation around its use, leaving a gap that enables intelligence agencies and law enforcement, as well as their private sector partners, to operate without sufficient checks and balances. The result is a secretive system that emboldens government entities to wield new and emerging technologies with impunity.

The enhanced computing power and algorithmic capabilities of AI systems can exacerbate issues such as bias, errors, and privacy infringements, raising profound ethical and legal considerations. Holding states accountable for violations is paramount to safeguarding individual liberties and maintaining the rule of law. The establishment of an independent review board can help ensure that national policies on the use of new technologies remain compliant with ICCPR standards on the right to privacy and freedom of expression. Such boards would benefit from multi-sectoral composition, including civil society organizations, legal experts, and human rights advocates along with security sector representatives and policymakers. Policy-level reviews can be augmented with specialized audits of particular programs to ensure compliance with human rights standards and data protection measures and to evaluate the potential impact on vulnerable populations.

Domestic administrative procedures provide another valuable avenue for holding states accountable. For example, in Australia, citizens and civil society entities can utilize ombudsman channels at both the federal and state/territory levels to raise concerns and disputes with government agencies or industry entities. The Office of the Australian Information Commissioner ("OAIC"), formerly known as the Privacy Commissioner, provides an independent mechanism to uphold and promote privacy and information access rights in Australia. Its primary objectives revolve around safeguarding individuals' privacy, promoting transparency and accountability in the government and private sectors, and ensuring compliance with Australia's privacy and freedom of information laws. The OAIC has regulatory powers to oversee compliance with privacy and freedom of information (FOI) laws in Australia. This includes monitoring the handling of personal information by government agencies and private sector organizations covered by the Privacy Act of 1988. The OAIC investigates complaints and breaches of privacy, conducts inquiries, and takes enforcement action where necessary.[54]

"Freedom of information" type laws offer a further framework for transparency and public accountability. Since 2019, there has been a global expansion of these mechanisms, with 125 countries enacting right-to-information laws.[55] In the United States, there has been a surge in FOIA requests from nonprofits, law firms, corporations, and individuals seeking documents from federal agencies: requests escalated from 514,541 in 2009, to 714,231 in 2014. This trend signifies a robust and expanded reliance on administrative mechanisms for civil society to gather essential information and hold institutions accountable.

In addition to national-level mechanisms, at the international level, the United Nations must serve as a normative leader and accountability mechanism to member states in cases where human rights are

54 *Privacy Commissioner v. Telstra Corporation Limited* [2017] FCAFC 4, 30 January 2017, https://timebase.com.au/news/2017/AT04069-article.html#:~:text=Privacy%20Commissioner%20v%20Telstra%20Corporation%20Limited%20%5B2017%5D%20FCAFC%204,-Monday%2030%20January&text=The%20Full%20Federal%20Court%20has,metadata%E2%80%9D%20held%20by%20the%20company.

55 "UNESCO Finds 125 Countries Provide for Access to Information," 25 July 2019, https://sdg.iisd.org/news/unesco-finds-125-countries-provide-for-access-to-information.

violated within their counterterrorism practices. Establishing a human rights oversight mechanism for UN programs, composed of diverse stakeholders including human rights experts, civil society organizations, and relevant governmental bodies, could help ensure that UN initiatives adhere to international human rights standards in the conduct of their programs. In parallel, the establishment of an independent oversight mechanism at the United Nations to effectively evaluate and address the adverse consequences stemming from counterterrorism efforts is necessary to address potential abuses in the use of new and emerging technologies for national security purposes and advocate for transparency and accountability in UN initiatives.

LITIGATION/LEGAL PROCESSES

Article 2 of the ICCPR provides to "ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity."[56] In practice, opportunities for redress are limited.

Litigation is unequivocally the most impactful method for challenging the use of new and emerging technologies in counterterrorism and national security contexts. Court decisions have established legal precedents. These precedents can guide future cases, shaping the interpretation and application of laws regarding national security and human rights. They can clarify the boundaries of government actions in the name of security and affirm the importance of protecting fundamental rights, even in times of crisis. Legal proceedings provide a platform to hold individuals and institutions accountable for their actions. This accountability is crucial for preventing abuses of power and ensuring that those responsible for human rights violations are held accountable under the law. Litigation can also bring attention to human rights violations, raising public awareness about the issues at hand. High-profile cases can attract media coverage and public scrutiny, fostering discussions about the balance between security and civil liberties. This increased awareness can lead to public pressure for reforms and changes in policy or practices that better protect human rights. Finally, successful litigation can catalyze policy changes. Court rulings may prompt legislative reforms, changes in government policies and practices, or the establishment of oversight mechanisms to ensure compliance with human rights standards. However, the viability of this mechanism is highly contingent on the ability of the affected party to access a fair, credible, and equitable criminal justice system. Even when such avenues are available, individuals struggle to mount legal challenges as government agencies can conceal actions and attempt to withhold information under the banner of national security.

If not directly involved in a lawsuit, individuals and organizations can also contribute amicus briefs—legal opinions submitted to a court by a party not directly involved in the lawsuit supporting a legal position—to support a position. International Courts such as the Inter-American Court of Human Rights and the European Court of Human Rights allow civil society representatives and organizations to submit briefs. In 2021, UNESCO created a guide to assist civil society organizations in developing amicus curiae for freedom of expression cases.[57]

ADVOCACY AND EDUCATION

Around the world, civil society is actively leading advocacy and education efforts to promote human rights–compliant and accountable government use of emerging technologies. Watchdog organizations track the development of technologies and document abuses; researchers and policy analysts seek to inform and shape the global discourse; and advocacy campaigns target policy development and challenge legal frameworks. The political and operational climate for these efforts varies significantly, and in many places,

56 ICCPR, Art 2.

57 "UNESCO Launches Practical Guide for Amicus Curiae Interventions in Freedom of Expression Cases," 23 September 2021, https://www.unesco.org/en/articles/unesco-launches-practical-guide-amicus-curiae-interventions-freedom-expression-cases.

civil society and activists experience real and pervasive security threats as a result of their work. In the United States,[58] civil society leverages opportunities like expert testimonies before Congress to influence decision-making, although it may be unsure of the extent of their impact.

Another approach involves direct collaboration between civil society and technology creators. This has been seen most prominently in relation to social media, with bodies like the Global Internet Forum to Counter Terrorism and Tech Against Terrorism fostering collaboration and information sharing between government, civil society, and the private sector to counter terrorism and violent extremist activity online. These multi-disciplinary forums play a critical role, given the global inconsistency in defining terms like "hate speech" and "terrorist organization" across platforms, providing an avenue to foster standardized definitions, strategies, and practices and to encourage cultural/linguistic sensitivity to mitigate discrimination in content moderation.

In addition to these efforts, there is growing recognition of the importance of digital literacy campaigns aimed at the wider public. These campaigns seek to equip individuals with the skills and knowledge necessary to navigate the digital landscape safely and responsibly. By promoting critical thinking, media literacy, and awareness of online risks, such campaigns empower users to protect themselves from misinformation and other online threats.

DIGITAL SECURITY MEASURES

Absent a robust legal framework that protects against unwarranted state intrusion, individuals and civil society organizations are put in the position of adopting measures to safeguard their own data and privacy. Especially in contexts where the Global War on Terror (GWOT) paradigm has been invoked to justify perpetual states of emergency, the need for robust digital security measures becomes even more pronounced. In such environments, civil society must actively resist encroachments on privacy and free expression by leveraging digital security tools. By embracing encryption, anonymization techniques, and secure communication platforms, organizations can more effectively shield themselves from unwarranted government surveillance and protect the integrity of their private communications.

Many different technologies make it harder for surveillance entities to monitor online activities. For example, Virtual Private Networks (VPNs) help encrypt data, mask internet traffic, and obscure IP addresses to make locations more difficult to trace. Encryption tools, such as end-to-end encrypted messaging platforms, work to make sure communications are secure and inaccessible to unauthorized parties. Many of these tools are widely available, with some at little to no cost. However, some countries have limited or banned their use—seeing them as a threat to national security or as part of an effort to control internet access and suppress dissent. There is also significant variance in the security protections of different communication platforms, data storage platforms, and encryption tools. Complicated user options and features, the inter-connectivity of applications, and reliance on third parties can make it difficult for users to understand or limit their access to the necessary information to make decisions about data security.

Digital literacy campaigns play an important role in helping people understand the risks posed by surveillance and adopt good practices for protecting their digital privacy. Capacity development programs can provide training and technological solutions to help civil society and humanitarian organizations enhance their data management, privacy protection, and cybersecurity measures as they navigate the complexities of data handling in conflict zones.

58 Nara Lacerda, "Brazilian Government Reinstates Civil Society Council to Debate the Country's Development," Brasil de Fato, 5 May 2023, https://www.brasildefato.com.br/2023/05/05/brazilian-government-reinstates-civil-society-council-to-debate-the-country-s-development.

CONCLUSION

The weaponization of new and emerging technologies under the pretext of national security represents a grave threat to democratic principles, fundamental freedoms, and human rights. As we look toward a future where AI plays an increasingly central role in national security strategies, it is crucial to recognize the amplified implications for human rights and civil liberties. The potential for bias, errors, and misuse looms larger as AI becomes more pervasive, necessitating proactive measures to mitigate risks and safeguard fundamental rights. While AI-driven technologies offer unparalleled capabilities in enhancing security efforts, their deployment must be guided by a steadfast commitment to upholding human rights principles.

The exponential growth in computing power and algorithmic sophistication inherent in AI-powered technologies highlights the urgent need to address the concerns outlined in this policy brief. Throughout this analysis, we have examined how governments exploit the ambiguous concept of national security to surveil, intimidate, and silence political opponents, journalists, and human rights defenders. The erosion of civil liberties and democratic norms perpetrated by such practices undermines the very fabric of democratic societies. Furthermore, the lack of transparency, oversight, and accountability surrounding surveillance programs exacerbates the risks of abuse. Without robust legal frameworks and independent oversight mechanisms, governments are emboldened to wield new and emerging technologies with impunity, unchecked by democratic checks and balances.

To safeguard individual liberties, comprehensive legal reforms must be enacted to ensure that surveillance is conducted within the bounds of international human rights standards. It also requires the empowerment of civil society, independent media, and judicial oversight mechanisms to serve as bulwarks against government overreach.

ABOUT THE AUTHOR

Annabelle Bonnefont

Annabelle Bonnefont is a Senior Legal Analyst and Human Rights Advisor for the Global Center. She provides research and programming support on criminal justice and rule of law issues. She has legal experience in France, China, and the United States in the fields of public and private international law, rule of law, counterterrorism, human rights law, and peace-building operations. After practicing as a trainee lawyer in international litigation and arbitration at international law firms, she was a consultant for the United Nations and conducted legal analysis in the areas of counterterrorism, investigation, and human rights law. She is a member of the Paris Bar, she holds a master's degree in international law from Paris 2 Université Panthéon-Assas, a master's degree in Chinese language and modern politics from INALCO, and an LLM from Columbia Law School.

ACKNOWLEDGMENTS

The Global Center on Cooperative Security gratefully acknowledges the support for this project provided by the government of the United Kingdom. The views expressed are those of the author and do not necessarily reflect the views of the Global Center or its advisory council, board, or sponsors or the government of the United Kingdom.

ABOUT THE GLOBAL CENTER

The Global Center on Cooperative Security is an international nongovernmental organization that advances human rights–centered responses to political violence, violent extremism, and injustice worldwide. We believe cooperation among community groups, governments, and international organizations such as the United Nations is critical to achieving a just and secure world.

GLOBAL CENTER
ON COOPERATIVE SECURITY

globalcenter.org
@GlobalCtr