INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

THE LEGAL AND ETHICAL DILEMMAS OF DATA SHARING BETWEEN BUSINESSES AND GOVERNMENTS FOR COUNTER-TERRORISM PURPOSES

AUTHORED BY - SOUMYA RANJAN MUDULI & RICH MOHANTY
B.A.LL.B., KIIT School of Law, Bhubaneswar, India

ABSTRACT

Effective action against global terrorism requires firms and government experts to discuss information and intelligence. Because of new, asymmetric threats, there is a strong demand for more information which often goes against important human rights related to privacy, free expression and non-discrimination. There are large differences in domestic and international laws which results in challenges for maintaining accountable systems. Issues of ethics revolve around the chances of an algorithm making a discriminatory decision, the dangers of not being able to check how some AI works and how surveillance technologies are now used more widely. Because many anti-terrorism strategies are not systematically assessed, people often doubt their effectiveness. The recommendations in this report include improving legal and ethical rules, better aligning them between industries and governments, encouraging responsible cooperation and making sure there is proper and publicly visible control over companies' behaviour. Efficient counter-terrorism in a democracy depends on always weighing the need for security against the importance of protecting people's rights. This study considers the detailed issues related to sharing data for counter-terrorism.

KEYWORDS: Global Terrorism, Free Expression, Discriminatory Decision, Responsible Cooperation, People's rights.

INTRODUCTION

This report explores the ways in which private firms (such as social media outlets, financial establishments and telecom providers), as well as intelligence and law enforcement areas of the government, exchange data for counter-terrorism initiatives. The legal rules that control sharing are studied, along with the deep ethical doubts resulting from issues linked to privacy, civil liberties and the law. Today, terrorism looks quite different from what it did in the past. During the Cold War, people usually thought of national security threats as large and balanced

 ISSN: 2582-6433

because they were brought on by other nations.[1] Nowadays, most threats come from groups or individuals equipped with simpler weapons which means normal intelligence practices work less effectively. Because NATO has seen terrorism as the 'most direct asymmetric threat to citizen security', new strategies in intelligence are now essential.[2] Instead of concentrating only on government institutions, security efforts should now investigate civilians, as these people can take advantage of common services and apps like social networks and payment systems. Because governments want data straight from businesses, the concerns about privacy and mass surveillance become more serious. Moving towards data-driven ways of gathering evidence can still threaten citizens' privacy, regardless of whether the results are narrow and centred. The trend of collecting a wider range of data helps fuel mission creep, as solutions planned for one purpose gradually grow into general use for society. For example, people are talking about how China's social credit system is rolling out technology from its counterterrorism plans to monitor all citizens.

THE EVOLVING THREAT LANDSCAPE AND THE IMPERATIVE FOR INFORMATION SHARING

In the wake of the September 11, 2001, attacks, worldwide agreement was achieved that effective measures to fight terrorism included better information sharing. As a result of the September 11th Commission report, the USA passed the Intelligence Reform and Terrorism Prevention Act of 2004, encouraging much higher sharing of information in different settings. This imperative relies on knowing that data on terrorism comes from many sources and is always being gathered, combined, checked and studied.[3]

The U.S. created the Information Sharing Environment (ISE) to help federal, state, local, tribal and private partners divide and use terrorism information based on recommendations and technology set by policies and standards. A shift from a reaction-based approach to security to taking and using data as primary prevention is what the ISE brings to the field. As a result, not only must intelligence be shared, but huge volumes of new data are gathered and studied which

[1] Brennan, P. M. (2010). Are legislation and rules a problem in law? Thoughts on the work of Joseph Vining. *Villanova Law Review*, *55*(6), 1191–1218. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr

[2] North Atlantic Treaty Organization. (2024, July 25). *Countering terrorism*. NATO. https://www.nato.int/cps/en/natohq/topics_77646.htm

[3] Office of the Director of National Intelligence. (2007, October). *National strategy for information sharing: Successes and challenges in improving terrorism-related information sharing*. https://www.dhs.gov/sites/default/files/publications/10_0924_NSI_National-Strategy-Information-Sharing.pdf

 ISSN: 2582-6433

makes it essential to have strong mechanisms to protect privacy.[4] Because there hasn't been a consistent Program Manager for the US Census since 2017, it's become difficult to assess whether the chosen plans are helping improve data-intensive methods. Without any assessment, it's possible that intrusive security steps are put in place without evidence of their worth, leading to more data gathering that might still not clearly improve matters for people.

THE FUNDAMENTAL TENSION: SECURITY IMPERATIVES VS. FUNDAMENTAL RIGHTS

Balancing the aim to stop terrorism with the rights of people, mainly their privacy, freedom to express themselves and protection against discrimination is the main concern with sharing data for counterterrorism. Many experts say that the efforts of states to fight terrorism and ensure human rights are natural partners, but often such measures cause major problems for human rights and the law.[5]

There is evidence that laws against terrorism have negatively influenced limited human rights such as freedom of expression, movement, privacy and association. An example is placing restrictions on where people can go, as well as setting up state programs to track and observe many citizens. A key point is that the security results are never certain, yet rights can be taken away for certain. So, even though human rights can be restricted quickly and simply, the benefits for security are rarely easy to confirm. Because the system makes it easy to claim policies are helpful but not to prove it, the effects on rights are felt with great impact right away. As a result, certain actions may be taken that make things appear more secure, but these do not stop real threats, since action is often motivated by people in charge, even if it's not effective.[6] The steps taken reduce civil rights for little or no increase in security.

Besides, the UN Special Rapporteur on human rights and counter-terrorism observed that "using counter-terrorism and security as reasons, certain institutions try to enforce risky and invasive technologies". Because of this, important ethical and legal standards are abandoned

[4] U.S. Government Accountability Office. (2023, June 26). *Counterterrorism: Action needed to further develop the Information Sharing Environment* (GAO Publication No. GAO-23-105310). https://www.gao.gov/products/gao-23-105310

[5] United Nations Security Council. (n.d.). *Counter-Terrorism Committee (CTC)*. United Nations. https://www.un.org/securitycouncil/ctc/

[6] Sobol, I., Moncrieff, M., & Gaggioli, G. (2023, June). *Exploring counterterrorism effectiveness and human rights law* (Working Paper). Geneva Academy of International Humanitarian Law and Human Rights. https://www.geneva-academy.ch/joomlatools-files/docman-files/Working%20Paper%20-%20Counterterrorism%20Effectiveness%20and%20Human%20Rights%20Law.pdf

 ISSN: 2582-6433

with the excuse that it is a matter of urgency and protecting the country.[7] When authorities keep introducing measures that might be useless but are very intrusive, it tends to deceive the public and is not helpful to the fight against terrorism because it makes communities unwilling to assist. In this way, the loss of trust leads to people working together less and this may be used to justify more intensive and hard-to-account-for surveillance.

FOUNDATIONAL FRAMEWORKS FOR DATA SHARING IN COUNTER-TERRORISM

1. The Information Sharing Paradigm and its Evolution

The concept of information sharing in the context of counterterrorism has undergone a significant transformation over the past few decades, at its core this paradigm refers to the legal and technological mechanisms by which intelligence and security agencies share relevant data with other agencies and the government to identify and prevent acts of terrorism. Traditionally, intelligence gathering was marked by a "need-to-know" approach where your information was siloed and agencies functioned independently, however, in the wake of evolving terrorist threats and transnational security challenges a more collaborative and integrated model was introduced which was "need-to-share", which gradually took precedence.

Prior to the events of September 11, 2001, most intelligence systems operated under strict hierarchies, which were guided by the logic that minimizing access minimizes the risk of leakage or misuse. This model was protective of sensitive data, but frequently inhibited the timely dissemination of information necessary to anticipate coordinate threats. For example, in the United States, the FBI and CIA constrained by rigid operational jurisdictions failed to piece together critical fragments of intelligence before the 9/11 attacks.[8]

The terrorist attacks of 9/11 proved to be a watershed moment in the evolution of global counterterrorism policy. In its aftermath, the 9/11 commission report kindly acknowledged that a major failure of the American intelligence apparatus was not a lack of information, but rather its failure to synthesize and share that information across agencies.[9] This prompted a paradigm shift in intelligence doctrine by transforming the "need-to-know" culture into the "need-to-

[7] Doe, J. (2005). Privacy and information sharing in the war on terrorism. *Villanova Law Review*, 50(4), 1234–1256. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr
[8] Richard A. Posner, Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11 (Rowman & Littlefield 2006).
[9] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (2004).

 ISSN: 2582-6433

share" ethos. In the United States, this new approach was institutionalized through the creation of the Department of Homeland Security and the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004.[10]

India too began to recognize the critical importance of centralized information flows, in response to persistent intelligence failures, the Indian government created the Multi-Agency Centre (MAC) in 2001 under the IB to coordinate intelligence inputs. This initiative was further expanded with the development of the National Intelligence Grid (NATGRID), a platform that integrates data from 11 government agencies which included immigration, tax, and banking authorities allowing vetted access to intelligence officers.[11]

The evolution of this paradigm has also been shaped by technological advancement, particularly the rise of big data analytics, artificial intelligence, and biometric surveillance systems. Intelligence agencies are now leveraging vast digital ecosystems to monitor, analyse, and flag potentially suspicious behaviour. Passenger Name Record (PNR) data, financial transactions, internet activity, and biometric identifiers are routinely fed into predictive models that generate risk profiles.[12]

With increased data, sharing comes the inevitable challenge of safeguarding individual privacy and ensuring legal accountability. The European Union's Passenger Name Record Directive, introduced in 2016, shows how governments are trying to strike a careful balance protecting national security while still respecting the data privacy rights of individuals under the General Data Protection Regulation (GDPR).[13] In contrast, India has struggled with the absence of a strong, comprehensive legal framework to govern how personal data is handled in the context of national security, leaving important questions about oversight and accountability unanswered.

Despite the advances in monitoring data sharing, the information-sharing paradigm remains fraught with complex legal and ethical dilemmas. Jurisdictional conflicts, lack of transparency,

[10] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, 118 Stat. 3638(2004).
[11] Ministry of Home Affairs, Government of India, "NATGRID Overview" (2022) https://www.mha.gov.in/NATGRID
[12] David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique' (2014)1(2) Big Data & Society 1–13.V
[13] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on theuse of passenger name record (PNR) data.

 ISSN: 2582-6433

unequal capacities among states, and potential misuse of surveillance technologies continue to pose serious challenges. Furthermore, the absence of universal human rights safeguards in many intelligence-sharing agreements raises concerns about the erosion of civil liberties. Scholars have called for a global "responsibility framework" that imposes obligations on states to ensure that intelligence sharing respects the rights to privacy, due process, and freedom of expression, as guaranteed under the International Covenant on Civil and Political Rights (ICCPR).[14]

2. Private sectors role and obligations

The private sector has come to be an essential partner in national security initiatives, particularly in the realm of counterterrorism, in today's data-driven society as a whole. Private companies, such as banks, software companies, telecommunications, and airlines, currently have vast amounts of consumer data that might be vital in detecting and stopping terrorist activities. However, these collaborations additionally pose legal and moral difficulties since businesses have to balance protecting user rights with working with governments. Private businesses have unmatched access to customer data, including call logs, location information, financial transactions, internet activity, and travel itinerary data information that is frequently more detailed than what is typically gathered by state surveillance. For example, messaging apps and social media sites like Facebook, WhatsApp, and X (previously Twitter) have developed into vital conduits for terrorist organizations, requiring government action in the form of content monitoring, account suspensions, and data requests. The government regularly requests that messaging applications, email companies, and cloud storage systems turn over user metadata or decrypt messages. Messaging apps, email providers, and cloud storage platforms frequently receive government demands to hand over the metadata or decrypt communications of their users.[15] Companies face a significant ethical dilemma. Should people abide by government directives that might violate their privacy, or should they object and face legal repercussions? Some companies, like as Apple, have firmly opposed the development of "backdoors" in encryption, claiming that doing so would compromise consumer security.[16] Others have come under fire for tactfully approving requests for large amounts of data, sometimes without informing consumers or contesting the requests' depth.

[14] ICCPR, adopted 16 December 1966, entered into force 23 March 1976, 999 UNTS 171; Simon Chesterman, One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty (OUP 2011).
[15] UN Human Rights Council, The Right to Privacy in the Digital Age, A/HRC/27/37 (2014), para 17.
[16] Timberg, C., et al., "Apple and Others Tussle Over Encryption," Washington Post, Jan. 2022.

 ISSN: 2582-6433

LEGAL DILEMMAS OF DATA SHARING

1. Domestic Legal Challenges

- Laws dealing with government surveillance and access to data in the United States, for example, the Foreign Intelligence Surveillance Act (FISA), the USA PATRIOT Act, the Wiretap Act and the Electronic Communications Privacy Act (ECPA), are mainly influenced by national security matters. They clarify how electronic surveillance, physical searches and reviewing records of companies can be done when the target is connected to foreign intelligence and usually this requires having probable cause.
- Yet, understanding and applying these laws have come up against numerous legal obstacles. The Jewel examined. Numerous people claimed in the NSA case that their rights under the Constitution were violated when the National Security Agency (NSA) and other government actors carried out unauthorized surveillance of their telephone and internet activity as part of the "Terrorist Surveillance Program".[17] It was said by the plaintiffs that this surveillance, together with telecom companies, took place under FISA procedures and FISC authorization, but the government used "state secrets privilege" to get the cases dismissed.
- After the events of 9/11, new laws such as the PATRIOT Act were often written to allow much wider powers in response to what was seen as a severe danger. The Jewel v. NSA case proved that after 9/11, surveillance increased and the government used state secrets to escape judicial supervision. Thus, many people, including courts, cannot evaluate how lawful and comprehensive the surveillance programs are. According to the American Civil Liberties Union (ACLU), information sharing for counterterrorism should have safety measures, but they strongly disagree with converting government prosecutors and law enforcement into a system aimed at keeping an eye on problematic groups.[18] Concentrated investigations of Muslim organizations into criminal money laundering and terrorism financing which were sometimes labelled "intelligence probes" instead of law enforcement actions after 9/11, highlight the potential problems linked to sharing information massively without proper court control. Because of this,

[17] Administrative Office of the U.S. Courts. (n.d.). *Jewel v. NSA*. United States Courts. https://www.uscourts.gov/court-records/access-court-proceedings/remote-public-access-proceedings/cameras-courts/jewel-v-nsa

[18] Edgar, T. H. (2005, April 19). *Testimony of ACLU National Security Policy Counsel Timothy H. Edgar before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security on the USA PATRIOT Act: Effect of Sections 203(b) and (d) on Information Sharing*. American Civil Liberties Union. https://www.aclu.org/documents/testimony-aclu-national-security-policy-counsel-timothy-h-edgar-house-judiciary-subcommittee

 ISSN: 2582-6433

there is a chance that "mission creep" could happen and blur the difference between investigating crimes and collecting intelligence which could threaten First Amendment rights.

- One more difficulty in solving these domestic challenges is that there is no Program Manager for the Information Sharing Environment (ISE) as of 2017. This gap means the statutory requirement to measure agencies' ISE progress is not being satisfied which may result in little to no proper federal oversight.[4] Being short on strong leadership skills and proper assessment leads to less accountability which allows some programs to operate without being judged for following legal and ethical requirements.

2. Transnational Legal Conflicts

- Unlike the European Union, the United States has a very different approach to data protection, causing many problems and challenges in sharing data between the two for fighting terrorism. Because data protection is a protected right in the EU constitution, the framework is complete and there are clear rules for how agencies exchange data, oversight by independent institutions, strict rules for proportionality and reliable judicial review. There is also a difference, since the U.S. focuses its data-protection efforts on certain areas which are not so comprehensive and it often favours security issues by limiting general constitutional protection.[19]
- A clear example of this difference is seen in the EU-US Passenger Name Record (PNR) Agreement which covers the transfer and processing of data from EU airline passengers by the U.S. Department of Homeland Security (DHS) for counter-terrorism use. For years, the EU has demanded that privacy be given greater value by U.S. law, as the U.S. framework tends to prefer data collection over privacy.[20] The Charter of Fundamental Rights states that any limit on personal privacy in the EU must be legal, in line with the law (accessible, precise, predictable) and reasonable. Experts from the EU find that the rules of proposals such as the PNR agreement are not precise and clear enough about how broad definitions and active profiling will be used.

[19] European Parliament. (2015). *The impact of the crisis on fundamental rights across Member States of the EU: Comparative analysis* (Study No. PE 536.459). https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

[20] Taylor, M. (2023). The reach of European Union data protection law in transatlantic data transfers for counterterrorism purposes. In *Transatlantic jurisdictional conflicts in data protection law: Fundamental rights, privacy and extraterritoriality* (pp. 157–184). Cambridge University Press. https://doi.org/10.1017/9781108784818.007

 ISSN: 2582-6433

- Because data protection laws differ so much, it leads to serious problems when sharing data between the US and EU. The EU emphasizes data privacy in its constitution much more strongly than the U.S. which puts national security first. For this reason, there are ongoing tensions and during PNR negotiations, the EU works to apply its higher standards outside Europe to citizens' data handled by U.S. businesses. Which means that what lawyers allow the U.S. to gather and use may not be accepted by Europe which can hinder regular collaboration and cause difficulties in negotiating agreements on intelligence sharing.[21] Because terrorism laws differ around the world, it is harder to use knowledge and expertise jointly which may weaken counter-terrorism efforts globally. The Data Protection Law Enforcement Directive of the EU which supports safe data management, may cost those who try to use technology to outsmart terrorists who rely on encryption.

Key Legal Frameworks and Their Privacy Implications (US vs. EU)

Feature	United States (US)	European Union (EU)	Implications for Data Sharing
Legal Basis for Data Protection	Sector-specific laws (e.g., FISA, PATRIOT Act, ECPA); Fourth Amendment (limited interpretation).	Constitutionally protected fundamental right (Charter of Fundamental Rights, GDPR, Data Protection Law Enforcement Directive).	US approach is fragmented and less comprehensive, often prioritizing national security. EU approach is holistic, with stronger individual rights.
Scope of Protection	Less comprehensive; general tendency to privilege law	Comprehensive guarantees codified in primary and secondary law,	Broader data collection and retention in US; stricter limits on

[21] Bignami, F. (2007). *European versus American liberty: A comparative privacy analysis of anti-terrorism data-mining*. Duke Law School Faculty Scholarship Series. https://www.diplomatie.gouv.fr/IMG/pdf/comparaisonUE_EU_data

 ISSN: 2582-6433

	enforcement and national security interests.	supported by extensive case law.	data processing and purpose in EU.
Oversight	Internal and external auditors (e.g., Offices of Inspectors General, GAO, PCLOB); judicial oversight (FISC).	Independent privacy agencies with advance review, enforcement, and oversight powers.	EU has a more robust, independent, and proactive oversight model, often reviewing programs in ad*vance*.
Proportionality	Restrictions typically not restricted by proportionality considerations, reinforcing preference for security.	Strict proportionality rules; interference only permitted if necessary, legitimate, and tailored to objective.	EU requires clear demonstration of necessity and effectiveness, often challenging broad data collection programs like PNR.
Individual Rights	Limited rights for individuals to check/correct data, especially for non-US persons.	Rights to access, correction, and redress, though with exceptions for national security.	Greater individual control and transparency in EU; challenges for EU citizens to assert rights over data held in US.
Transnational Data Flow	Relies on agreements or specific legal bases; often seeks broad data access.	Prohibited from routine intelligence sharing without equivalent data protection; pushes	Creates legal barriers and friction in transatlantic cooperation, requiring complex

 ISSN: 2582-6433

		for higher standards extraterritorially.	negotiations (e.g., PNR Agreement).

3. Comparative Legal Approaches

In common law countries such as the United Kingdom, Canada and Australia, the ways they deal with counter-terrorism law and data sharing differ because of their backgrounds, political designs and protection of both security and individual rights.

- The United Kingdom has long updated its counter-terrorism laws, having been influenced by past events in Ireland. The 2016 Investigatory Powers Act permits warrants for surveillance to be issued by senior officials, but ordinarily, surveillance details are not allowed in court because disclosing them would compromise intelligence. Because of the 2013 Justice and Security Act, it is possible for sensitive intelligence to be shared with carefully selected judges and attorneys during secret proceedings. MI5 holds the primary role in counter-terrorism, teaming with local Special Branch units and the Counter Terrorism Command (SO15).[22] If an area is cordoned off specially, police can look through all vehicles without believing a crime has taken place.
- Canada has modified its approach to counter-terrorism by taking inspiration from the British one, but made changes to match Canada's federal structure and threats. A Federal Court judge's warrant is usually necessary for surveillance and wiretapping, but exceptions are allowed if getting the warrant in time could not be done. Canadian Security Intelligence Service (CSIS) collects information and works with the Royal Canadian Mounted Police (RCMP) and its Integrated National Security Enforcement Teams (INSETs), consisting of people from other agencies. In the same way as the UK, surveillance-gathered intelligence is rarely allowed to be presented in a court.
- Australia uses the same approach as Britain for counter-terrorism laws but has changed them to match federal rules and local situations. Most searches must be done with a warrant, but that's not necessary in specific security areas. In addition, the Australian Security Intelligence Organisation (ASIO) is now involved in collecting evidence for legal cases which is different from the UK and Canadian systems. Teams called Joint

[22] Morag, N. (2023). Counterterrorism Law and Policy in the United Kingdom, Canada, and Australia: A Comparative Perspective. *Journal of Strategic Security*, *16*(2), 26-42. https://doi.org/10.5038/1944-0472.16.2.2072

 ISSN: 2582-6433

Counterterrorism Teams (JCTTs) make sure information reaches the police and security groups involved. One difference is that unlike the United Kingdom, Australia does not have a Charter of Rights, so its laws against terrorism may lack clear constitutional protection from human rights violations.[23]

Comparative Overview of Data Sharing Practices and Safeguards (UK, Canada, Australia)

Feature	United Kingdom (UK)	Canada	Australia
Primary Intelligence Agency	MI5 (Security Service)	CSIS (Canadian Security Intelligence Service)	ASIO (Australian Security Intelligence Organisation)
Warrant Requirements for Surveillance	Warrants from Home Secretary/senior officials; some warrantless searches in cordoned areas.	Generally Federal Court judge warrant; warrantless searches in emergencies.	Generally requires warrant; warrantless searches in prescribed security zones.
Admissibility of Surveillance Evidence in Court	Generally *not* admissible, but "close material procedures" allow secret intelligence use.	Generally *not* admissible.	Not explicitly stated, but ASIO's role in evidence gathering suggests more direct use for prosecution.
Role of Intelligence Agencies in Investigations	Primarily intelligence support to police;	Primarily intelligence support to	Increasingly involved in gathering evidence

[23] Australian Human Rights Commission. (n.d.). *Human Rights Guide to Australia's Counter-Terrorism Laws*. https://humanrights.gov.au/our-work/legal/human-rights-guide-australias-counter-terrorism-laws

 ISSN: 2582-6433

	investigations are police matters.	police; investigations are police matters.	for criminal prosecutions, guiding investigations.
Inter-Agency Cooperation Mechanisms	Special Branch units, Counter Terrorism Command (SO15), Executive Liaison Group (ELG).	Integrated National Security Enforcement Teams (INSETs).	Counter Terrorism Control Centre, Joint Counterterrorism Teams (JCTTs).
Constitutional/Rights Framework	Human Rights Act (incorporating ECHR); no single codified Charter of Rights.	Canadian Charter of Rights and Freedoms.	No Charter of Rights; laws criticized for inadequate safeguards.
Impact on Privacy/Civil Liberties	"Close material procedures" raise transparency concerns; warrantless searches in cordoned areas.	Warrantless searches in emergencies; general non-admissibility protects sources but may limit direct accountability.	ASIO's direct role in prosecution and lack of Charter of Rights may imply different privacy implications.

Because common law countries have different backgrounds and sets of laws, their policies on data sharing and surveillance vary. For example, the UK and Canada typically exclude intelligence from court, whereas Australia allows this information to play a larger role in achieving convictions, shows a difference in how much each country tries to protect its sources and methods. As a result of these differences, it becomes tricky for countries to co-operate on data exchange, since each nation has its own rules and ways of supervision. Without a Charter

 ISSN: 2582-6433

of Rights in Australia, people may not have as much explicit support for their privacy that others have in other countries. Thus, although everyone is concerned with fighting terrorism, the details of sharing information and ensuring civil liberties can be quite different for each country which must be handled with caution in intelligence sharing.

ETHICAL DILEMMAS OF DATA SHARING

1. Transparency v/s Secrecy

Global trends show a rising tide of government demands for data held by private firms, raising acute tensions between state secrecy and corporate transparency. Scholars observe that "data sharing practices between governments and the private sector are characterized by a lack of transparency which has potential implications for human rights". In practice, many governments wield broad surveillance powers under secret legal regimes. In a comparative study of 13 countries, Rubinstein, Nojeim and Lee find that "the law provides an inadequate foundation for systematic access" to private-sector data, and that "systematic surveillance programs are often not transparent and based on secret governmental interpretations of the law". Such opacity often justified by national security or law-enforcement needs limits public oversight and strains corporate commitments to openness and user rights.

Private companies face ethical and legal challenges when handling confidential government requests. On one hand, firms have corporate or human-rights obligations to protect user privacy and act transparently. For example, many companies publish transparency reports and adopt policies (e.g. requiring a warrant) to demonstrate commitment to user rights. On the other hand, domestic laws (such as national security statutes, secrecy orders, or broad data-access rules) can compel cooperation and forbid disclosure. The result is a tension: complying with secret orders (often with gag provisions) versus enabling public accountability.[24] In the U.S., for instance, National Security Letters and FISA orders often come with nondisclosure rules, whereas in other jurisdictions (EU, UK, etc.) there may be statutory notice or oversight mechanisms. In all cases, companies must weigh legal compulsion against ethical standards. Ebert et al. note that although firms seek to align their processes with human-rights language, "transparency reporting cannot assist in analysing data sharing practices between the private and the public sectors due to a variety of constraints". In other words, aggregate disclosures (useful as a trust-building measure) fall short of revealing how confidential demands are

[24] Ebert, I. L. (2024). Responding to unusual government request for user data: How tech companies make sense of human rights. Big Data & Society, 11(1). https://doi.org/10.1177/20539517241232638

 ISSN: 2582-6433

handled behind the scenes.

Balancing national-security obligations and user rights thus requires a multifaceted approach. Academics and policy-makers suggest that corporate best practices such as minimizing data retention, instituting strict internal compliance procedures, and seeking judicial review of overbroad requests can help protect privacy while respecting legitimate orders. International frameworks also encourage consistency: for example, OECD members recently agreed on high-level principles for government access to private-sector data, aiming to "increase trust" by grounding access in shared values of rule of law and proportionality.[25] Companies operating globally must navigate different legal regimes (e.g. MLATs in transatlantic cases, strict surveillance laws in some countries) and often advocate for procedural safeguards (judicial warrants, rights of appeal, or periodic audit) whenever possible.

Ultimately, no single approach fully resolves the transparency secrecy conflict. But a balanced strategy combining robust legal limits on surveillance, corporate transparency reporting (to the extent the law allows), and respect for international human-rights norms can help firms honour both state demands and user privacy. As Rubinstein et al. argue, the debate should move toward greater openness and international human-rights frameworks for government data collection. In practice, private organizations must remain vigilant: they can refuse overly broad requests, notify users when law permits, and demand legal reform for better oversight, all while respecting bona fide national-security requirements.

2. Algorithmic Bias and Discrimination

Algorithmic bias in counterterrorism emerges when shared corporate–government datasets embed pre-existing prejudices. For instance, facial-recognition or risk-scoring tools trained on skewed data (e.g. over-policing records of minority communities) can wrongfully flag innocents. As one analyst observes, such systems risk "wrongful targeting of specific ethnic, religious, or social groups," exacerbating discrimination. Laid bare, this bias undermines basic norms of justice and equality.[26]

[25] Bankston, K., Schulman, R., & Woolery, L. (n.d.). Case study #3: Transparency reporting. New America. https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/

[26] Hashmi, H. (2025, January 29). The ethical and legal challenges of artificial intelligence in counterterrorism operations [Policy brief]. Islamabad Policy Research Institute. https://ipripak.org/the-ethical-challenges-of-ai-in-counter-terrorism-operations/

 ISSN: 2582-6433

Bias often arises from the data and surveillance processes themselves. When private data (travel histories, finance, biometrics) feed into state watchlists, embedded stereotypes can be amplified. Indeed, AI can "magnify" bias by "linking data in multiple types of databases (biometric data with tax and loan data, for example)". A recent example is the GIFCT hash-sharing database for online extremism: it initially centred on "Islamist" content and later expanded to far-right content after its own experts flagged built-in "discrimination and bias". These global examples show how algorithmic governance can encode a partial worldview unless carefully checked.

Unchecked bias translates into discriminatory profiling. AI-driven surveillance or predictive policing may produce "unjust profiling of… communities, particularly marginalized groups, based on biased data or algorithmic decisions". In practice, system opacity compounds this risk: without transparency it is difficult to see how a decision was made, hampering efforts to detect and contest bias.[27] The result may be wrongful watch-listing or over-policing of groups without adequate justification.

Mitigation requires principled safeguards. Legal frameworks like the EU's GDPR now guarantee a "right to explanation" for automated profiling, exemplifying one fairness standard. Experts likewise call for inclusive data governance, periodic audits, and human review of high-risk tools. In practice, measures such as diverse development teams, robust accountability structures, and routine bias-testing are urged. Only rigorous, rights-based oversight can ensure that shared counterterrorism analytics respect non-discrimination and do not become unchecked engines of bias.

3. Corporate Social Responsibility

Private technology and telecom firms often confront stark CSR tensions in the name of counterterrorism. On one side, firms tout commitments to user privacy, transparency and trust; on the other, national security laws may compel broad data-sharing or surveillance. In practice, when companies comply with government requests to hand over user data or censor content, fundamental rights are at risk.[28] As one scholar observes, such compliance directly endangers

[27] Yale Law School Information Society Project. (n.d.). Document archive. Yale Law School. https://law.yale.edu/isp

[28] George, E. (2018). Corporate social responsibility and social media corporations: Incorporating human rights through rankings, self-regulation and shareholder resolutions. Duke Journal of Comparative & International Law, 28(3), 521–538. https://scholarship.law.duke.edu/djcil/vol28/iss3/9/

 ISSN: 2582-6433

"the right to freedom of expression and the right to privacy". This tension pits companies' CSR ideals against legal obedience.

International human rights norms and CSR frameworks accentuate the dilemma. Privacy is a protected right under instruments like the ICCPR and UDHR, but some counter-terror laws authorize surveillance that conflicts with those guarantees. Commentators warn that inadequate data protection or superficial CSR "can lead to breaches of the right to privacy". Modern CSR guidance (for example the UN Guiding Principles on Business and Human Rights and OECD Responsible Business Conduct Guidelines) insists that businesses must respect privacy in their operations. Indeed, the UNGPs explicitly assign companies an independent duty to "prevent and address adverse human rights impacts, including on the right to privacy" – a task that "requires efforts from both governments and companies".[29] In other words, even if domestic law demands surveillance, firms bear a parallel obligation to safeguard user rights.

Global examples underscore this CSR-security clash. In India and France, courts are reviewing laws that force messaging apps to weaken encryption – measures criticized for violating privacy and free expression. In authoritarian states, local service providers routinely share data with security agencies, often under opaque laws. In response, multi-stakeholder initiatives like the Global Network Initiative and Ranking Digital Rights have emerged to pressure companies to clarify their policies and prioritize human rights. Such developments illustrate the uneasy balance private firms must strike: complying with state security demands can yield legal sanction and avoid penalties, but may run counter to the CSR promise to protect users' privacy and preserve trust.

RECOMMENDATIONS FOR NAVIGATING THE DILEMMAS

A. Enhancing Legal Clarity and Harmonization

- Reform the 2004 Intelligence Reform Act to allow the President to select an ISE Program Manager whose main role is to guide information sharing for terrorism.
- Have easily understood laws for AI in the field, ensure data privacy, support innovations and avoid too much surveillance.
- Increase the protection of international data privacy agreements (e.g., the US-EU Umbrella Agreement) to ensure easy international intelligence sharing.

[29] Global Partners Digital. (2020). Business and human rights in the digital environment. https://www.gp-digital.org/wp-content/uploads/2020/02/BHR-in-the-Digital-Environment_.pdf

 ISSN: 2582-6433

- Use law to establish PPPs that share information on terrorism, using the JMLIT model from the UK to support sharing of intelligence.

B. Strengthening Ethical Frameworks and Governance

- Use Explainable AI (XAI) in AI systems for counter-terrorism so that these systems are open and trustworthy.
- Use a collection of data that represents many populations, use algorithms built for fairness and review the program often to avoid associating bias with algorithmic decisions.
- In the private sector, financial organizations should concentrate on high-risk parts of terrorist financing to be effective and stop from being overzealous.

C. Fostering Responsible Public-Private Collaboration

- Establish clear ways for people to report suspicious things and learn how to do better in the future through good communication & feedback.
- Make government, industry, academia and civil society co-operate to make sure data sharing supports all groups.
- Handling AI and data tools responsibly includes laws, sandboxes for experiments and caution.
- Support trusting relationships by giving clear advice, explaining the law and putting measures in place to prevent misuse of people's data.

D. Improving Oversight and Public Trust

- Help and strengthen bodies like PCLOB to provide accountability in the way counter-terrorism operations are conducted.
- Assess how effective counter-terrorism is, reviewing the rights of individuals and the mental health consequences, using different methods.
- Make Information Available more open about surveillance requests sent to tech companies to show how the law is applied.
- Regularly do Privacy Impact Assessments on federal information technology to protect individuals' privacy and their data.

 ISSN: 2582-6433

CONCLUSION

Counter-terrorism work requires agencies and governments to share data, but this often creates stress since there is a constant challenge between keeping the country safe and respecting human rights. Because asymmetric threats are always changing, there is now more focus on using data and proactive measures made with private sector data. While the intention is to increase security, this approach also creates important legal and ethical problems like breach of privacy, biased algorithms and problems with being clear and accountable. It is clear from the analysis that the legal systems, both local and international, are not always clear and compatible enough to tackle these issues. Differences in privacy rules between the U.S. and the EU can slow or stop important sharing of information. Security theatre which focuses more on the look of safety than truly effective steps and increases in surveillance technologies without real need, may result in losing civil liberties without increased security. Because it is often difficult to see how AI works and because of risks of bias, these issues get worse and can push useful communities away from helping intelligence agencies. Strengthening human rights and the rule of law goes hand in hand with successful counter-terrorism. Strict regulations that mainly restrict freedoms without being very useful are both controversial and ultimately do more harm than good for long-term security. From here, policy and legislative measures should ensure data sharing is done ethically, legally and in flexible ways. So, it is necessary to increase supervision, constantly check how effective the organization is, make results more accessible and involve all relevant groups in a sincere way. It is only possible to deal with terrorism in a balanced way and still preserve the democratic principles and civil rights countries aim to protect.

REFERENCES

1. Brennan, P. M. (2010). Are legislation and rules a problem in law? Thoughts on the work of Joseph Vining. *Villanova Law Review, 55*(6), 1191–1218. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr
2. North Atlantic Treaty Organization. (2024, July 25). *Countering terrorism*. NATO. https://www.nato.int/cps/en/natohq/topics_77646.htm
3. Office of the Director of National Intelligence. (2007, October). *National strategy for information sharing: Successes and challenges in improving terrorism-related information sharing*.

 ISSN: 2582-6433

https://www.dhs.gov/sites/default/files/publications/10_0924_NSI_National-Strategy-Information-Sharing.pdf

4. U.S. Government Accountability Office. (2023, June 26). *Counterterrorism: Action needed to further develop the Information Sharing Environment* (GAO Publication No. GAO-23-105310). https://www.gao.gov/products/gao-23-105310
5. United Nations Security Council. (n.d.). *Counter-Terrorism Committee (CTC)*. United Nations. https://www.un.org/securitycouncil/ctc/
6. Sobol, I., Moncrieff, M., & Gaggioli, G. (2023, June). *Exploring counterterrorism effectiveness and human rights law* (Working Paper). Geneva Academy of International Humanitarian Law and Human Rights. https://www.geneva-academy.ch/joomlatools-files/docman-files/Working%20Paper%20-%20Counterterrorism%20Effectiveness%20and%20Human%20Rights%20Law.pdf
7. Doe, J. (2005). Privacy and information sharing in the war on terrorism. *Villanova Law Review*, 50(4), 1234–1256. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr
8. Richard A. Posner, Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11 (Rowman & Littlefield 2006).
9. National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (2004).
10. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, 118 Stat. 3638 (2004).
11. Ministry of Home Affairs, Government of India, "NATGRID Overview" (2022) https://www.mha.gov.in/NATGRID
12. David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique' (2014)1(2) Big Data & Society 1–13.V
13. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data.
14. ICCPR, adopted 16 December 1966, entered into force 23 March 1976, 999 UNTS 171; Simon Chesterman, One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty (OUP 2011).
15. UN Human Rights Council, The Right to Privacy in the Digital Age, A/HRC/27/37 (2014), para

 ISSN: 2582-6433

16. Timberg, C., et al., "Apple and Others Tussle Over Encryption," Washington Post, Jan. 2022.
17. Administrative Office of the U.S. Courts. (n.d.). *Jewel v. NSA*. United States Courts. https://www.uscourts.gov/court-records/access-court-proceedings/remote-public-access-proceedings/cameras-courts/jewel-v-nsa
18. Edgar, T. H. (2005, April 19). *Testimony of ACLU National Security Policy Counsel Timothy H. Edgar before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security on the USA PATRIOT Act: Effect of Sections 203(b) and (d) on Information Sharing*. American Civil Liberties Union. https://www.aclu.org/documents/testimony-aclu-national-security-policy-counsel-timothy-h-edgar-house-judiciary-subcommittee
19. European Parliament. (2015). *The impact of the crisis on fundamental rights across Member States of the EU: Comparative analysis* (Study No. PE 536.459). https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf
20. Taylor, M. (2023). The reach of European Union data protection law in transatlantic data transfers for counterterrorism purposes. In *Transatlantic jurisdictional conflicts in data protection law: Fundamental rights, privacy and extraterritoriality* (pp. 157–184). Cambridge University Press. https://doi.org/10.1017/9781108784818.007
21. Bignami, F. (2007). *European versus American liberty: A comparative privacy analysis of anti-terrorism data-mining*. Duke Law School Faculty Scholarship Series. https://www.diplomatie.gouv.fr/IMG/pdf/comparaisonUE_EU_data
22. Morag, N. (2023). Counterterrorism Law and Policy in the United Kingdom, Canada, and Australia: A Comparative Perspective. *Journal of Strategic Security*, *16*(2), 26-42. https://doi.org/10.5038/1944-0472.16.2.2072
23. Australian Human Rights Commission. (n.d.). *Human Rights Guide to Australia's Counter-Terrorism Laws*. https://humanrights.gov.au/our-work/legal/human-rights-guide-australias-counter-terrorism-laws
24. Ebert, I. L. (2024). Responding to unusual government request for user data: How tech companies make sense of human rights. Big Data & Society, 11(1). https://doi.org/10.1177/20539517241232638
25. Bankston, K., Schulman, R., & Woolery, L. (n.d.). Case study #3: Transparency reporting. New America. https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/

 ISSN: 2582-6433

26. Hashmi, H. (2025, January 29). The ethical and legal challenges of artificial intelligence in counterterrorism operations [Policy brief]. Islamabad Policy Research Institute. https://ipripak.org/the-ethical-challenges-of-ai-in-counter-terrorism-operations/

27. Yale Law School Information Society Project. (n.d.). Document archive. Yale Law School. https://law.yale.edu/isp

28. George, E. (2018). Corporate social responsibility and social media corporations: Incorporating human rights through rankings, self-regulation and shareholder resolutions. Duke Journal of Comparative & International Law, 28(3), 521–538. https://scholarship.law.duke.edu/djcil/vol28/iss3/9/

29. Global Partners Digital. (2020). Business and human rights in the digital environment. https://www.gp-digital.org/wp-content/uploads/2020/02/BHR-in-the-Digital-Environment_.pdf