Transnational governance and law

Citation for published version:
Sullivan, G 2021, Transnational governance and law: Global security and socio-legal studies. in M Valverde, KM Clarke, ED Smith & P Kotiswaran (eds), *The Routledge Handbook of Law and Society.* 1 edn, Routledge, pp. 59-66. https://doi.org/10.4324/9780429293306-10

Digital Object Identifier (DOI):
10.4324/9780429293306-10

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
The Routledge Handbook of Law and Society

Routledge Handbook of Law and Society

Transnational Governance and Law: Global Security and Socio-Legal Studies

Gavin Sullivan

The last decade has witnessed a resurgence of right-wing populism and the rapid spread of nativist politics across what were once thought liberal democracies. This shift has been accompanied by strongman rhetoric denouncing the perils of 'globalism' and attacks on the multilateral institutions and norms that defined the late twentieth century international order. For Trump, and other authoritarian populists like him in Brazil, UK, Hungary and elsewhere, 'the future belongs to patriots' ready to defend national sovereignty from 'outside' dilution and 'take back control'. International organisations (IOs) are critiqued, treaties are either neglected or abandoned and global governance is derided in favour of self-interested state behaviour across key foreign policy areas.

Yet despite these reassertions of sovereignty from the populist right, global political and economic problems continue to generate new regulatory instruments and processes that enmesh national and international laws and public and private norms together in novel ways. From climate change to migration, financial crises, and internet governance, cross-border risks and problems are being governed in ways that transversally cut across national boundaries.

The regulatory tools used to govern transnational problems often bear little resemblance to the formal laws used by states, including international law. Informal 'soft law' measures (like indicators, rankings and best practice guidelines) and forms of private ordering (such as private contracts and terms of service, standard setting and dispute settlement) are on the rise, whilst formal international lawmaking is in decline. The expansion of data harvesting within surveillance capitalist societies and correlated growth in algorithmic decision-making is also stimulating new information infrastructures and ways of governing through data, that are reordering relations between individuals, states and global bodies in far-reaching ways. In the conventional Westphalian worldview, the state is the locus of both national and international lawmaking.

In transnational governance arrangements, the state is only one actor among many in the norm making process and may not be the most important or, sometimes, even present at all. Key here is that 'transnational' is not another word for 'international.' Transnational law and regulation is pluralistic and often characterised by friction between multiple or conflicting regimes. It is an area where socio-legal studies can make a real difference in charting how global power is being enacted.

One area where these regulatory changes have been profoundly felt is the domain of global security. The global 'war on terror' that followed the 9/11 terrorist attacks on the US catalysed an international state of emergency marked by visible excesses of sovereign power. From the indefinite detention of 'enemy combatants' in Guantanamo Bay, the extraordinary rendition and torture of suspects in secret black sites around the globe and massive expansion of surveillance powers to 'connect the dots' of terrorist-related information, the US-led war on terror has often been represented as a draconian example of contemporary state sovereignty in action. Yet some of the most profound and enduring regulatory changes made to threats posed by groups like Al-Qaida (AQ) and the Islamic State in Iraq and the Levant (ISIL or ISIS) are transnational in nature and scope. They engage diverse ensembles of actors into novel global security governance processes and generate norms and standards that cannot readily be explained through the traditional framework of national and international law.

In this contribution I briefly outline three key problem areas where we can observe this transnational security governance in action – (i) Terrorism Financing; (ii) Foreign Terrorist Fighters; and (iii) Terrorism and Extremism Online – before closing by highlighting a few salient points arising from this shift for the socio-legal study of transnational governance and justice struggles more generally.

1. Terrorist Financing

After the September 11, 2001 attacks on the United States, countering the financing of terrorism became a key regulatory concern. Freezing the assets of suspected terrorists, targeting them with sanctions and listing individuals and groups for providing support to terrorism is a strategy that can produce visible results in the 'war on terror' in ways that invading states harbouring terrorists (Afghanistan) and indefinitely interning suspects (Guantanamo) cannot. This approach was also consistent with the doctrine of pre-emption which began dominating security policymaking in this period. The US National Security Strategy (2002), for example, aimed to 'disrupt and destroy terrorist organisations at an early stage by denying … sponsorship, support and sanctuary'. Techniques of financial warfare and incapacitation were deemed critical towards this endeavour.

Terrorist financing is a paradigmatic trans-boundary collective action problem. If states fail to effectively co-operate in their efforts, there will be gaps in the transnational chain where financing of terrorism or potentially terrorist groups can flourish. Without a consistent approach, the actions of the reluctant few can undermine the governance efforts of the many and enable further terrorist attacks to take place.

The UN Security Council led the way, through the adoption of Resolution 1373 (2001), agreed within weeks of the September 11, 2001 attacks. It required all states to change their domestic legal systems by introducing laws that criminalise terrorism, terrorist financing and support and to freeze the assets of terrorism suspects and prohibit the provision of funds to them. It also created a Counter-Terrorism Committee to monitor implementation, and required states to report steps taken in compliance with it.

Historically, the UN Security Council had adopted resolutions in response to particular and concrete threats to international peace and security that were time-limited and would expire once the threat receded. But through this resolution, and other sweeping measures adopted since, the UNSC has transformed itself into a new kind of quasi-world government - imposing binding legal obligations (or 'global legislation') on all states in ways not tied to specific conflicts that apply indefinitely by default.

UN sanctions have also been radically expanded since 9/11 to target individual terrorism suspects and groups deemed 'associated with' Al Qaida and ISIL. The UN Al Qaida and ISIL terrorist list has been a hugely controversial mechanism of global security governance. It relies on secret intelligence and an incredibly opaque nomination process by states. It fails to provide targeted individuals with an effective remedy or access to the underlying material to challenge their listing. This list is not merely a sanctioning tool of the UN Security Council. It also puts an array of transnational regulatory arrangements into motion and is the conduit for new forms of security governance to develop. The UN expert group responsible for administering this listing regime, for example, routinely make far-reaching recommendations to the Security Council to legislate on issues such as border control practices, biometric identification and data interoperability standards to enhance implementation of the list.

Norms aimed at terrorist financing have also been translated and strengthened by a range of transnational regulatory bodies. The Financial Action Task Force (FATF) was originally set up by the G7 group of wealthy nations to combat money laundering, but after 9/11 its mandate was extended to include terrorist financing. The FATF is a powerful transnational standard-setting and policy diffusion network. The key regulatory instruments it uses include: the 40 FATF 'International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation', the detailed interpretative guidance on how these standards should be applied, best practice guidelines and a regular 'mutual evaluation' process (akin to peer review) to monitor compliance and identify high-risk jurisdictions. Whilst these standards are technically non-binding, non-compliance can have powerful and coercive effects. Jurisdictions identified as deficient are subjected to corrective Action Plans and publicly identified as high-risk, effectively rendering them pariah states in the global economy until they introduce regulations that meets FATF standards.

Not for profit and charitable organisations have been singled out by the FATF for being at particular risk of 'terrorist abuse'. This has facilitated crackdowns on human rights defenders and restrictions on NGOs and civil society organisations by repressive governments under the guise of countering terrorism. Humanitarian, peacebuilding and development organisations now have to comply with norms aimed at terrorist financing control as condition of their funding. This has securitised their work in far-reaching ways and lead to some aid agencies withdrawing from conflict zones under de facto control by listed groups (such as in Somalia). Money transfer businesses crucial for transferring remittances from diaspora communities to family members in countries like Somalia have also been severely restricted as a result of terrorist financing norms and the 'de-risking' practices of large banks. In such ways, counterterrorist financing norms are disproportionately targeting Muslim communities.

The FATF requires states to create Financial Intelligence Units for collecting and analysing 'suspicious action reports' from financial institutions, placing banks on the frontline of transnational norm implementation. This privatisation of global counterterrorism governance has spawned a massive industry in compliance and risk mitigation software. Data companies like World Check compile more than 400 sanctions and watchlists into a database for financial institutions and others to do due diligence checks to 'Know your Customer'. They also create their own listings of individuals and organisations that World Check deem to be risky or associated with terrorism, based on publicly available sources (including online news stories, court records and blogs). Individuals removed from formal sanctions lists (like those of the UN Security Council) often remain on the World Check database and are left unable to open a bank account or work as a result. In these ways, public and private governance and formal and informal norms work together to control risky financial flows.

2. Foreign Terrorist Fighters

After the Islamic State declared a worldwide caliphate in Syria and Iraq in 2014 around 12,000 foreign fighters from more than 80 countries travelled to join the fight with them. By 2015 this number had swollen to almost 30,000 foreign fighters from 100 countries. Since the caliphate's collapse, the key security issue has become about identifying and controlling the movements of these people and governing the threat they pose as they seek to return home. The 'foreign terrorist fighter' threat is another paradigmatic transboundary security problem: a globally diffuse risk difficult to counter using conventional tools of national and international law.

In response, the Security Council adopted resolutions that introduce sweeping measures to stem the flow of people travelling to and from conflict zones to fight, train with or support terrorist groups. Like earlier Council measures, Resolutions 2178 (2014) and 2396 (2017) are 'global legislation' that impose binding obligations on all states to change their legal frameworks. Yet these measures go much further by putting far-reaching transnational data infrastructure programs into motion that require new forms of information exchange, public-private collaboration and data-driven governance.

Commercial airlines, for example, are required to provide Advance Passenger Information to states for algorithmic analysis and states must 'intensify and accelerate the exchange of operational information' across a range of different areas and formats. Systems for collecting and analysing Passenger Name Record from the aviation industry and biometric data must be developed to identify terrorists and 'foreign terrorist fighters'. Watchlists and databases of known or suspected terrorists are to be constructed for screening all travellers and conducting 'evidence-based traveller risk assessment[s]'. All this data should be shared 'responsibly' with other states and organisations like Interpol, and widely distributed amongst law enforcement, border security, customs, military and intelligence agencies in ways that comply with international human rights and the rule of law.

This governance is extended by the Global Counterterrorism Forum (GCTF), which defines itself as an 'informal, a-political, multilateral counterterrorism platform'. The GCTF was designed by the US as an expert-led and action-orientated body, structured around a number of transnational thematic working groups. It produces best practice guidelines to assist states and others to meet their security governance obligations, channels technical expertise to support technical capacity building across different areas (from watchlisting to countering violent extremism) and promotes 'flexible partnerships' between a range of public, private and civil society actors. Despite their 'soft law' status, informal GCTF norms often shape more formal international lawmaking processes like those of the UN Security Council.

The 'foreign terrorist fighter' has also catalysed swathes of other informal best practice initiatives and collaborative governance programs that overlap and compete for dominance. Concerned by the clear threats that the resolutions and practices mentioned posed to the protection of human rights, in

2018 the UN Office for the High Commissioner for Human Rights produced a guidance document for states with best practices on human-rights compliant responses to the 'foreign terrorist fighter' threat. The UN Counter-Terrorism Committee similarly produced the *Madrid Guiding Principles on Foreign Terrorist Fighters*, consisting of 52 'practical tools' to help states stem the flow of FTFs. The guiding principles are non-binding, but like the GCTF memoranda that many of them build upon, they have been endorsed by the Security Council – which bolsters their legitimacy and power as transnational norms.

The *Countering Terrorist Travel Programme* (CTTP), launched in 2019 by the UN Office of Counter-Terrorism, globally coordinates capacity building to collect and analyse aviation data. It aims to share targeting rules between states, standardise protocols for transnational data exchange and disseminate best practices for stopping terrorist travel. The CTTP works closely with a wide range of UN agencies as well the International Civil Aviation Organization, the International Air Transport Association, and Interpol. One of the main aims of the CTTP is to provide states with expertise needed to establish dedicated Passenger Information Units for the collection and algorithmic analysis of passenger data. They have also made targeting software (*goTravel*) available to states to support automated data analysis.

Together these measures are constituting an increasingly thick web of transnational norms and regulatory obligations both formal and informal in nature. A diverse array of actors and institutions – from the Security Council and other UN agencies and organisations like Interpol and international air transport organisations, civil society organisations, security think-tanks, radicalisation experts, national states and private bodies – are all immersed in this legal work and competing to exert influence. Building and interconnecting new information infrastructures for transnational data-driven governance to identify and stop 'risky' travellers before they board planes or cross borders is widely seen as the key way to effectively counter the 'foreign terrorist fighter' threat. This regulatory work is constructing new forms of transnational surveillance and movement control that apply to all travellers, altering the ways borders are enacted and building capacity for pre-emptive security to proliferate around the globe, with potentially grave consequences for the protection of rights.

3. Terrorism and Extremism Online

The sophisticated use of the Internet by ISIL to recruit fighters from other countries to Syria and Iraq made terrorist use of the internet and online extremism an urgent issue of global security concern. As the former UN Secretary General Ban Ki-Moon put it, ‘The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner’. But both states and international organisations are limited in what they can do to prevent online extremism because much of the Internet’s infrastructure and data is administered by the world’s privately-owned Internet platforms. Social media platforms used to argue that it wasn’t their responsibility to regulate online extremist content, but rather the responsibility of governments. But with such phenomena as the livestreaming of terrorist attacks, powerful states (UK, France and Germany), regional bodies (EU) and intergovernmental organisations (G7) have pressured platforms to proactively regulate online terrorism and extremism and take Internet content moderation more seriously. As a result, online terrorism is now subject to novel transnational governance arrangements involving private platforms, states and IOs, using mostly private norms and regulatory techniques along with machine learning algorithms and other digital technologies to ‘clean’ the Internet.

In June 2017, for example, four of the world’s largest tech companies – Microsoft, YouTube, Twitter and Facebook – launched the *Global Internet Forum to Counter Terrorism* (GIFCT). The GIFCT was set up by the tech industry as a voluntary self-regulation initiative to disrupt the promotion of extremist propaganda online. It also administers a program of knowledge-sharing and technical collaboration between larger and smaller platforms and formulates best-practices for transnational governance in this area. The EU was threatening to regulate and fine platforms for failing to remove extremist content at the time of its inception. The GIFCT was advanced by platforms to offset this move by showing that a ‘for-industry, by-industry’ approach works better. But at the time of writing, the Forum is being reconstituted as an industry-funded independent organisation.

Each of the platforms involved have different policies, Terms of Service and other private norms for defining and enforcing the removal of offending content. YouTube governs violent extremism using policies on hateful and violent content that prohibit material deemed ‘shocking, sensational or gratuitous’. In addition, it relies on the US Foreign Terrorist Organisation list and UK List of Proscribed Terrorist Groups or Organisations to remove ‘content intended to recruit for terrorist organizations’. Facebook has its own ‘Dangerous Individuals and Organizations’ policy that regulates material from ‘any organizations or individuals that proclaim a violent mission’, which include far-right groups such as the English Defence League and so goes much further than any government proscription list. They also use their own internal definition of terrorism to govern terrorist content, which has been criticised as too broad and imprecise by UN human rights experts.

All of this private regulatory activity is taking place within a context where there is no internationally agreed definition of terrorism or extremism. So, each of the large platforms is effectively endorsing and exporting particular domestic definitions of terrorism around the globe, generating a private transnational legal ordering that is reshaping how terrorism and extremism should be governed.

Algorithmic governance and other digital technologies are critical in this regulatory space because of the immense global scale in which platforms have to moderate online content. 98% of the videos YouTube removes for violent extremism, for example, are detected by machine-learning algorithms. But how such algorithms associate scraps of data to infer 'terrorism' or 'extremism' remains opaque, presenting complex accountability and governance problems. When YouTube began using machine learning to detect extremist content online, thousands of videos documenting human rights violations and potential war crimes in Syria by independent news agencies and bloggers were automatically deleted. When those affected complained, YouTube said their algorithmic processes for detecting extremist content were new and they advised users to add metadata to their content so the algorithms could learn to differentiate terrorist propaganda videos from news coverage of violence more effectively. After the 2019 terrorist attack in Christchurch, New Zealand, was livestreamed on Facebook and circulated on Twitter, both platforms were roundly criticised for their ineffective response. Yet the key problem was that their algorithms for detecting terrorist content had been largely trained on the basis of how Islamist users behave, not far-right white supremacists, so platforms failed to spot it.

Another crucial governance technology used by the GIFCT to regulate online terrorism and extremism is the Hash-Sharing Database. A hash is a unique digital 'fingerprint' of an image or video file. Because the same files have the same hash, hash databases can quickly identify duplicates online and automate their removal. There are more than 200,000 unique hashes of 'known terrorist images and videos' in the GIFCT database. It was used by Facebook after the Christchurch terrorist attacks to remove 1.5 million online videos of the attacks within 24 hours. As a result, this database has been widely touted by the GIFCT platforms as an effective regulatory instrument. Yet how offending content is classified, included, shared and removed from the database remains poorly understood. Because it removes all copies of flagged content across all platforms and jurisdictions in which the platforms operate, there is a clear risk that legitimate online expression may be indefinitely and globally deleted without any form of redress by being included in the hash-database.

The GIFCT is not the only transnational governance platform active in this space. In 2019, after the Christchurch attacks, France and New Zealand convened the Christchurch Call to Action Summit. The summit, attended by numerous states and the world's leading Internet platforms, adopted the *Christchurch Call*. The Call is an informal 'action plan' in which states and platforms pledge to work collaboratively and commit to a range of voluntary rules to eliminate terrorist and extremist content from the Internet. It operates as a multi-stakeholder initiative or transnational public-private partnership, with no binding powers or enforcement mechanisms. The Call has rapidly grown since inception and currently includes 50 states, 8 leading online service providers (including Amazon, Facebook and Google), the Council of Europe, UNESCO, the European Commission, and an Advisory Network of more than 40 civil society organisations. As with the GIFCT, the Christchurch Call is imbricated in extending new forms of privatised governance on the Internet. This transnational governance is enacting and reshaping rights (eg, to freedom of expression) through the technical design choices and user agreements deployed by platforms to regulate online security.

Conclusions

The landscape of contemporary transnational governance is dynamic, diffuse and exponentially expanding. Powerful actors are increasingly opting for faster and more flexible regulatory solutions to cross-border problems than multilateral diplomacy has traditionally provided. And as new actors are enrolled into transnational norm-making processes, the scope of this governance is broadened even further. The foundational principles that have defined national and international law (eg, 'the state', 'sovereignty', 'international authority', 'human rights', 'public/private') no longer work in the ways they once did. There are huge stakes involved in these transformations: the strengthening of global hegemonic powers, deepening economic immiseration and inequality, the erosion of rights and freedoms, the emergence of new forms of domination and the diminishing capacity to hold the powerful accountable through legal means. Yet this reordering is also an opening for socio-legal studies to chart and critique new architectures of transnational power and thus contribute to emergent justice struggles around the world.

Many of the shifts in transnational security governance outlined above aren't being enacted through traditional formal laws but through a diverse array of other regulatory devices. These include best practice guidelines, global legislation, lists and databases, forms of standardisation, transnational data exchange networks, data infrastructures, Terms of Service and algorithms. Empirical socio-legal scholarship is uniquely placed to follow how these devices are reassembling social, political and legal relations. Rather than engaging in abstract debates about what law and authority *is*, socio-legal studies can redefine the terms by showing *how* transnational legal ordering and power are unfolding in practice. Informal norms (like those generated by the FATF and GCTF) are reshaping formal laws and interacting in complex ways. Platforms, 'action plans' and other flexible regulatory initiatives are increasingly being used to govern global problems instead of more traditional forms of organisation. Private actors (like banks, airlines and Internet platforms), once reluctant followers of counterterrorism laws, are increasingly being enrolled into doing frontline security governance work. New forms of security expertise and novel assemblages of actors are empowered through these shifts and older forms of authority are recomposed, rather than replaced. And as in other regulatory fields, the prolific spread of algorithmic decision-making and predictive analytics is radically transforming the way security is done. Mapping how norms circulate and are embedded, unmasking the operations of global power and articulating the possibilities for justice is something socio-legal studies can do very well. The stakes have never been higher.

Selected Further Readings

Nathanael Tilahun Ali, *Regulatory Counter-Terrorism: A Critical Appraisal of Proactive Global Governance* (Routledge, 2018)

Keller Easterling, *Extrastatecraft: The Power of Infrastructure Space* (Verso, 2014)

Alejandro Rodiles, *Coalitions of the Willing and International Law: The Interplay between Formality and Informality* (Cambridge University Press, 2018)

Isobel Roele, *Articulating Security: The UN and its Infra-Law* (Cambridge University Press, forthcoming)

Gavin Sullivan, *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law* (Cambridge University Press, 2020).

Peer Zumbansen (ed.), *Oxford Handbook of Transnational Law* (Oxford University Press, 2020)