

From ‘Terrorizing the Other’ to Securitising All: The Turn towards Coercive Identity Management

Author(s)	Dr. Romyana van Ark*
Contact	R.vanArk@asser.nl
Affiliation(s)	Dr. Romyana van Ark (née Grozdanova) is a Senior Researcher in International Law at the T.M.C. Asser Institute of the University of Amsterdam
Keywords	Identity, digitalisation, risk, security, borders, counter-terrorism, immigration, citizenship, governance, rights
Published	Published: 31 Mar 2026

Citation Dr. Romyana van Ark, From ‘Terrorizing the Other’ to Securitising All: The Turn towards Coercive Identity Management, *Technology and Regulation*, 2026, 28-43 • 10.71265/7372ae11 • ISSN: 2666-139X

Abstract

The management of individuals and their physical and digital identities has become vital to contemporary security and border governance. In targeting a certain set of ‘unsafe’ individuals deemed to pose a threat to national security, states’ multi-layered counter-terrorism toolkits have enabled a downward recalibration of the rights of these individuals; a recalibration that has since become both palatable and entrenched. With the ever-increasing reliance on new and emerging digital solutions to existing and perceived future security risks, individual physical identities have been gradually translated into, arguably *narrower*, digital identities. As a corollary, the recalibration has not only shifted further downward but now impacts a much larger set of individuals depending on national and international political priorities.

* Romyana van Ark is Senior Researcher in International Law and Security at the TMC Asser Institute of the University of Amsterdam Law School, the Netherlands. The author would like to thank the participants of the “Security in the Digital Age” workshop (Erasmus School of Law), the editors of the “*Security, Digital Infrastructure & Fundamental Rights*” special issue and the peer reviewers for their insightful comments and suggestions.

1. Introduction

Identities' management through technology has become a vital component of contemporary (trans)national security governance.¹ Whether on behalf of individual states such as the United States (US)² or supranational organisations like the European Union (EU) and the United Nations (UN), this management has further enhanced the reach of the already comprehensive security toolkits aimed at early mitigation of threats and risk pre-emption.³ Spurred on by various UN Security Council (UNSC) Resolutions and EU instruments, especially since the early 2000s, many states have vastly expanded their immigration, criminal law, counterterrorism and other security provisions. More effective border control infrastructures, improved procedures *vis-a-vis* the administration around identity and/or travel documents and intensified information exchange in respect of the movements of certain actors were some of the many means utilised to enhance (trans)national security toolkits at an operational level. Through a range of hard and soft regulatory recommendations, the UNSC has also facilitated and stimulated the expansion of various surveillance practices and intelligence-gathering mandates such as the collection of API/PNR data lists,⁴ the implementation of biometric identification of travellers and the development of (trans)national counterterrorism watchlists.⁵

Within the EU, the Prüm I framework enabled participating states to exchange anonymised DNA and fingerprint data, certain vehicle registration data, and associated policing information for the prevention and investigation of criminal offences.⁶ The ensuing wide spread embedding of biometrics⁷ and the ubiquitous reliance on expansive databases containing DNA profiles, fingerprints and other individual identifiers have since normalised a so-described regime of 'governing by identity'.⁸ For others, states' persistent efforts to find innovative and dependable means to categorise individuals into 'knowable' and therefore governable and 'unknowable' and thus a potential threat are part of the broader 'governing through risk'⁹ security

- ¹ See for example Katja Franko Aas, 'The body does not lie': Identity, risk and trust in technoculture' (2006) 2 (2) *Crime, Media, Culture* 143; David Lyon, 'Biometrics, Identification and Surveillance' (2008) 22 (9) *Bioethics* 499; Benjamin Muller, *Security, Risk and the Biometric State: Governing Borders and Bodies* (1st edn, Routledge 2010) or Tasniem Anwar and Klaudia Klonowska, 'The Techno-Legal Co-production of Terrorist Suspects' (2025) 7 (1) *Law, Technology and Humans* 139.
- ² In 2008 the US proposed the "Server in the Sky" programme aimed at swift exchange of biometric measurements, irises and/or palm prints to streamline and enhance cooperation between police services beyond sharing fingerprints. Owen Bowcott, 'FBI wants instant access to British identity data' *The Guardian* (15 January 2008) https://circ.jmellon.com/docs/html/fbi_wants_instant_access_to_british_identity_data.html accessed 17 July 2025. While this particular proposal does not seem to have proceeded, in 2022 the US offered other states access to 1.1 billion biometric "encounters" in return for reciprocal database access through so called 'Enhanced Border Security Agreements'. 'USA offers foreign states access to 1.1 billion biometric "encounters" in return for reciprocal database access' *Statewatch* (22 July 2022) <https://www.statewatch.org/news/2022/july/usa-offers-foreign-states-access-to-1-1-billion-biometric-encounters-in-return-for-reciprocal-database-access/> accessed 17 July 2025.
- ³ Especially through its law-making UNSC Res 1373 (28 September 2001) Un Doc S/RES/1373 since reaffirmed by a few others. Aside from the text of UNSC Res 1373 itself see also commentary in Richard Ashby Wilson, *Human Rights in the 'War on Terror'* (Cambridge University Press 2005); Stefan Talmon, 'The Security Council as World Legislature' (2005) 99 (1) *American Journal of International Law* 175; Jose E Alvarez, 'The UN's 'War' on Terrorism' (2003) 31 (2) *International Journal of Legal Info* 238 and Matthew Happold, 'Security Council Resolution 1373 and the Constitution of the United Nations' (2003) 16 (3) *Leiden Journal of International Law* 600.
- ⁴ UNSC Res 2396 (21 December 2017) UN Doc S/RES/2396.
- ⁵ See further the Counterterrorism Watchlisting Toolkit, developed under the auspices of the Global Counterterrorism Forum and in collaboration with some UN institutions. 'The Counterterrorism Watchlisting Toolkit' (*GCTF*, October 2021) <https://www.thegctf.org/Resources/Framework-Documents/Policy-Toolkits/Counterterrorism-Watchlisting-Toolkit> accessed 17 July 2025.
- ⁶ See further information through here: 'Stepping up cross-border cooperation – the Prüm decision' (*European Union*, 3 June 2024) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:jl0005> accessed 18 July 2025 and 'Cross-border cooperation (Prüm Treaty)' (*European Data Protection Supervisor*, 4 April 2007) https://www.edps.europa.eu/data-protection/our-work/publications/opinions/cross-border-cooperation-pr%C3%BCm-treaty_en accessed 18 July 2025. The recent Prüm II introduced new data exchange categories, including facial biometric matching and pseudonymised police records.
- ⁷ Muller has described biometrics as "simply physiological characteristics in digital form" with the most commonly relied on being "digital fingerprints, iris and/or retinal scans, and facial recognition." Muller (n 1) 16.
- ⁸ Lyon (n 1) 500 – 502.
- ⁹ Or "the need (and possibility) of measuring, preventing, and pre-empting all imagined sources of harm". Benjamin Muller, 'Unsafe at any speed? Borders, mobility and 'safe citizenship'' (2010) 14 (1) *Citizenship Studies* 75, 77. For Ericson, this type of governance – or security strategy – is saturated with the desire and motivation to "cast the net as widely as possible, identify suitable enemies, [and] not worry about false positive identifications.' Richard V. Ericson, *Crime in an Insecure World* (Polity Press 2007) 48. See also Marieke de Goede, 'The Politics of Preemption and the War on Terror in Europe' (2008) 14 (1) *European Journal of International Relations* 161.

strategies. These strategies have driven the (re)construction and growing reliance on wide reaching risk pre-emption measures such as deprivation of citizenship¹⁰ and watchlists.¹¹

As a corollary development, individual physical identities have been gradually translated into, arguably *narrower*, digital identities. Anchored on digitally-traceable activities such as travel history and online social media behavioural patterns, these narrower identities are increasingly relied on to determine whether an individual is a security threat.¹² To put it differently, in aiming to fulfil their numerous legal, policy and operational undertakings,¹³ states have voluntarily – and *determinately* – created pathways towards downward rights recalibration¹⁴ of their relationship with certain individuals. This recalibration has since become both *entrenched* and *publicly acceptable*.¹⁵ Moreover, as the initially temporary expansive (trans)national legislative, policy and operational measures have become first palatable and subsequently embedded,¹⁶ this recalibration no longer affects only those suspected of terrorist activity. Those who *may* become a terrorist,¹⁷ those who are unknown to the state and thus might potentially be a security threat or those who have somehow challenged the state’s capacity to determine who poses a risk and why¹⁸ have also experienced this recalibration. The ever-changing national and international political and security priorities threaten to expand the net even further with the hostility towards those seeking entry in flight from conflict zones, poverty or the impact of climate change continues to grow and, at times, reaches crescendo levels.¹⁹ Regrettably, as the below discussions will aim to demonstrate, a folding of the widely cast security net seems unlikely.

The distinct effects of the persistent tightening of border security management regimes, the expansion of immigration and criminal justice measures and the increasing reliance on various technological developments even before the early 2000s is well documented. Yet, the enduring impact within and beyond

¹⁰ See the varied works of Prof. Devyani Prabhat (University of Bristol) and Prof. Lucia Zedner (University of Oxford) on citizenship, immigration and border control.

¹¹ Gavin Sullivan, *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law* (Cambridge University Press 2020) and Ramzi Kassem, Rebecca Mignot-Mahdavi and Gavin Sullivan, “‘Watchlisting the World: Digital Security Infrastructures, Informal law, and the ‘Global War on Terror’” (*Just Security*, 28 October 2021) <https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/> accessed 17 July 2025.

¹² In a 2005 commissioned report, it was expressly noted that physical identities were increasingly being replaced and/or supplemented by digital ones due to the broader needs of the emerging “networked Information Society”. This required the design and development of “more and better means of identification” through (enhanced) biometric technologies. Improvement in overall security was highlighted as the “main reason for introducing biometric systems”. European Commission Directorate-General Joint Research Centre, ‘Biometrics at the Frontiers: Assessing the Impact on Society’ (February 2005) EUR 21585 EN.

¹³ Undertakings here refers to commitments and obligations flowing from various UNSC Resolutions, regional treaty obligations and/or soft law instruments aimed at mitigating and/or preventing various risks predominantly associated with terrorism. The library of resources of the Global Counterterrorism Forum (GCTF) offers a fascinating insight into the various soft law instruments – and priority areas – of an illustrative set of states since the 2010s: Global Counterterrorism Forum <https://www.thegctf.org/> accessed 18 July 2025.

¹⁴ The concept of ‘downward recalibration’ of rights has been discussed in detail in Fiona De Londras, *Detention in the ‘War on Terror’: Can Human Rights Fight Back?* (Cambridge University Press 2011) and Helen Fenwick, ‘Recalibrating ECHR Rights and the Role of the HRA post 9/11: Reasserting International Human Rights Norms in the ‘War on Terror?’ (2010) 63 (1) *Current Legal Problems* 153.

¹⁵ The prevailing public attitude towards Shamima Begum – and those suspected of terrorist activities in general – is one particularly illustrative example.

¹⁶ See for example Helen Duffy, *The ‘War on Terror’ and the Framework of International Law* (2nd edn, Cambridge University Press 2015); Laura Donohue, *The Cost of Counter-Terrorism: Power, Politics and Liberty* (Cambridge University Press 2008); Victor V Ramraj, *Global Anti-Terrorism Law and Policy* (2nd edn, Cambridge University Press 2012); Aniceto Masferrer and Clive Walker, *Counter-Terrorism, Human Rights and the Rule of Law* (Edward Elgar Publishing 2013).

¹⁷ Romyana van Ark, Devyani Prabhat and Faith Gordon, *Children’s Rights, ‘Foreign Fighters’ and Counter-Terrorism: Children of Nowhere* (Edward Elgar Publishing 2024).

¹⁸ ‘Global Study on Counter-Terrorism & Civic Space’ (*United Nations Human Rights Special Procedures*, 2023) <https://defendcivicspace.com/> accessed 17 July 2025

¹⁹ Valsamis Mitsilegis, ‘Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State’ (2012) 19 (1) *Indiana Journal of Global Legal Studies* 3; Mary Bosworth, Katja Franko Aas and Sharon Pickering, ‘Punishment, Globalisation and Migration Control’ (2018) 20 (1) *Punishment & Society* 34 and Lucia Zedner, ‘Citizenship Deprivation: Punishment or Rights Revocation?’ in Bosworth M, Franko K, Lee M and Mehta R (eds) *Handbook on Border Criminology* (Edward Elgar Publishing 2024).

states' borders *after* certain extensively scrutinised terrorist events make it rather difficult not to describe them as *the* crucial transformational impetus behind the almost unbridled widening of the security net after the early 2000s. By building on the existing literature, the following sections will aim to demonstrate not only *why* these events have had such a transformative impact but *how* they have been utilised to (turbo) accelerate and normalise the voracious security pursuit towards making individuals (much) more knowable and thus governable in a variety of contexts. Other reflections on these questions have focused on specific components of the pursuit such as identity and risk management through biometrics or watchlists or the impact of specific security or immigration measures on (certain groups of) individuals and the corollary negative effects on rights protections. The more expansive assessments, have directed their critical gaze at the various infrastructures designed to more efficiently counter, mitigate and prevent terrorism and violent extremism.

This contribution will aim to illustrate how much 'further a field' governing through risk now takes place with even the infrastructures around mega sporting events increasingly becoming part of the broader (trans)national security toolkits. What is perhaps the most concerning, and still to be more extensively evaluated, aspect of this development is the willingness of many individuals to voluntarily contribute to the (re)construction of their own identities as well as those of others through the volitional surrender of core personal data. Highlighting some illustrative examples of *how* and *why* this occurs will be the focus of Section 3. Section 1 will provide the backdrop by reflecting on how the ever-expanding counter-terrorism framework has served as a particularly nifty floodgate the opening of which has facilitated and galvanised both the expansion *and* amalgamation of a set of previously mostly parallel developments. The result – a recurrent, and arguably relentless, (re)calibration of the relationship between the individual and the state with the set of affected individuals constantly expanding. By thus 'terrorising' identities through the various multifaceted measures available in domestic and transnational security toolkits, the scale and reach of the voracious pursuit for enhanced security has transcended significantly beyond any previous similar attempts as Sections 2 and 3 will aim to sketch out.

2. (Re)Evaluating and (Re)Constituting Belonging in the Name of Security

The (re)categorisation of individuals based on the 'right/wrong' credentials – i.e. the requisite paperwork, valid citizenship and/or immigration status – and the corollary designation of worthiness or not, inclusion or exclusion, permission or refusal of admission is not a new phenomenon. For as long as there have been modern states, those tasked with managing and securing internal and external state borders have been required to distinguish between those who can and cannot (re)enter and enjoy the full protections and opportunities a state has to offer. Citizenship by its nature is, after all, inherently exclusive as defining a state's citizenry is simultaneously confirming who is not a citizen.²⁰ It is also a vital constituent element of state-individual relations when defining, conferring, extending or withdrawing membership within a (political) community.²¹ Although the most common means to (re)enforce non-citizenship and not belonging is at border crossings, citizenship can also be revoked, withdrawn or lost through fundamental changes in the nature of the state (e.g. civil war) or *via* new or revived legislative means.²² Endowing citizenship – or certifying belonging – has thus always been within the purview of the state; as past and more recent history indicates this endowment is not necessarily permanent. When (re)evaluating and (re)certifying belonging, ever since efforts were first made during the 19th century to rely on the body itself as a key source

^{20.} Matthew J Gibney, 'Who should be included? Non-citizens, Conflict and the Constitution of the Citizenry' in Stewart F (ed) *Horizontal Inequalities and Conflict: Understanding Group Violence in Multiethnic Societies* (Palgrave Macmillan 2008).

^{21.} Rainer Bauböck, and Vesco Paskalev, 'Cutting Genuine Links: A Normative Analysis of Citizenship Deprivation' (2015) 30 (1) *Georgetown Immigration Law Journal* 47 and Katja Franko, 'On the Relevance of Citizenship in Criminal Law: Implications for Proportionality, Equality, and Justice' (2023) 11 (2) *Bergen Journal of Criminal Law and Criminal Justice* 1.

^{22.} Lucia Zedner, 'Is the Criminal Law only for Citizens? A Problem at the Borders of Punishment' in Katja Franko Aas and Mary Bosworth *The Borders of Punishment* (Oxford University Press 2013) 45 and Sangeetha Pillai and George Williams, 'Twenty-First Century Banishment: Citizenship Stripping in Common Law Nations' (2017) 66 (3) *International Comparative and Law Quarterly* 521. "While security-based revocation has been described as historically "not unprecedented" in common law countries such as the United Kingdom and Australia, the recent revival is "nonetheless remarkable, as it follows decades of disuse in each country" 523.

of identifying data,²³ states have attempted various means to ‘code’ or categorise bodies.²⁴ The core aim of this coding – transform bodies into functioning as ‘passwords’ as means of establishing stable and easily verifiable identities.²⁵ It was not until the early 2000s however that the requisite (trans)national political will, legal, policy and operational frameworks and private-public partnerships came into place to facilitate the technological advances and infrastructures needed to achieve this goal.²⁶

2.1 Redefining the Scope and Reach of Trans(National) Security Toolkits

A key galvanising factor – perhaps *the* key one – was the moral and security panic²⁷ or “dread risk”²⁸ triggered by terrorist events such as those on 11 September 2001. The scale of the destruction, the callousness of the attack and the number of casualties arguably touched a chord within the international community in a manner previous terrorist attacks had not.²⁹ States’ abilities to ensure (trans)national security, to effectively protect the public and the integrity of the (inter)national order in a world increasingly reliant on transnational networks was challenged in an unprecedented manner.³⁰ The ensuing intense moral panic and fear of whether/when another attack might occur continued to linger and were re-flamed following subsequent highly publicised attacks such as those on 7 July 2005 in London³¹ or on 13 November 2015 in Paris³² or due to the so-defined “foreign terrorist fighters”³³ phenomenon from approximately 2014 onwards. States had to be seen to respond forcefully or, to quote former President George W. Bush, “every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war” had to be used for “the destruction and the defeat of the global terror network”.³⁴

Within 7 days of these comments, UN Security Council Resolution (UNSCR) 1373 delivered the “by all means necessary” blueprint.³⁵ In what has since proven to be a particularly consequential recommendation,³⁶ by expressly urging states to ensure that refugee status is not abused by *prospective* terrorists, the operational clauses of the Resolution both encouraged and enabled states to intertwine national security considerations with immigration status *and* criminal law provisions. While this interlinkage was a first within the range of

²³ Lyon (n 1) 504 – 505.

²⁴ Aas (n 1) 143.

²⁵ Aas (n 1) 143.

²⁶ John Torpey *The Invention of the Passport: Surveillance, Citizenship and the State* (Cambridge University Press 2000); David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001) and Aas (n 1).

²⁷ The impact of moral panics is magisterially discussed in Stanley Cohen, *Folk Devils and Moral Panics* (3rd edn, Routledge 2002). See also David Jenkins, Amanda Jacobsen and Anders Henriksen, *The Long Decade: How 9/11 Changed the Law* (Oxford University Press 2014); Arianna Vidaschi, and Kim Lane Scheppelle (eds), *9/11 and the Rise of Global Anti-Terrorism Law* (Cambridge University Press 2021) (Kindle edition) and Fiona De Londras, *The Practice and Problems of Transnational Counter-Terrorism* (Cambridge University Press 2022) amongst numerous other contributions on this point.

²⁸ Lyon (n 1) 503. For Lyon, terrorism is a ‘dread risk’ or a (very) low probability event the consequences of which are perceived as so dramatic that ‘zero risk’ elimination options are favoured over mere threat management.

²⁹ Jenkins and others (n 27) 5.

³⁰ Jenkins and others (n 27) 9.

³¹ London Assembly, ‘Report of the 7 July Review Committee’ (*Greater London Authority*, June 2006) https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/archives/assembly-reports-7july-report.pdf accessed 18 July 2025.

³² ‘Paris attacks: What happened on the night’ *BBC* (9 December 2015) <https://www.bbc.com/news/world-europe-34818994> accessed 17 July 2025.

³³ See amongst others Marnie Lloyds, ‘Foreign Fighters under International Law and Beyond’ (2017) 18 (1) *Melbourne Journal of International Law* 95; Andrea de Guttry, Francesca Capone and Christophe Paulussen *Foreign Fighters under International Law and Beyond* (T.M.C Asser Press 2016), Francesca Capone and others, *Returning foreign fighters: responses, legal challenges and ways forward* (T.M.C. Asser Press 2023) and John Ip, ‘Reconceptualising the Legal Response to Foreign Fighters’ (2019) 69 (1) *International and Comparative Law Quarterly* 103.

³⁴ See further ‘Transcript of President Bush’s Address’, *CNN News* (21 September 2001) <http://edition.cnn.com/2001/US/09/20/gen.bush.transcript/> accessed 17 July 2025.

³⁵ UNSC Res 1373 (n 3) was adopted on 28 September 2001 while the comments were made on 21 September. The full text of the Resolution is available at United Nations Security Council ‘Resolution 1373 (2001)’ (*United Nations*, 28 September 2001) https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf accessed 18 July 2025.

³⁶ UNSC Res 1373 (n 35). See also the various discussions in Wilson (n 3).

UNSCRs focused on combatting various aspects of terrorism,³⁷ it has since become commonplace across international, regional and domestic instruments. The newest Eurodac legislation, for example, now permits border control authorities to store not only fingerprints but also facial images of asylum seekers with the age for allowed collection lowered from 14 to 6.³⁸ Article 36 expressly notes that “the expansion of the scope of and simplification of the access to Eurodac for law enforcement purposes should help Member States deal with the increasingly complicated operational situations and cases involving cross-border crimes and terrorism” which have a direct impact on EU security. Furthermore, the revised “conditions for access to Eurodac for the purposes of the prevention, detection or investigation of terrorist offences” should now better facilitate Member States’ law enforcement authorities in tackling cases of suspects using multiple identities. The provisions of Article 36 echo those of various UNSCRs starting from 1373 which urged states to prevent the movement of “terrorist persons or networks” through improved measures to thwart the use of counterfeit documents or fraudulent use of valid documents as well as accelerated exchange of operational information in respect of forged or falsified travel documents usage.

It is important to note that the binary merger of immigration and criminal law – or ‘cimmigration’³⁹ – principally applying to the criminalisation of arriving migrants was already taking shape before the early 2000s. Triggered by the siren call of security, the scope and substance of criminal law and immigration measures have changed even more significantly in the two last decades.⁴⁰ “Terrorizing criminal law” is how Zedner described the consequences of the numerous expansions within criminal law frameworks stemming from the additions and amendments of various terrorism offences.⁴¹ The growing number and reach of domestic crimes of association (with designated/proscribed groups), planning or possession offences in respect of (*prospective*) terrorist activities and offences of inchoate (or preparatory) and *pre-inchoate* liability illustratively reflect the decidedly more preventative and coercive turn of criminal justice measures.⁴² At international level, in the backdrop of the foreign terrorist fighters (FTF) phenomenon, UNSCR 2178 appeared to request of states to criminalise domestically those travelling abroad with ‘terrorist intent’. Yet, the conduct outlined in paragraph (6(a)) of the Resolution did not reflect any instrument negotiated in the context of a multi-lateral regional or international process.⁴³ Thus, other than the text of this particular Resolution, states had no alternative basis in international law to criminalise such travel.⁴⁴ Nevertheless, the siren call of security was such that many governments went beyond what was strictly required by adopting a wide range of measures to disrupt or prevent the travel – and especially the return of alleged FTFs and their families – such as revoking travel documents or depriving individuals suspected of terrorist activities of their nationality.⁴⁵

Questions of security have thus grown to have an almost immediate relevance to criminal and immigration law both as drivers of changes in the substantive scope of measures *and* as a goal that cimmigration is

³⁷ For an overview of the relevant resources, see further ‘UNODC Teaching Module Series: Organized Crime / Counter-Terrorism / Module 16: Linkages between Organized Crime and Terrorism’ (UNODC SHERLOC) <https://sherloc.unodc.org/cld/en/education/tertiary/organized-crime/module-16/key-issues/terrorism-international-framework---general-uns-c-resolutions-on-terrorism.html> accessed 17 July 2025.

³⁸ Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of ‘Eurodac’ for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1315 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council [2024] OJ L, 2024/1358.

³⁹ Juliet Stumpf, ‘The Cimmigration Crisis: Immigrants, Crime, and Sovereign Power’ (2006) 56 (2) *American University Law Review* 367 and Katja Franko Aas and Mary Bosworth, *The Borders of Punishment: Migration, Citizenship, and Social Exclusion* (Oxford University Press 2013).

⁴⁰ Lucia Zedner, ‘Terrorizing Criminal Law’ (2014) 8 (1) *Criminal Law and Philosophy* 99.

⁴¹ Zedner (n 40).

⁴² Zedner (n 40).

⁴³ Fionnula Ní Aoláin, ‘The Ever-Expanding Legislative Supremacy of the Security Council in Counterterrorism’ in Vidaschi and Scheppele (n 27).

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*

increasingly called upon to serve.⁴⁶ In parallel, new and expanded surveillance and enforcement measures have been regularly imposed within the nation state *and* in territories overseas extending the geographical realm of border controls to hundreds or thousands of miles away from the national physical border.⁴⁷ Sanctioned by various influential international and regional instruments, the intertwining of immigration law, criminal justice, border control management, counter-terrorism and other security measures has thus arguably resulted in a much more complex and impactful security matrix beyond crimmigration and/or a ‘terrorized criminal law’. This is a matrix aimed at anticipation, pre-emption and (very) early mitigation of a wide range of present and perceived future security risks as well as detection, immobilisation and sanctioning of individual and collective security threats. Knowledge and, more specifically, *knowledge about individuals* is now the cornerstone of (trans)national security toolkits as the various agencies tasked with ensuring (trans)national and regional security aim to address and comply with distinct aspects of the security matrix.⁴⁸ In addition to managing individuals who pose a threat through technology and managing populations through crimmigration, the contemporary drive of security is now especially driven by the desire to pierce through potentially “deceptive practices of dress, language, or identity presentation” and capture the “truth of the body” by making it readable and thus knowable.⁴⁹ The trusted traveller programmes offered by the US’ Department of Homeland Security or the FAN-ID system increasingly used for mega sporting events, both to be discussed in Section 3, are a good illustration of how further a field the efforts to make individuals knowable have extended. The border is no longer a “purely geographical entity” with the desire to uncover *the* “truth of the body” at the core of this shift.⁵⁰

2.2 Optimising (Trans)national Security by ‘Terrorizing’ the Other

This desire is arguably rooted – at least partially – in the particular circumstances around how the perpetrators of 9/11 attacks managed to enter the US from abroad. While these individuals had legitimately obtained visas, there were a number of irregularities in the manner some of these were obtained.⁵¹ Regardless of the errors and inadequacies within the relevant states’ border and immigration control checks and their disastrous consequences, distinguishing between procedural (or legal) and implementation, enforcement and intelligence failures is important.⁵² The lack of coordination, collaboration and sharing of information among the relevant security, immigration and intelligence agencies within and between states, should have been dealt with as a systemic malfunction in the enforcement and implementation of existing immigration and crime prevention powers *only*.⁵³ As noted by Waldron, “given the record of the bumbling incompetence and in-fighting of American intelligence and law-enforcement agencies wielding the already very considerable powers that they had” prior to 9/11, there was no good justification to provide them with even more extensive tools and powers in the efforts to enhance effectiveness.⁵⁴ Instead, the bumbling incompetence triggered a (trans)national legislative and policy (re)drafting fever of an intensity arguably not experienced before. The result – extensive new legal, policy and operational provisions targeting a broadly defined type of criminality and set of individuals.⁵⁵ The events in Paris on 13 November 2015, the broader FTF phenomenon and, more specifically the indefinite threat of returnees,⁵⁶ resulted in a similar (re)drafting fever. The explanations of, or reflections on, systematic failures do not possess “the simplicity and emotive power of invoking the spectre of the foreigner as an intrinsic menace to national security” after

⁴⁶ Zedner (n 40).

⁴⁷ Zedner (n 19) 91.

⁴⁸ Lauren B. Wilcox, *Bodies of Violence: Theorizing Embodied Subjects in International Relations* (Oxford University Press 2015) 104.

⁴⁹ Wilcox (n 48).

⁵⁰ *Security in a Global Hub* (UK Cabinet Office Report, 2007) as quoted in Zedner (n 19) 94.

⁵¹ Many of the perpetrators had acquired new passports before obtaining the visas. Some of the passports were fraudulently doctored and some of the visa applications contained false statements. See further the National Commission on Terrorist Attacks Upon the United States, ‘The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States’ (9/11 Commission, 22 July 2004) <https://www.govinfo.gov/app/details/GPO-911REPORT> accessed 17 July 2025.

⁵² See in particular Audery Macklin, ‘Borderline Security’ in Kent Roach, *The Security of Freedom* (University of Toronto Press 2001). See also National Commission on Terrorist Attacks Upon the United States (n 51).

⁵³ Audery Macklin, ‘Borderline Security’ in Kent Roach, *The Security of Freedom* (University of Toronto Press 2001); National Commission on Terrorist Attacks Upon the United States (n 51).

⁵⁴ Jeremy Waldron, *Torture, Terror, and Trade-offs: Philosophy for the White House* (Oxford University Press 2020), (Kindle edition ch 2).

⁵⁵ Vedaschi and Scheppele (n 27) and De Londras (n 27).

⁵⁶ David Malet and Rachel Hayes, ‘Foreign Fighter Returnees: An Indefinite Threat?’ (2020) 32 (8) *Terrorism and Political Violence* 1617.

all.⁵⁷ In circumstances such as these, the general public can regrettably be less interested in the necessity, effectiveness or (il)legality of the adopted measures. The sense that “something striking and unusual is being done” against those posing a risk to prevent the occurrence of another “catastrophic moral horror” tends to dominate considerations.⁵⁸

The aforementioned security matrix – or the “something striking” – has since tended to “generate more severe outcomes, limit procedural protections, and encourage enforcement and adjudication processes that segregate non-citizens”.⁵⁹ UNSCR 1373 arguably paved some of the paths towards this downward recalibration of the rights of certain individuals in more ways than one. Human rights obligations were barely mentioned other than to tie them with the security and immigration considerations of ensuring that a prospective asylum seeker did not engage in the preparation or commission of terrorist offences.⁶⁰ Furthermore, the Resolution did not offer a definition of terrorism despite the particularly pejorative power of terrorism as a descriptor to stigmatise, dehumanise and banish individuals away from communities.⁶¹ There were no references to homegrown terrorism; it was the incoming outsider, potentially abusing refugee status and related protections, that could pose a security threat once they crossed the border. Within weeks of the adoption of UNSCR 1373, the former UK Prime Minister Tony Blair announced that increasing the ability to exclude and remove those suspected of terrorism and prevent them from abusing asylum procedures should be a priority.⁶² In a follow-up in early 2003, Blair expressly stated that the “rising tide of asylum-seekers, combined with the renewed terrorist threat was unacceptable”.⁶³ On the other side of the Atlantic, George W Bush expressly linked “non-citizens” with terrorism activities with the Military Order of November 13, 2001 on “The Detention, Treatment, and Trial of Certain Non-Citizens in the War against Terrorism”.⁶⁴ At EU level, the timing of the establishment of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) in 2004 was arguably also quite telling.⁶⁵ Until 2001, the External Border Practitioners Common Unit – a group composed of the members of the Strategic Committee on Immigration, Frontiers, and Asylum (SCIFA) and heads of national border control services – coordinated the national projects of *Ad Hoc* Centres on Border Control.⁶⁶ After 2001, “ensuring a uniform and high level of control and surveillance” was considered

⁵⁷ Macklin (n 52) 383 – 384. See also Lucia Zedner, ‘Citizenship Deprivation, Security and Human Rights’ (2016) 18 (2) *European Journal of Migration and Law* 222.

⁵⁸ Waldron (n 54).

⁵⁹ Stumpf (n 39) and Aas and Bosworth (n 39).

⁶⁰ UNSC Res (n 3).

⁶¹ On the problems with this definitional vacuum see further Ben Saul, *Defining Terrorism in International Law* (Oxford University Press 2006); Romyana Grozdanova, ‘Terrorism’ – Too Elusive a Term for an International Legal Definition?’ (2014) 61 (3) *Netherlands International Law Review* 305; Alan Greene, ‘Defining Terrorism: One Size fits All?’ (2017) 66 (2) *International and Comparative Law Quarterly* 411 and De Londras (n 27) amongst many others. See also recent comments by Professor Fionnuala Ní Aoláin, the former UN Special Rapporteur on Countering Terrorism and Human Rights, that this vacuum – or “loose space” – has facilitated the establishment of counter-terrorism which have evolved from overt crackdowns to more subtle forms of prevention and regulation. Summary of her talk ‘Former UN Special Rapporteur Discusses Global Challenges to Human Rights’ (*Yale Law School*, 3 February 2025) <https://law.yale.edu/yls-today/news/former-un-special-rapporteur-discusses-global-challenges-human-rights> accessed 17 July 2025.

⁶² HC Deb 4 October 2001, vol 372, cols 671–676.

⁶³ ‘Human Rights in the Balance’ *The Independent* (4 February 2003) <https://www.independent.co.uk/news/uk/crime/human-rights-in-the-balance-117943.html> accessed 18 July 2025.

⁶⁴ Section 2 – Definition and Policy – used the following phrasing: “the term “individual subject to this order” shall mean any individual who is not a United States citizen ... or ... (2) it is in the interest of the United States that such individual be subject to this order.” Such individuals, when captured, were to be tried within military commissions rather than the standard criminal justice framework. See ‘Military Order of November 13’ (*Federal Register Presidential Documents*, 16 November 2001) <https://irp.fas.org/offdocs/eo/mo-111301.htm> accessed 16 July 2025.

⁶⁵ Council Regulation (EC) 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union [2004] OJ L349/1. This Regulation was repealed by Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC [2016] OJ L251/1.

⁶⁶ ‘Frontex: Who We Are’ (*Frontex*) <https://www.frontex.europa.eu/about-frontex/who-we-are/tasks-mission/> accessed 17 July 2025.

necessary and of utmost importance.⁶⁷ This was the start of a progressive securitization, surveillance and militarisation of the EU's borders.⁶⁸

By further inflating the threat of insecurity and exploiting the broader domestic and international sentiments, these comments, developments and designations (re)focussed attention – rather effectively – on the outsider. The foreign national became the folk devil⁶⁹ – the source of unprecedented danger which required ever more comprehensive means to fortify internal and external borders. In his magisterial work, Cohen has compellingly reflected on the construction – and *significance* of – a suitable enemy or folk devil⁷⁰ in order to create and sustain a moral panic. When a relatable victim⁷¹ is added to the mix and a consensus emerges that the actions being denounced were not insulated but could become regular occurrences, the ensuing moral panic demands that decisive action is taken – or that “something striking and unusual” is done.⁷² Once an individual or a group has been identified as being (potentially) responsible for causing the damage or continuing to pose a threat, it is critical that the relevant institutions first swiftly assess the level of risk and then urgently implement the measures required to apprehend those responsible to thus pre-empt further occurrences of violence.⁷³ The aftermath of events such as those on 9/11, 7/7, Paris 2015 and Nice 2016 or the constantly stoked fear of FTF returnees are illustrative of the immense emotive power that can be wielded in the backdrop of needing to act decisively to prevent the occurrence of another “catastrophic moral horror”.

What the response to these events has also aptly illustrated is how significant the labelling of individuals – and events – can be in a highly charged political and public environment. The security populism, which tends to follow a well-publicised terrorist event or the foiling of a security threat, is no longer premised on the vilification of the other alone. Increasingly, it has relied on the systemic vilification of outsider groups with corollary impact on who is a ‘deserving’ or ‘underserving’ rights-bearer and, more broadly, the protections associated with being a citizen and/or (seeking) belonging to a community.⁷⁴ These politics of fear combined with the adoption of the legal, policy and operational measures to address the incalculable but potentially catastrophic threat of terrorism have thus resulted in the construction of new “suspect communities” – or “new enemies within” and outside the national border.⁷⁵ Having first ‘terrorized criminal law’ and entrenched crimmigration, the insatiable pursuit of security has thus also ‘terrorized’ the other – the folk devil, the enemy within and outside the border who is deemed to pose a threat that needs to be mitigated before another catastrophic event. When the dangers and impact of homegrown terrorism⁷⁶ became a more visible (trans)national preoccupation after the events on 7 July 2005 in London and the subsequent foiled attack on 21 July 2005,⁷⁷ the response of the then British government was rooted in the already expanded border control and immigration measures originally enacted to address external security threats. The Borders Act of 2007 granted immigration officers increased police powers of entry, search, seizure and detention

⁶⁷ Council Regulation (EC) No 2007/2004 of 26 October 2004.

⁶⁸ Katja Aas Franko and Helene O.I. Gundhus, ‘Policing Humanitarian Borderlands: Frontex, Human Rights and the Precariousness of Life’ (2015) 55 *British Journal of Criminology* 1.

⁶⁹ Stanley Cohen, *Folk Devils and Moral Panics* (3rd edn, Routledge 2002).

⁷⁰ Described as soft and easily denounced target with little power.

⁷¹ Someone with whom individuals could easily identify with.

⁷² Cohen (n 69) xii.

⁷³ Cohen (n 69) xxxii.

⁷⁴ Benjamin J Goold, and Liora Lazarus (eds), *Security and Human Rights* (2nd edn, Hart Publishing 2019) (Kindle edition ch 1).

⁷⁵ Christina Pantazis and Simon Pemberton, ‘From the “Old” to the “New” Suspect Community: Examining the Impacts of Recent UK Counter-Terrorist Legislation’ (2009) 44 *British Journal of Criminology* 646 and Goold and Lazarus (n 74) ch 6.

⁷⁶ Clive Walker, ‘“Know Thine Enemy as Thyself”: Discerning Friend from Foe under Anti-Terrorism Laws’ (2008) (32) *Melbourne University Law Review* 275. He argues that “it can no longer be claimed that the ‘enemy’ is ‘in a specially intense way, existentially something different and alien!’” 276. At international level, with UNSC Res 1611 (7 July 2005) Un Doc S/RES/1611 [on bomb attacks in London on 7 July 2005], the UNSC reminded states to “cooperate actively in efforts to find and bring to justice the perpetrators, organizers and sponsors of these barbaric acts” in “accordance with their obligations under resolution 1373 (2001)”. United Nations Security Council, ‘Resolution 1611’ (2005) <https://digitallibrary.un.org/record/552683?ln=en&v=pdf> accessed 18 July 2025.

⁷⁷ ‘Failed 21/7 London Bombers Lose Court Claim’ *BBC* (13 September 2006) <https://www.bbc.com/news/uk-37353533> accessed 17 July 2025.

irrespective of citizenship status.⁷⁸ As a more recent example, the designations⁷⁹ of trans-border criminal organisations by both the US and Canada and the exponential growth in the use of the 1798 Alien Enemies Act⁸⁰ should not be viewed as an aberration – or overreach – by a particular administration but rather as a continuation of a deeply rooted pattern. While the designations can be viewed as a (temporary) political posturing, they have also instantly opened the door for reliance on the full range of available counter-terrorism measures in respect of the targeted set of individuals. Instead of the more ‘classic’ sanctions under criminal law, these individuals can now be placed on watchlists in order to disrupt or pre-empt their travel for example. The various effects of the shifting of border control management from ports, airports and other traditional physical coordinates to within and much further beyond nation state boundaries as well as who falls within the category of the unsafe other will be examined next. With technology playing an ever bigger role in securing internal and external borders as well as transforming the body into a more knowable and thus governable digital identity, the security means and measures constructed to identify and ‘terrorize’ the other have now arguably been extended to a much larger group of individuals.

3. From ‘Terrorizing the Other’ to Securitising All

As states’ security toolkits to address and mitigate against cross-border crime, international and domestic terrorism, and politically unwanted migration have grown, states’ borders have gradually emerged as key sites for surveillance, exclusion and social sorting.⁸¹ The border is no longer a physical place where individuals cross spatial coordinates; it is both a physical and a *virtual* space in which the categorisation and management of an identity is at the core.⁸² At the heart of this transformation has been the ‘securitisation of identities’ through the coupling of citizenship with identity management.⁸³ Some have continued to experience border security mostly as a series of (minor) inconveniences such as taking your belt or glasses off despite the intensification of almost every aspect of border surveillance and security.⁸⁴ The experiences of those others designated as ‘high risk’ or deemed to have the ‘wrong’ passport have been characterised by (highly) intrusive surveillance, continuous suspicion and lingering uncertainty and fear.⁸⁵ How much particular individuals will be affected by this ‘hardening’ and ‘thickening’ of borders – or even notice it – is largely determined not only by their citizenship and/or immigration status but also by their race, ethnicity, socio-economic background, and the ever changing landscape of national and international political and security populism.⁸⁶ In short, factors they cannot control and the impact of which is increasingly exacerbated by the regularised reliance on ever more sophisticated digital means of de-coding, tracking and managing identities.

3.1 Identities at the Border

When individuals now cross borders, they do not simply have their documents checked. Their identities are evaluated against an array of national and international databases with their physical selves squared

⁷⁸ The full text of the Act is available at: ‘UK Borders Act 2007’ (*HM Government*, 15 July 2025) <https://www.legislation.gov.uk/ukpga/2007/30/contents> accessed 18 July 2025.

⁷⁹ ‘Designation of International Cartels’ (*U.S. Department of State*, 20 February 2025) <https://www.state.gov/designation-of-international-cartels/> accessed 17 July 2025. Government of Canada lists seven transnational criminal organizations as terrorist entities, Public Safety Canada, ‘Government of Canada lists seven transnational criminal organisations as terrorist entities’ (*Government of Canada*, 20 February 2025) <https://www.canada.ca/en/public-safety-canada/news/2025/02/government-of-canada-lists-seven-transnational-criminal-organizations-as-terrorist-entities.html> accessed 17 July 2025.

⁸⁰ ‘Invocation of the Alien Enemies Act Regarding the Invasion of The United States by Tren De Aragua’ (*The White House*, 15 March 2025) <https://www.whitehouse.gov/presidential-actions/2025/03/invocation-of-the-alien-enemies-act-regarding-the-invasion-of-the-united-states-by-tren-de-aragua/> accessed 17 July 2025.

⁸¹ Benjamin J Goold, ‘Trusted Travellers and Trojan Horses: Security, Privacy, and Privilege at the Border’ in Goold BJ and Lazarus L (eds), *Security and Human Rights* (2nd edn, Hart 2019) (Kindle edition ch 6). See also Sharon Pickering and Leanne Weber, *Borders, Mobility and Technologies of Control* (Springer 2006).

⁸² Muller (n 9).

⁸³ Lyon (n 1).

⁸⁴ Goold (n 81). See also ‘United States: Repeal the Alien Enemies Act’ (*Human Rights Watch*, 1 May 2025) <https://www.hrw.org/report/2025/05/01/united-states-repeal-alien-enemies-act/human-rights-argument> accessed 17 July 2025.

⁸⁵ Goold (n 81).

⁸⁶ Goold (n 81).

against data doubles that are largely constructed and controlled not only by states but, increasingly, by private companies tasked with certain security and/or immigration functions.⁸⁷ This more specific convergence of technology, surveillance and sovereignty within border control and management has been described by some as a “surveillance assemblage”⁸⁸ constructed in a context of progressive globalisation and transformation of the nation state into novel “assemblages of territory, authority and rights”^{89,90} This surveillance assemblage arguably operates within a broader one – the “security assemblage”.⁹¹ In aiming to fulfil their obligations under various UNSC Resolutions and other relevant regional instruments, states have become more and more accustomed to working together with corporate actors within these broader security assemblages. As a result, they have gradually become entangled in transborder structures that co-produce and sustain “deterritorialized security governance”.⁹² This governance is de-territorialized in terms of actors, technologies, applicable norms and discourses with the overall assemblages embedded in a complex transnational architecture that defies the conventional distinctions of public-private and global—regional—local.⁹³ Ensuring security is thus increasingly an occupation within and *beyond* the state and its institutions.

Within these assemblages, algorithmic technologies have become crucial enablers that determine patterns of ‘normal’ behaviour and detect ‘suspicious’ activities.⁹⁴ It is also these technologies that determine more and more often who is known or unknown with the effects of this ‘decision-making’ having immediate and long-term impacts. Identities – or bodies⁹⁵ – fused by the latest technologies, are now a key aspect to contemporary governance in general and security in particular. Citizenship has thus been de-constructed into identity management with a consequent shift in focus from questions of rights protections and entitlement to ones of verification or authentication for the purposes of accessing rights, spaces or support.⁹⁶ An early but a particularly illustrative example was the introduction by the UN High Commissioner for Refugees (UNHCR) in 2002 of “state-of-the-art iris recognition” scans for refugees seeking humanitarian aid and assistance upon return to Afghanistan.⁹⁷ Once taken, the photos were converted into digital code and stored in a database. Within a year, more than 200 000 Afghans had undergone the process. UNHCR described this highly intrusive use of biometrics targeting particularly vulnerable individuals as a “successful means to verify” identities and reduce assistance fraud.⁹⁸ In 2003, the age of those tested was lowered to six years to ensure that “children are not being forced to make repeated trips with various adults – an abuse of the assistance programme and a danger to the children.”⁹⁹ Despite its aspiration to protect children due to their vulnerability, oddly, this briefing by UNHCR made no explicit references to the UN Convention on the Rights of the Child and its tailored protections to the children’s right to privacy.¹⁰⁰ Since then, UNHCR’s collection of biometrics has evolved significantly to include, for example, index fingers or thumbs scans in order to better anchor and protect identities against misrepresentation and identity theft, and for the prevention of

⁸⁷ Goold (n 81) and Gavin Sullivan, ‘Algorithmic Governance of ‘Terrorism and ‘Violent Extremism’ Online’ (2025) 13 (1) *London Review of International Law* 1.

⁸⁸ Kevin D. Haggerty and Richard V. Ericson, ‘The Surveillant Assemblage’ (2000) 51 (4) *British Journal of Sociology* 605.

⁸⁹ Saskia Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages* (Princeton University Press 2006).

⁹⁰ See also Katja Franko Aas, ‘Crimmigrant Bodies and *Bona Fide* Travellers: Surveillance, Citizenship and Global Governance’ (2011) 15 (3) *Theoretical Criminology* 331.

⁹¹ Rita Abrahamsen and Michael C. Williams, *Security beyond the State: Private Security in International Relations* (Cambridge University Press 2011) ch 6.

⁹² Abrahamsen and Williams (n 91).

⁹³ Abrahamsen and Williams (n 91).

⁹⁴ Sullivan (n 87); Anwar and Klonowska (n 1).

⁹⁵ Aas (n 1).

⁹⁶ Benjamin Muller, ‘(Dis)qualified Bodies: Securitization, Citizenship and “Identity Management”’ (2004) 8 (3) *Citizenship Studies* 279, 280.

⁹⁷ Ron Redmond, ‘Afghanistan: Iris-testing proves successful’ (*UNHCR*, 10 October 2003) <https://www.unhcr.org/news/briefing-notes/afghanistan-iris-testing-proves-successful> accessed 17 July 2025.

⁹⁸ Redmond (n 97). According to UNHCR’s own statistics, this new system had detected approximately 1,000 people who had tried to claim assistance for a second time which was not allowed. This was in addition to more than 70,000 families that were rejected under other screening methods, including more than 20,000 who were trying to recirculate through the system a second time.

⁹⁹ *Ibid.*

¹⁰⁰ Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, art 16.

duplicate registrations.¹⁰¹ Having gradually been deployed to all regions in which UNHCR operates, by 2023, almost 12 million biometric records have been collected for persons registered with UNHCR.¹⁰²

Translating human identity into information patterns not only provides more data as illustrated by the above example but it also creates new conceptions of identity.¹⁰³ Moreover, as part of the voracious pursuit of security, databases of DNA samples, iris scans and/or fingerprints can offer quicker and more reliable assessments of the trustworthiness of those who were previously unknown.¹⁰⁴ With prompt risk assessment and efficient management of the transnational data flows lying at the heart of national and international security efforts, states and transnational institutions have unsurprisingly sought to embed these new technologies into existing and emerging means to identify and (re-)classify those seeking to cross borders. No longer simply a physical gateway, borders now operate as key sites of information-gathering, risk assessment and (re)categorisation of safe and unsafe identities, of trusted insiders and untrustworthy outsiders, of the dangerous other.¹⁰⁵ The fixity of biometric identities, their lack of ambiguity and binary language have enabled more efficient border checks, faster movement, and, as far as states are concerned, more reliable verification of identities even when crossing through automated border crossings.¹⁰⁶

3.2 Reinforcing the (Un)Trustworthiness of Identities

The proliferation of safe or trusted traveller programmes such as US' Global Entry system,¹⁰⁷ UK's Registered Traveller Service¹⁰⁸ or Germany's EasyPass¹⁰⁹ system has, in this context, proven to be a particularly useful means to harvest large quantities of personal data before, at and beyond the border.¹¹⁰ Muller has described these as a marriage of increased surveillance techniques and identification technologies such as biometrics sold in the enticing packaging of efficiency, security and modernity.¹¹¹ To criticise these programmes and associated developments is to be anti-modernity and progress.¹¹² All of these programmes aim to enable citizens and permanent residents from the home state – and, in some cases, travellers from a select set of favoured states – to gain access to streamlined immigration and security procedures at various types of border crossings including airports and ports.¹¹³ Trustworthy or governable (digital) identity rather than citizenship is now arguably the leading factor in being allowed to join such a programme.¹¹⁴ The privilege of high mobility is not reserved only for – or enjoyed by all – US or EU or Canadian citizens, for example, but rather for the safe, *bone fide*, trusted travellers of various nationalities.¹¹⁵ In their respective descriptions, phrasing such as “faster and more convenient entry at passport control for frequent travellers”¹¹⁶ or “quick,

¹⁰¹. ‘Keeping UNHCR’s Biometrics System up to date’ (UNHCR, 2 August 2023) <https://www.unhcr.org/blogs/keeping-unhcrs-biometrics-system-up-to-date/> accessed 17 July 2025.

¹⁰². UNHCR (n 101).

¹⁰³. Aas (n 1).

¹⁰⁴. Aas (n 1).

¹⁰⁵. Goold (n 81).

¹⁰⁶. Aas (n 90) 341.

¹⁰⁷. Administered by the US Department of Homeland Security, Global Entry is a U.S. Customs and Border Protection (CBP) Trusted Traveler Program that allows expedited clearance upon arrival in the United States. All applicants must undergo a background check. This is also a multi-faceted programme which encompasses five distinct sub-programmes namely Global Entry, TSA PreCheck, NEXUS, SENTRI and FAST. For full details see ‘Global Entry’ (U.S. Customs and Border Protection, 9 July 2025) <https://www.cbp.gov/travel/trusted-traveler-programs/global-entry> accessed 17 July 2025.

¹⁰⁸. See further ‘Registered Traveller’ (HM Government) <https://www.faster-uk-entry.service.gov.uk/about> accessed 17 July 2025.

¹⁰⁹. See further ‘EasyPASS’ (Bundes Polizei) https://www.easypass.de/EasyPass/EN/What_is_EasyPASS/home_node.html accessed 17 July 2025.

¹¹⁰. Goold (n 81).

¹¹¹. Muller (n 1).

¹¹². Muller (n 1).

¹¹³. Muller (n 1).

¹¹⁴. Aas (n 90).

¹¹⁵. Aas (n 90).

¹¹⁶. HM Government (n 108).

simple, modern”¹¹⁷ is quite common as the key selling point. The combination of an e-passport¹¹⁸ and a membership in the UK’s Registered Traveller service not only reduces waiting time to a bare minimum, it also negates the need to deal with a border agent and/or face extra scrutiny as one can simply use automated e-gates. The US’s Global Entry system description is an outlier by expressly referring to – or *openly admitting* – that it facilitates efficient entry for “pre-approved, low-risk travelers”. In exchange for the promise of frictionless travel and membership in a select group, the trusted, low risk travellers need to voluntarily impart with extensive personal data including biometrics. While the exact procedures vary, those assessed to be eligible need to complete an application form, attend a screening interview, provide certain amount of documentation and pay a fee. The NEXUS programme, part of the US’ Global Entry, is also striking as its membership imposes a series of responsibilities including an obligation to report to a NEXUS Enrolment Centre to notify officials of any changes to citizenship documents, permanent residency cards, naturalisation certificates, work visas and study permits.¹¹⁹ Failure to keep one’s NEXUS profile (or digital identity) up to date or to notify a NEXUS official of relevant changes to your circumstances and/or eligibility can result in a *permanent* exclusion from the programme. In short, your digital identity can be re-categorised as unsafe with potentially significant and multi-faceted negative consequences the next time you attempt to cross a physical or virtual border.

Described by some as a modern day Trojan Horse, these programmes can be seen as a poisoned gift, promising freedom from tedious and time-consuming security procedures to those willing to surrender their privacy rights and consent to a level of state scrutiny they might find unacceptable in other contexts.¹²⁰ Aside from facilitating the mass collection and processing of extensive data across borders by both public and private actors, these programmes also exacerbate existing social and political divisions by indirectly further normalising and entrenching the exclusion of those categorised as high risk or unsafe. The NEXUS programme together with the Western Hemisphere Travel Initiative, for example, were inspired by and later operationalised through the 2001 Smart Border Declaration¹²¹ and the subsequent Smart Border Accord between the US and Canada.¹²² The preoccupation with precautionary and pre-emptive risk assessments before, at and beyond the border was one of the main motivating forces behind these programmes.¹²³ ‘Upstream’ interventions¹²⁴ and impeding the mobility of unknown and thus unsafe identities posing potential security threats are others. Moreover, arguably inadvertently, those who have willingly joined these programmes to enjoy the convenient means of (re)entry have collaborated in the (re)categorisation of who is a safe and unsafe identity even before the physical self has reached the border. In other words, the selected trusted travellers are some of the actors within the de-territorialised security assemblages referred to above. A role that perhaps they are unaware of or is in fact enthusiastically played in order to maintain one’s privilege at the border through securing frictionless and essentially priority access.¹²⁵ The willingness to obtain such access is not only growing but can be increasingly seen in less expected contexts than those more obviously related to (border) security.

¹¹⁷. Bundes Polizei (n 109).

¹¹⁸. According to the International Civil Aviation Organisation (ICAO), currently more than 140 States and non-state entities (e.g. United Nations, European Union) issue ePassports with over 1 billion ePassports in circulation. ePassports add a layer of security to traditional nonelectronic passports by embedding an electronic chip in the passport booklet that stores the biographical information visible on page 2 of the passport, as well as a digital security feature. This digital security feature is a country specific “digital signature”. These digital signatures are unique and can be verified using their respective certificates. See further ‘ePassport Basics’ (ICAO) <https://www2023.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx> accessed 17 July 2025.

¹¹⁹. Goold (n 81).

¹²⁰. Goold (n 81).

¹²¹. More details of the Declaration and the text of the associated plan to implemented it are available at ‘Summary of the Smart Border Action Plan Status’ (*The White House*, 9 September 2002) <https://georgewbush-whitehouse.archives.gov/news/releases/2002/09/20020909.html> accessed 17 July 2025. There are express references to “high-risk travellers” in the context of visa processing and advanced passenger information sharing.

¹²². Agreement Between the Government of Canada and the Government of the United States of America for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security (1 June 2004) E105000, full text is available at <https://www.treaty-accord.gc.ca/text-texte.aspx?id=105000> accessed 17 July 2005.

¹²³. Muller (n 1) 14.

¹²⁴. *Security in a Global Hub* (UK Cabinet Office Report, 2007) as quoted in Lucia Zedner, ‘Citizenship Deprivation: Punishment or Rights Revocation?’ in Bosworth M, Franko K, Lee M and Mehta R (eds) *Handbook on Border Criminology* (Edward Elgar Publishing 2024) 94.

¹²⁵. Goold (n 81).

3.3 Securitising Mega-Sporting Events

In order to attend any of the 2018 FIFA World Cup matches in Russia, participating football fans had to obtain a personalized card, a so-called FAN ID, which was required in addition to their match ticket.¹²⁶ This card was issued on an individual basis and was mandatory for all the spectators including children as well as Russian citizens. For non-Russian citizens, the FAN ID facilitated a visa-free entry into the Russian Federation and free travel on match days to the respective host cities. For all fans, it allowed visiting each of the 2018 FIFA World Cup™ matches for which a spectator had a valid ticket. In order to obtain this card, fans had to provide an extensive range of personal details including full details of their identity documents (i.e. document's type, series, number, etc) and a recent of a photo (with a number of stipulations attached). FAN ID, also known as a Hayya card, was used for the Qatar 2022 World Cup. To receive approval for a Hayya card, fans had to show proof of allocated match ticket(s) and secured lodgings. Entry into Qatar for the purposes of enjoying the World Cup without a Hayya card was not allowed; in order to enter a stadium, every fan had to rely on the card including Qatari citizens.¹²⁷ The human rights track records and the lack of privacy protections of both of these countries have been sufficiently rehearsed. Aside from confirmation that the FAN ID cards used for both the 2018 and 2022 World Cup were considered to be a success, it has proven exceptionally challenging to find any details on which domestic institution(s) were involved in the processing of the fan applications, for how long their personal data would be held and by which institution. The original bid requirements¹²⁸ for the 2026 World Cup make it clear that FIFA expects similar arrangements for the upcoming tournament to be jointly hosted by the Canada, Mexico and the US.

While it is still unclear what shape the 2026 FAN ID might take, as indicated in their shared bid, Mexico, Canada and the US do intend to develop a multi-country FAN ID system once prospective attendees have obtained the necessary visa(s). The above discussed trusted traveller programmes – especially those streamlining travel between Canada and the US – are likely to be an important component of the resultant FAN ID. Biometrics will thus yet again play a crucial role in the (un)successful (re)entry of various sets of individuals not only through state borders but also within fan zones and stadiums. Perhaps not widely known but fingerprinting was already used in the 1996 Olympics in Atlanta (US) to regulate the access to the Olympic Village of the participating athletes and their teams.¹²⁹ Since then, biometric security systems and algorithmic surveillance have been part of several Olympic Games such as those in London, Tokyo, and Paris all designed with the aim of easing the access of the athletes, their teams and the volunteers to the various venues and zones.¹³⁰ While there have been numerous critical reflections on the impact on the right to privacy of these particular sets of safe or low risks individuals, there have been far less discussions that entering into a stadium or a fan zone may no longer be simply the start of supporting your team or favourite athlete but also a (recurrent) virtual border crossing subject to stringent pre-clearance requirements.

As preparations for the 2026 World Cup and the 2028 Olympics shift up a gear, concerns over what impact the ever-increasing securitisation of borders and individuals will have on these mega sporting events have unsurprisingly risen. These comments by Vice-President JD Vance offered a clear indication of what is to be expected: “[e]veryone who wants to come here to enjoy, to have fun to celebrate the game, will be able to do that” however “... when the time is up, they'll have to go home.”¹³¹ In other words, enjoying the “biggest,

^{126.} For further information see here 'Fan ID' (*Visa House*) <https://www.visahouse.com/en/visa/fan-id/> accessed 17 July 2025.

^{127.} See further 'Applying for Hayya Card in Qatar 2022' (*The World Cup Guide*, 2022) <https://www.theworldcupguide.com/applying-for-hayya-card-in-qatar-2022/> accessed 17 July 2025.

^{128.} 'FIFA Publishes guide to bidding process for the 2026 FIFA World Cup' (*InsideFIFA*, 7 November 2017) <https://inside.fifa.com/tournaments/mens/worldcup/canadamexicousa2026/news/fffa-publishes-guide-to-bidding-process-for-the-2026-fifa-world-cuptm-2916170> accessed 17 July 2025.

^{129.} Lyon (n 26).

^{130.} See for example Luba Zatsepina and Jan Andre Lee Ludvigsen, 'Algorithmic Olympics: exploring the ethical and social implications of AI surveillance through the case of Paris 2024' (2025) 17 (3) *International Journal of Sport Policy and Politics* 439 and Robin Tudge, 'Every Movement of London's Olympics will be monitored – including yours' *The Guardian* (22 February 2012) <https://www.theguardian.com/commentisfree/libertycentral/2012/feb/22/london-olympics-security-surveillance> accessed 17 July 2025.

^{131.} Alexander Abnos, 'They'll have to go home': Trump's World Cup taskforce dismisses fears but warns visitors' *The Guardian* (7 May 2025) available at <https://www.theguardian.com/football/2025/may/06/trump-world-cup-task-force-infantino> accessed 17 July 2025.

safest and most extraordinary soccer tournament in history”¹³² will only be accommodated up to a certain point. These comments should not come as a surprise. FIFA’s own guidelines have expressly confirmed that ease of access to the host states “must by no means adversely affect the national immigration and security standards”¹³³ of those host states. In other words, those travelling to support their team, should expect more stringent security checks at the relevant stadiums and surrounding areas on the back of the broader domestic political priorities. With most of the games planned to take place in the US and with the US leading the cross-border security Task-Force, a FAN ID system supported by existing pre-screening programmes, offers a particularly advantageous opportunity to the current US administration to turbo-charge its (re-)categorisation of safe and unsafe identities and, by proxy, its efforts to govern through risk before, at and beyond the border.

What the discussion of the trusted traveller programmes and the backdoor embedding of these within the logistics around mega sporting events has aimed to show is that the securitisation of and at the border is not merely about inclusion and exclusion of low and high-risk travellers respectively; this is only part of the story. While citizenship – or immigration status – are the primary lines of distinction between the gate closing and the gate opening, at its core a great deal of contemporary border surveillance is biopolitical¹³⁴ in nature. The power of the state is now also directed at its own populace with the view of distinguishing between more and less deserving individuals as discussed in Section 2 above.¹³⁵ This process is aptly exemplified by the persistently heated debates around individuals suspected of terrorist activities, ‘crimmigrants’ and the (lack of) integration of immigrant populations.¹³⁶ This security populism, premised on the fear and vilification of the other, has created groups of sub-citizens – or what might be termed ‘outsiders inside’ – who, although territorially included, find their citizenship status heavily securitised (or ‘terrorized’) and thus substantially depleted.¹³⁷ By punctuating the seeming universality of citizenship through the elevation of identity management, the possibility of depriving one of nationality and the digital (re)categorization of individuals as safe and unsafe, states have constructed a “double otherness” – an internal and external otherness which cohabit the same as well as exist in entirely separate spaces.¹³⁸

Through divergent paths and motivations, the various actors and institutions within the de-territorialised security assemblages have thus not only shifted the legal, popular and political discourses around (countering-)terrorism, (crim)migration and rights but have also facilitated the creation of new, narrower and quasi-official forms of identity before, at and beyond borders.¹³⁹ The border is now something of a laboratory; it is a physical and virtual location where the state is able to test the limits of its authority and exercise raw sovereign power.¹⁴⁰ In this context, the infrastructures behind trusted traveller programmes and the FAN ID for mega sporting events offer a valuable insight into the ever evolving and impactful complexities at the intersections of human rights, individual dignity and public security. Given the ‘right’ incentive within the ‘right’ context, individuals can become active and *willing* participants in facilitating the coercive surveillance of the other, their social sorting and exclusion more broadly. To put it differently, one of most consequential effects flowing from the opening of the counter-terrorism floodgate, is the normalisation of new hierarchies of privilege based on categorisation of trusted/safe and unsafe/high-risk (digital) identities. The relationship between rights and security has become ever more complicated with individuals actively encouraged and facilitated in participating in the securitisation of their own identity in various contexts and aspects of daily life. Surveillance and social divisions have become pervasive yet acceptable depending on their presentation, reach and application. Digital identities as passwords are now the norm.

¹³². Abnos (n 131)

¹³³. *InsideFIFA* (n 128) .

¹³⁴. [B]iopolitical surveillance internally differentiates the bios, and its forms of exclusion are primarily scientific and moral, rather than territorial exclusion from the polity as such.

¹³⁵. Aas (n 1) and Lyon (n 1).

¹³⁶. See in particular the introductory comments in Goold and Lazarus (n 74).

¹³⁷. *Ibid.*

¹³⁸. Etienne Balibar, ‘At the Borders of Citizenship: A Democracy in Translation?’ (2010) 13 (3) *European Journal of Social Theory* 315, 321.

¹³⁹. Anwar and Klonowska (n 1) and Sullivan (n 87).

¹⁴⁰. Goold (n 81).

4. Concluding Remarks

Within what has been described as the pursuit of the “voracious ideal” of security,¹⁴¹ questions of effectively anticipating, pre-empting and countering terrorism have persistently dominated (trans)national and regional institutions in the last two decades. Human rights have been frequently invoked to justify (trans)national security efforts but rarely regarded as imposing limits on the reach or ambitions of the counter-terrorism driven security apparatuses.¹⁴² Most tellingly perhaps, despite constructing a “comprehensive and multilateral security architecture” aimed at norm setting, capacity building and enhancing sanction regimes, neither the UNSC nor other UN institutions have defined terrorism at international level or at least provided a uniform guidance on what is actually (violent extremism conducive to) terrorism.¹⁴³ The result has been operational definitions or guidance for narrow and concrete circumstances; in other words, highly useful elasticity as to who falls within or outside the category of a security threat i.e. who is a safe or unsafe identity. In a related development, the increasingly onerous and multi-faceted physical and virtual border control management measures have become a core constituent element of the voracious security pursuit through pre-empting, mitigating and/or disrupting the (re)entry of individuals deemed to pose a potential (security) risk. Spurred on by the various UNSCRs and other relevant instruments within the EU framework or by transnational bodies such as the GCTF, states steadily developed a multi-layered cross-border framework for interdiction to intercept and prevent the movement of those alleged to be terrorist or other suspicious actors. These technical solutions have inspired and allowed states to both physically and *virtually* monitor the whereabouts of countless individuals suspected of illicit activities, pre-empt their travel and screen *before* arrival at various types of border crossings.

Thus while not everything changed after events such as those of 9/11, the consequent multi-faceted repercussions continue to reverberate in foreseen and unforeseen ways even today. The lingering fear of further high-casualty terrorism activities has, and will likely continue to, sustained the multi-layered transnational efforts to pre-empt and eliminate existing and identify emerging security threats. When the proclivity of states to favour high technological ‘solutions’¹⁴⁴ as a response to particularly intense moral and security panics is factored in, states’ now automatic reflex to adopt new and adjust existing measures, increase surveillance and tighten internal and external border management will remain the norm.¹⁴⁵ In the ever present backdrop of hyper-inflated insecurity threats, respect for human rights and tolerance towards others will regrettably continue to be under an acute pressure. The recurrent, onerous, and at times unlawful, restrictions of the rights and liberties of those deemed to be unsafe, combined with the enduring moral panic over terrorism, have ushered and normalised a downward recalibration of the relationship between these individuals and the state. The greater social stratification at the border – trusted (low-risk) vs unsafe (high-risk) travellers – has extended this recalibration beyond citizenship or immigration statuses. The backdoor embedding of trusted traveller programmes – and, more broadly, digital identity management – within the logistics around mega sporting events is illustrative of how further a field border security management now takes place. The voracious pursuit to uncover or decode the ‘truth(s)’ that the new categories of (digital) identities are telling us,¹⁴⁶ has arguably not only recalibrated the relationship between numerous individuals and the state but it is also the harbinger of a recalibrated relationship between individuals and the human rights framework more broadly.¹⁴⁷ With ever more people voluntarily transferring core personal data to various actors within the de-territorialized security assemblages thus becoming key actors themselves, the entry zones to what constitutes in-/exclusion, belonging and privilege will become increasingly hard to access and navigate. If the body doesn’t lie,¹⁴⁸ what ‘truth(s)’ it telling us about its own role?

¹⁴¹ Jeremy Waldron, *Torture, Terror, and Trade-Offs: Philosophy for the White House* (Oxford University Press 2010), Kindle edition.

¹⁴² De Londras (n 27).

¹⁴³ De Londras (n 27).

¹⁴⁴ Lyon (n 1).

¹⁴⁵ Donohue (n 16).

¹⁴⁶ Aas (n 1).

¹⁴⁷ Goold (n 81).

¹⁴⁸ Aas (n 1).

