Volume 7 (1) 2025 https://doi.org/10.5204/lthj.3740

The Techno-Legal Co-production of Terrorist Suspects

Tasniem Anwar
Vrije Universiteit van Amsterdam, The Netherlands
Klaudia Klonowska
University of Amsterdam; Asser Institute, The Netherlands

Abstract

From domestic lists to kill-lists deployed in counter-terrorism operations, lists have been a central tool in tracing, targeting and identifying terrorist suspects. Such lists increasingly make use of algorithms and surveillance technologies, quickly filtering through vast amounts of data in a promise of providing more accurate and almost real-time updates on the terrorist threats. In this article, we empirically study how different lists in domestic and international contexts are becoming central to the classification of terrorist behaviour and suspects, and how they (re)shape legal definitions and possibilities for intervention. The empirics show that traditional logics of the law that classify measures into legal regimes, separate the domestic from the international, isolate digital infrastructures and divide terrorists from non-terrorists fail to capture the complex and messy socio-technical security assemblage that works to produce these terrorist suspects. Based on the empirical analysis, the article addresses three concerns about traditional legal reasoning based on strict categories and straightforward solutions and argues instead that legal approaches need to be better attuned to the complex associations that produce terrorist suspects in these security and counter-terrorism spaces.

Keywords: Counter-terrorism; algorithmic surveillance; legal assemblage; behavioural patterns.

1. Introduction

Deploying terrorist lists has become a widespread practice since the 'War on Terror' sparked by 9/11. From border controls, to domestic criminal databases, to dynamic target lists in armed conflicts, lists have been a central tool in targeting and identifying terrorist behaviour.[1] These lists are powerful techniques of governance that bring individuals into legal relations and allow legal interventions against them.[2] For example, being included on a terrorist list may lead to constant surveillance, freezing of bank accounts, deportation, additional security checks at airports and, in the worst-case scenario, death.[3] These lists are considered useful and reliable tools to monitor and track citizens and are used to justify such legal interventions prior to an actual terrorist attack. Increasingly, such listing tools are accompanied by the use of machine-learning algorithms to identify suspicious behaviour patterns.[4] Despite the promises of improved accuracy, current trends show that terrorist databases and surveillance continue to expand, suspicion rather than evidence continues to underpin the listing mechanisms and many people are still misidentified. Meanwhile, the legal frameworks within which these lists operate remain ambiguous and unable to satisfactorily address the ongoing human rights infringements that come with wrongful inclusion on the list.[5]

In this article, we empirically study how new technologies are becoming central to *identifying* terrorists and how this challenges, shapes and reshapes the very ways in which these terrorist categories gain legal meaning. Zooming in on these practices and

[1] De Goede, "Introduction."
[2] Sullivan, "Between Law and the Exception"; Johns, "Global Governance."
[3] Leander, "Technological Agency."
[4] Johns, "Global Governance," 134.
[5] Aradau, Algorithmic Reason; Amoore, Cloud Ethics.

Except where otherwise noted, content in this journal is licensed under a Creative Commons Attribution 4.0 International Licence. As an open access journal, articles are free to use with proper attribution. ISSN: 2652-4074 (Online)

© The Author/s 2025

interactions, we show that the algorithmic models that promise more precise and accurate predictions of potential terrorist threats paradoxically do not lead to better legal actions. While the lawyers, the data-analysts, the military and the many other actors involved aspire to decide who is 'in' and who is 'out' of the terrorist categories, they end up co-producing an assemblage where everyone and everything is potentially suspicious and where legal interventions are easily justified and hardly challenged. Three core concerns are identified: (1) the expanding, loosely defined use of behaviour patterns as markers for 'guilt by association'; (2) the efforts to make security lists interoperable with various databases such as healthcare databases, which leads to obscuring the source of behavioural markers and further impedes successful removal of identities from lists; and (3) the role that legal instruments and vague legal terms play in enabling and facilitating the associative work of algorithmically filtered lists in producing terrorist suspects. We argue that the logic that drives the list – more precise and better-defined legal options to intervene – is the opposite of what the list produces. Although similar arguments critiquing the promises of listing as technologies of precision, stability and ordering have been made before (see also section 2), the novelty and the main contribution of our article is the exploration of this dynamic in two empirical areas of listing practice.

Our argument is based on two empirical case studies where terrorist lists are deployed. Our selection of cases was driven by the interest in tools that monitor citizens and identify terrorist suspects for the purpose of interventions justified by national security, both domestically and internationally. Our first case centres on a French watchlist called the 'Le Fichier des Signalements pour la Prévention de la Radicalisation à caractère Terroriste' (FSPRT). The second case revolves around military algorithmic and listing technology: the Skynet program used by the United States to identify, surveil and target Al-Qaeda members in Pakistan. Our aim is not to conduct a full legal comparison, but rather to examine the practices of producing 'terrorist suspects' who emerge at the intersection of law, security and surveillance in the two case studies of counter-terrorism interventions. The list finds itself at the centre of these intersections.

Despite the focus on the FSRT list and the Skynet kill list, the conclusions from this analysis are of high relevance to automated decision-making practices in security contexts more broadly. Techno-legal logics of listing and algorithmic filtering of terrorist suspects continue to be employed in various contexts today, continuously blurring the lines between domestic and international, suspicion and evidence, peace and war. For instance, in a recently reported case, the Israeli Defence Force deployed a listing mechanism called 'Lavender' that nominates targets in the genocide on Gaza based on the suspected life patterns matching those of the Hamas associates.[6] Fears are also growing in the United Kingdom, where data about suspected radicalised individuals is being widely shared with police, immigration authorities and intelligence agencies, raising concerns about human rights violations and racial profiling.[7]

The next sections are organised as follows. First, we present relevant literature that conceptualises the pre-emptive character of counterterrorism interventions and the role of international law in security assemblages. Conceptually, we build on the growing scholarship in socio-legal studies that examines law as an assemblage of material and discursive practices.[8] We then move on two conduct an analysis of the two case studies based on the qualitative analysis of academic literature, policy documents, non-governmental reports and media articles. First, we investigate the procedures and markers that accompany the identification of suspicious individuals. The deployment of the assemblage approach points us to study the mundane and even absurd relationships between data points as a prediction for human behaviour. Second, we map how these lists are entangled with broader questions of law and regulation. This mapping attunes us to the pre-emptive and speculative production that defines the relationship between law, security and surveillance. After the empirical analysis of the two case studies, we mobilise the notion of 'association' to highlight the connections that listing practices enable and the broader implications of such associating practice to international law. This discussion shows how, in both cases, loose associations become grounds for legal decisions and security interventions. Accordingly, pre-emptive interventions enabled by listing tools do not just blur or complicate legal categories, but more fundamentally co-constitute how legally justifiable suspicion is produced.

[6] Abraham, "Lavender." Note that many automated decision-making tools are also being used in the ongoing war between Russia and Ukraine. Even if those tools are used to identify targets (e.g. location of adversarial military vehicles), they are not designed to predict suspected association with what are framed as "terrorist groups" or "terrorist activities." In this way, such tools fall outside the scope of this article's focus on algorithmically automated terrorist lists. We do not exclude the possibility that automated listing tools will be used in the future in the context of the Russo-Ukrainian war, as both governments are passing legislations that expand the scope of prohibited terrorist activities and applicable sanctions.

[7] Amoore, "The Deep Border."

[8] Sullivan, "Law, Technology"; Smith, "Drones as Techno-Legal Assemblages"; Cloatre, "Law and ANT "; Johns, Non-Legality in International Law.

2. Pre-emptive Security and International Law

Our article questions how security and surveillance technologies are challenging and reshaping the way these terrorist categories gain legal meaning. For such an interdisciplinary question, we deploy an assemblage approach. This approach, further developed in security and surveillance studies, conceptualises surveillance as the interaction between technologies, humans, infrastructures, legal practices and data flows. As such, surveillance and regulatory frameworks are not static phenomenon or simply 'out there', but produced through myriad practices and materials. Indeed, for our argument and in the context of databases of terrorists, it is relevant to examine how individuals are made calculable and how their digital data traces are *assembled* to create a profile of their persona and their behaviour that is used to conduct counter-terrorism interventions. Sullivan similarly uses the assemblage approach in international law, arguing that security governance operates through 'heterogeneous socio-technical infrastructures or assemblages that are constantly unfolding in practice'.[9] In this approach, the assemblage of countering terrorism consists of multiple actors, including legal institutions, security actors, infrastructures to share data among these actors, risk indicators of suspicious behaviour, software designers and many others. The concept of 'co-production', borrowed from Jasanoff, allows us to further conceptualise the relation of actors within an assemblage as co-constitutive and co-emergent in produced effects. Co-production is 'a way of interpreting and accounting for complex phenomenon' of knowledge-making, and helps us to highlight that 'knowledge' about who is a terrorist is constructed through a combination of expertise, technical practices and material objects.[10] The role of law is therefore not hierarchical (i.e. above or beyond the listing practice) but better understood as co-constitutive of the security assemblage.[11] Similarly, the role of law is not external to surveillance or security, but legal practices and materials are part of the assemblage.[12] Taking an assemblage approach allows us to conduct interdisciplinary research, combining insights from security studies and law. Furthermore, it enables the study of law beyond the regulatory frameworks, but as a form of governance that is fluid and emerges through material practices.

This article combines multiple scholarly debates to better understand the legal governance of novel surveillance and security technologies. Although surveillance is not a new phenomenon, security scholars argue that contemporary technological developments such as artificial intelligence (AI) and Big Data have significantly altered and escalated the pre-emptive security practices worldwide.[13] States are using predictive analytics to filter vast amounts of data with the objective being 'to uncover unexpected patterns and pinpoint potentially suspected "needles"'.[14] AI's *modus operandi* is inherently reliant on 'prognostications' rather than certainties, on uncovering what might be or could be, and thus to 'identify' future terrorist activities before they materialise.[15] Using calculations and statistics from gathered data, AI-enabled predictive analytics effectively conflates past, present and future occurrences of risk.

Predictive analytics that are inherent to this pre-crime analysis are different from other counter-terrorism measures such as biometric verification or body scans at border crossings.[16] Instead of verifying an existing terrorist threat (e.g. a hidden gun or an identity theft), predictive data-driven analytics tools forecast *possible constellations of future human behaviour*. Such tools can theoretically draw statistical correlations from any type of data: text, images, web searches, transactions, clicks, sensors and cameras. Examples of such correlations are data extracted from cell phones that inform with whom and how frequently a person had contact; financial transactions that reveal behavioural patterns and allegedly inform about potential involvement in or support of terrorist groups; and social media that can reveal a lot about friendships and motivations.[17] The adoption of AI techniques further pushes security agencies to compile multi-modal datasets (i.e. data captured from different sources), with the hope that the more data is gathered, the most accurate the predictions of future behaviour and potential threats will be. These debates illustrate how critical security scholarship has addressed the way speculative security allows for decisions based on predictions of the future. Such insights are equally relevant for legal scholars, as legal practices are increasingly confronted with similar speculative measures. Johns argues that even though there is a common assumption of international lawyers that lists are as 'orderly, stable, and predictable as possible', list-plus-algorithms are nonetheless unreliable, inaccessible and unprincipled.[18] There is therefore an urgency for legal scholars to empirically examine how security, surveillance and law come together and what effects they produce in the data-driven terrorist listing practices.

[9] Sullivan, The Law of the List, 5.
[10] Jasanoff, States of Knowledge, 1–4.
[11] Sullivan The Law of the List
[12] Sullivan, The Law of the List.
[13] Aradau, "Politics of Prediction."
[14] Aradau and Blanke, "Politics of Prediction."
[15] Downey, "Algorithmic Predictions," 125.
[16] Kaufmann , "Predictive Policing."
[17] Sullivan, "Law, Technology."
[18] Johns, "Global Governance," 135.

Furthermore, the pursuit of the pre-emptive modes of counter-terrorism is both enabled and produced by the growing informality of law and legal institutions. Ní Aoláin has highlighted that the lines between hard and soft law are increasingly blurred, leading to an intimately intertwined and mutually reinforcing relationship between formal and informal law-making.[19] This includes loose definitions of terrorist groups and individuals in domestic and international law, lower standards of evidence and less-formalised accountability for security and surveillance actors. Additionally, the emergence of law-making bodies such as the Global Counterterrorism Forum has contributed to the increase of counter-terrorism regulations and practices.[20] The introduction of algorithmic decision-making tools in security practices is not troubled by these blurry legal frameworks, but rather facilitates informality and loose definitions through its fluid connections and interpretation of data. As such, the increasing fluidity and informality of legal categories in counter-terrorism operations stress the importance of understanding how law, surveillance and security are entangled in the production of 'terrorist suspects'.

3. Case Studies

In this section, we elaborate on our methodology and present the findings of our empirical analysis. Although listing practices are common for most European Union member states, their exact materials and practices are clouded by secrecy. As such, we are inspired by critical security scholars[21] who argue that secrecy is not a barrier to overcome, but that rather, in studying security settings, scholars need to work *with* secrecy and acknowledge it as part of their methodological reflections. Our selection was hence limited to cases with available reports and accounts of their use. Using desk-based research, we compiled and analysed documents from government databases, public statements and leaked accounts in investigative reports.

For the first case study, a qualitative analysis was undertaken on the basis of media reports obtained via NexisUni, reporting directly on the FSPRT between 2017 and 2023.[22] We also analysed official reports by the French Government[23] and legislative debates.[24] The FSPRT list, which was opened after the *Charlie Hebdo* attacks, is a secretive database used to store data of persons suspected of Islamist radicalisation and involvement in terrorist attacks. Individuals found on the FSPRT list are not only subject to surveillance but have also been deported.[25]

The second case revolves around military algorithmic and listing technology: the Skynet program used by the United States to identify, surveil and target Al-Qaeda members in Pakistan based primarily on the collection and processing of mass-surveilled phone sim data.[26] Individuals who were found on this list were subjected to increased surveillance and, in some cases, targeted drone attacks. For this analysis, we relied mostly on an investigative report released by Intercept in May 2015, which also included leaked screenshots of government slides explaining the Skynet program.[27] We also analysed the documents released in relation to the *Zaidan et al v Trump et al* trial (2017–2019), in which the defendant challenged the suspected inclusion on the Skynet list and targeted drone attacks against him.[28] Furthermore, in the analysis and interpretation of the leaked materials, we also reviewed relevant academic publications that discussed the primary sources.

3.1 Case Study 1: The FSPRT Watchlist

Background

In 2015, the French government created a new database, alongside the existing sources of the Ministry of Interior to list suspected criminals. This new list, which was called, *Fichier des Signalements pour la prevention de radicalization à caractère terroriste* (FSPRT) contains names of known and suspected terrorists and focuses almost exclusively on the inclusion of

[19] Ní Aoláin, "Soft Law."
[20] Kassem, "Watchlisting the World."
[21] Bosma, Secrecy and Methods.
[22] The media corpus existed of more than 10 reports published in newspapers such as Le Monde, Le Parisien and TF1. The full overview can be requested from the authors.
[23] Le fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT); Interministerial Committee for the Prevention of Crime and Radicalisation.
[24] In particular, the legislative debates around privacy were analysed: see, for example, *Conseil d'Etat 27 Mars 2020 Analyse n° 431350*, *Conseil D'état, 13 March 2020, N°s 431350, 431530, 432306, 432329, 432378, 435722*.
[25] Hellmuth, "Countering *Jihadi* Terrorists."
[26] We recognise the debates and disagreements on the classification within International Law of the US drone war in Pakistan. We do not attempt to contribute to this classification, but rather draw out how the law interacts with the technological decision-making process in the identification of terrorists.
[27] Currier, "U.S. Government."
[28] *Zaidan et al v Trump et al.* Complaint; *Zaidan et al v Trump et al.* Memorandum Opinion.

(potentially) radicalised Muslims.[29] The list is governed by UCLAT, a specialised counter-terrorism unit within the French government.[30]

In our empirical example, the list is not a static device, but a fluid and living document that stratifies legal possibilities and delegates legal powers to monitor and intervene across the security domain. During its peak in 2018, the list comprised more than 20,000 names.[31] In its most recent public update from 2020, the list had shrunk to 8000 names that were actively being monitored according to the authorities, yet the overall number of individuals on the list remains at about 22,000.[32] Reasons for this downgrading of the top-segment are not explained by the authorities. Even if accounts of individuals are closed, their data continue to be stored for another five years.[33] The list is deployed as the main tool by the French security services to monitor and prevent radicalised youth attempting to travel to Syria, but also allows for increased surveillance of those who are suspected of plotting terrorist activities on French soil. The list follows a ranking based on the 'dangerousness' of the listed individuals. While concrete indicators of this decision are not made public, the ranking is based on the level of radicalisation and proximity to concrete terrorist activities.[34] Individuals in the 'top segment' are closely monitored by the General Directorate of Internal Security (DGSI). In 2018, this 'top segment' consisted of about 11,000 individuals, who were tracked through phone taps, tracing of online behaviour and geolocation, and other surveillance mechanisms. This top category of 'dangerousness' also contains known terrorists, including individuals who are currently serving jail time or are released from prison. The 'middle segment' includes 4000 names of individuals who are not considered an imminent threat but remain under surveillance. They are monitored by a different unit, the Central Territorial Intelligence Service (SCRT). The lowest rank consists mainly of individuals who are suspected of radicalisation or those whose level of radicalisation is still being assessed. They are monitored by local institutions and educational committees. In other words, the category of 'suspected terrorist', a legal category that captures those who *might* break the law, is not a solid category but is further divided into different ranks. The ranking does not only indicate a differentiation of riskiness, but also points us to the different institutions that can surveil them and the permissible legal interventions such as sharing of data of those considered to pose the highest terrorist threat. In its report, the Ministry of Interior included the following graph, showing a high peak of 'top-segmented' individuals, followed by the categories of closed cases, other and stand-by.

Behaviour-Based Analytics and 'Suspicious' Patterns

Getting on to the FSPRT list can happen in multiple ways. The watchlist depends, on the one hand, on sophisticated technologies to filter and detect suspicious behaviour. On the other hand, family members, schools, employers and others can also directly report suspicious radicalised behaviour to the authorities. In practice, these two forms of collecting data (human and technological) are used in a complementary way. Data for the list is shared between various domestic security and legal institutions, including intelligence services, police, courts, TRACFIN,[35] the Department of Justice and even psychiatric institutions. These institutions have far-reaching possibilities to legally share and request data on suspected terrorists, cooperate on an international level with EUROPOL and access databases such as the Schengen Information System (SIS) and the Visa Information System (VIS).

From domestic actors, much of this data derives from surveillance techniques such as phone taps and monitoring of geolocations. Since 2015, it has been legal for the French intelligence services to deploy an algorithm that does not collect personal data on phone calls, but analyses data connections between suspected terrorists and large groups of individuals.[36] This Act allows intelligence services to collect personal and metadata (without judicial oversight) for a specific objective, including the prevention of terrorism. Based on this law, the intelligence services can mobilise telecom companies to deploy tracking devices on all their data infrastructure for the aforementioned purpose of real-time tracking of potential terrorists. These so-called 'black boxes' can track individuals, vehicles and other objects. It is thus not only the individual on the list who is affected

[29] While it is outside the scope of this article to discuss the lawfulness of targeting a racialised community as inherently suspicious, we refer to the work of Puar for an excellent analysis of the role of racism, islamophobia and homophobia in the 'War on Terror': see: Puar, Terrorist Assemblages.

[30] For more information, see https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents/fichier-de.

[31] Interministerial Committee for the Prevention of Crime and Radicalisation, The State, Territorial Authorities and Society.

[32] Le Parisien, "Terrorisme."

[33] Le Parisien, "Le Plus."

[34] The website of the DGSI reads: "It is most often the DGSI for the 'top of the spectrum' (people with the highest signs of dangerousness). Other people are, depending on the situation, followed by the central territorial intelligence service (SCRT) or the Directorate of intelligence of the Paris Police Prefecture (DRPP) according to their home (the SCRT, present throughout the territory via its territorial services as close as possible."

[35] TRACFIN is the French Financial Intelligence Unit. For more information see: https://www.economie.gouv.fr/tracfin.

[36] Code de la sécurité intérieure, ReplierPartie législative (Articles L111-1 à L898-1).

by this law but everyone in contact with potential terrorists. The purpose of this exercise is to identify potential terrorist suspects through analysis of the metadata. If the algorithm detects a potential terrorist threat, the Prime Minister can issue an order to the telecom companies to share the personal data of the targeted individual with the intelligence services for more targeted surveillance, and possible inclusion on the FSPRT list.[37] In 2016, the Minister of Interior claimed that, 'by cross-referencing data with an already-known very powerful algorithm, we could be able to monitor those 11,700 persons [of the S-List] in real time'.[38] The S-list is another watchlist that targets 'wanted persons' more broadly, while the FSPRT focuses exclusively on Muslim individuals in the context of potential radicalisation. While not all names on the S-List appear on the FSPRT list, it is safe to assume that similar surveillance algorithms are used for both watchlist practices.

Aside from the automated decisions, many of the traces that come to the attention of the UCLAT are initiated by manual reporting of individuals by ordinary citizens, educators or other local actors. The police officers from the UCLAT receive multiple reports on denounced individuals from multiple sources as described above. They need to decide whether reports of new individuals can be submitted to the list, monitor the individuals who are already on the list, add new relevant data, and remove individuals from the list. These decisions are based on behavioural data that is collected by intelligence services, international security actors such as EUROPOL, but also local police, community workers, and family members. The exact indicators remain secretive, but we compiled a list of key behavioural features used for analysis from available public statements:

1. Increasing gender segregation
2. Legitimisation of attacks
3. Zealous application of Islamic doctrine
4. Suddenly sleeping on the floor
5. Tears up over family photos
6. Gouges eyes of stuffed animals
7. Resenting dogs
8. Change of dress to a more conservative clothing style
9. Growing a beard
10. Watching violent videos online
11. Prohibiting music
12. Conspiracy-like statements
13. Association with other known or suspected terrorists.

When a report is made by a family member, educator or others, the officer consults with the departmental security group (GED) and together they decide on a classification of this individual. In case the report leads to a denunciation, the data are shared with the UCLAT for listing purposes, and to collect more information from other security actors. Depending on the seriousness of the threat, which is assessed by GED, institutions proceed to monitor this individual, adding more data to the file. This includes information on other individuals, mapping of meeting points and connections with other individuals on the watchlist. In sum, while many studies focus exclusively on algorithmic detection of anomalies in travelling patterns or online behaviour, our example highlights the complexity of the entire process. We show that the list is an assemblage of digital surveillance, manual reports, unusual observations from family members, stereotypes and snippets of fragmented data that feed into the production of knowledge about the observed behaviour, whether deemed 'normal' or 'anomalous'. The label 'terrorist suspect' here is not a fixed or single category with clear legal consequences. On the contrary, it is a fluid and dynamically changing label, influenced by the technical possibilities of surveillance and the mandates of different governmental institutions. Due to the secretive nature of this counter-terrorist practice, it is difficult to fully unpack how these different entities work in detail. Nevertheless, our case study shows that these forms of surveillance take different forms and practices and rely on various ways of knowing and seeing potential terrorists – both digital and non-digital.

Legal Indeterminacies

Watchlists are made possible through the adoption of international and domestic legal frameworks that legitimise the use of mass surveillance and the exchange of data for security purposes. As noted in the previous paragraph, French legislation since

[37] Christakis, "National Security."
[38] Follorou, "Les failles de la lutte antiterroriste."

2015 has facilitated far-reaching surveillance practices, including automated monitoring of phone data and geolocation.[39] This results in surveillance practices such as the deployment of 'black boxes' as described above.

The automated decisions that co-produce the FSPRT list are not only fed by predetermined categories of suspicion. Rather, the surveillance practices broaden the boundaries of the legal classification of terrorist suspect. For example, as part of the automated surveillance practices that compose the FSPRT list, intelligence services can access psychiatric dossiers (also known as the HOPSY files) of psychiatric patients, including those committed against their will. This access was authorised by a decree in 2019,[40] allowing for medical databases of psychiatric patients to be shared with the FSPRT database. The security logic behind this decision assumes that there is an identifiable link between mental health and radicalisation, pulling psychiatric disorders into the realm of pre-emptive securitisation. At the time of writing, the data sharing happens as follows: every day and with every new entry into both the FSPRT database as well as the psychiatric disorder database, the two systems connect surnames, first names and date of birth registered. If the two lists (the psychiatric dossier and the watchlist) match an identity, an officer from the hospitalising institutions begins a 'removal of doubt' procedure to ensure that the two data entries are not coincidental matches but indeed represent the same person. The officer will request additional information on the flagged individual to make this decision. After this confirmation of identity match, intelligence services and other relevant authorities will be informed and the psychiatric data will be shared with the FSPRT database.[41] As a result, mental health issues and psychiatric disorders become a part of the behavioural analysis of those who are suspected terrorists.

The French National Commission for Information and Freedom (CNIL) has indicated a few controversies with this exchange of data: first, this process of removal of doubt is barely regulated and it is unclear what kinds of data are collected and shared to reach this decision. The 'removal of doubt' is an informal process that theoretically could even be executed over the phone.[42] To this, they suggest secure and more regulated ways of sharing information.[43] Second, the data that are stored in these HOPSY files are collected for the purpose of medical help, so do not match or relate to the data categories developed in the pursuit of terrorist activities. There is no further legal framework that prescribes how these data will be matched, leaving such decisions up to security and medical professionals with little oversight. Third, the connection between the medical files and the intelligence services, including the medical data of those hospitalised against their will, forms a breach of the medical secret that is embedded in French law. While the government has made minimal changes to the text after these controversies,[44] the main proposal to connect these two databases remains unquestioned. A political decision that was confirmed by the *Conseil D'état* in a legal proceeding ruled that the state can take far-reaching measures to prevent terrorist activities.[45] This example shows how the boundaries of the law are increasingly being stretched to accommodate expanding definitions of suspicion and terrorist threat.

3.2 Case Study 2: The Skynet Algorithm and Kill List

Background

Besides watchlists that may prevent individuals from crossing borders or accessing their financial assets, governments around the world also use so-called 'kill lists' or 'hit lists', which designate an individual as a terrorist who can be killed by national armed forces.[46] Targeted killings and signature strikes often take place within the context of an armed conflict governed by international humanitarian law, while other (suspected) terrorist targets are executed extrajudicially, creating additional challenges to the interpretation of their legality.

Despite their distinct name and purpose to eliminate terrorists involved in armed conflicts, kill lists are not necessarily separate or independent from watchlists. On the one hand, kill lists are fed with data directly from the battlespace using, for example, drone footage, geolocation data and sim phone data. On the other hand, data gathered by domestic agencies and private partners that are stored on national watchlists are also used to feed the kill lists.[47] The governments use a variety of sources with the aspiration of analysing associations and interactions between all available data points to identify terrorist suspects. Examples of government projects that strive to achieve forecasting capacity in an armed conflict and accurately identify potential targets are ample. We choose to focus on the Skynet program deployed by the United States to counter terrorism in

[39] LOI n° 2015-912 du 24 juillet 2015 relative au renseignement (1).
[40] Décret n° 2018-383.
[41] Decree No. 2018-383.
[42] Deliberation no. 2018-354.
[43] Deliberation No. 2022-046.
[44] Fédération Francaise de Psychiatrie, "Affaire Hopsyweb."
[45] Conseil D'état, N°s 431350.
[46] Weber, "Keep Adding."
[47] Weber, "Keep Adding."

Pakistan. Skynet originated as a program under the leadership of the United States National Security Agency (NSA) to detect terrorist activities in Pakistan using phone, geospatial and geotemporal data. The leaked presentation slides reveal that the NSA searched for Al-Qaeda's couriers. The algorithm under the Skynet program was built on the assumption that Al-Qaeda's couriers are 'different people that use phones in similar ways'.[48] This assumption served as the basis for the development of machine-learning algorithms that could detect the 'characteristic' patterns of behaviour.

Reports of this program, together with the classified PowerPoint presentations revealing the interface of the system, were leaked by Edward Snowden and published by the Intercept on 8 May 2015, but the Skynet program is considered to have been in use at least since 2004. Since 2016, information about the Skynet program has been scarce, revealing little to no credible data about whether or not the project has been terminated. The case of the Skynet program has been analysed by various scholars, whose work is included hereinafter, highlighting the controversies related to the secrecy of the lists, the algorithmic processing of data and surveillance of Pakistani populations, and the creation of suspicion from travel patterns. In this article, we add to this breadth of literature by combining the analysis of the algorithm's dependence on metadata[49] with the analysis of the legal categories and how they together co-produce terrorist suspects.

Behaviour-Based Analytics and 'Suspicious' Patterns

The Skynet project lacked specific legal or administrative criteria that would determine the inclusion of an individual on the kill list. From the outset, it was an experimental program. In the development phase, analysts used a dataset of phone records of known Al-Qaeda couriers to train a machine-learning algorithm in identifying target profiles. These data points became the 'behavioural features' or criteria predictive of 'courier-like travel patterns'. For example, in their analysis, there was an indication that Al-Qaeda couriers travelled more often, made more daily outgoing calls and stayed in groups more often 'than typical Pakistani selectors'. On the basis of these indicators, the algorithm developed additional behavioural features, including regular or repeated visits to locations of interest, low use of the phone, frequent powering off, information on co-travellers, permanent moves or common visits to airports (see Figure 1).

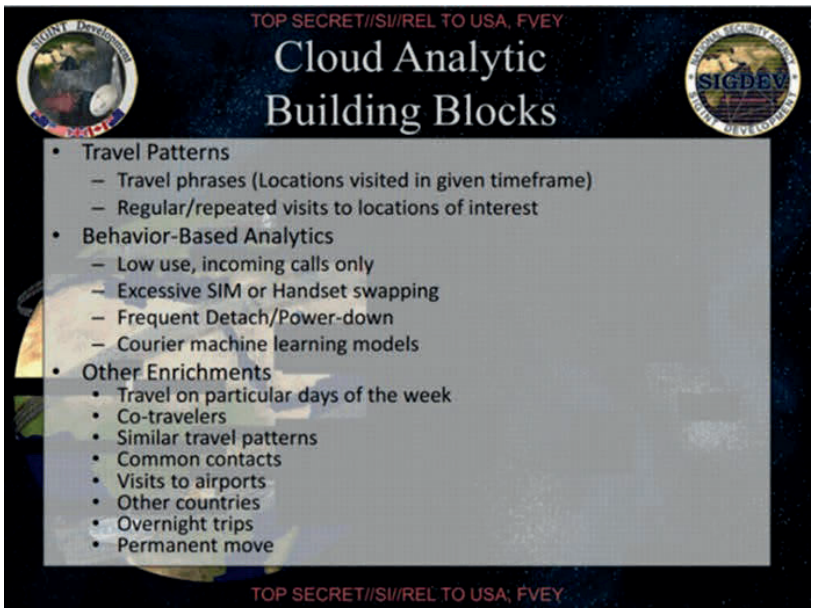

Figure 1. Determinant behavioural features of Al-Qaeda's courier identity. A slide from the PowerPoint presentation leaked by the Intercept, 8 May 2015.

[48] The Intercept, "Skynet."

[49] Often what are available to authorities are the so-called 'metadata' – data that do not reveal the content (e.g. what has been spoken on the phone) but provide basic information about occurrences (e.g. which phone number was called, from where and at what time). see Aradau, "Assembling."

On many of the leaked slides, we can see that data analysts kept changing and 'experimenting' with the algorithm until they saw that top individuals on the lists produced were meeting their logical expectations and concluded that the algorithm was 'on the right track'.[50] In the deployment phase, Skynet filtered phone sim data that matched the behavioural features. For example, a digital profile was created for a person whose phone sim data revealed '5-or-fewer-contacts', 'sms-and-zero-duration-calls-only' and 'low-use'. This was a trial-and-error process.

What was ultimately produced was a list of 'selectors', as the US government officials and data analysts used to call them. Sometimes selectors included real names of persons matched with a specific pattern-of-life, but at other times names or even nationalities were unknown; instead, imprecise identity markers were used, such as 'Sikh Extremist'.[51] This practice was further facilitated by policy means, such as the Presidential Policy Guidance, in which agencies were allowed to conduct lethal action even in the absence of a target's full name as long as they 'employ[ed] all reasonably available resources to ascertain the identity of the target so that action can be taken'.[52]

This aspect of identifying targets without the knowledge of their full name is also related to the collection of data in the form of metadata. Authorities received data points that served as a proxy of behaviour, revealing no content of the SMS messages or phone calls. Based on these data points, Skynet created digital maps of suspected terrorist couriers' travel patterns and networks on the ground in Pakistan. In this process, data traces were transformed into digital identities. Even though the authorities had no way of understanding the intentions of surveilled individuals, the collection of vast phone sim data together with behaviour-based analytics was considered a sufficient basis to suspect or conclude the involvement in terrorist activities.

This aspect of creating terrorist suspects has been problematised by several scholars. Perugini and Gordon, for example, observed that maps of features, relationships, places and things constituted a pattern of life that was 'considered co-extensive with the life of a terrorist' in the eyes of the analyst.[53] Weber further adds that the association made between the patterns of life and the terrorist suspicion is an arbitrary one, lacking any 'transparent or consistent line of argument that would justify the criteria and render them coherent'.[54] In their analysis, Aradau and Blanke emphasise that what makes the transformation from anomalies to suspicion possible is the use of socio-technical devices such as Skynet. As they explain, algorithmic tools significantly influence the production of knowledge and formation of terrorist profiles, transforming the unknowable digital points into *tenable* terrorist identities.[55] Below, we expand on ways in which legal devices (or a lack thereof) enable the co-production of suspected terrorists.

Legal Indeterminacies

In this sub-section, we further elaborate on the role of legal instruments in these socio-technical practices. The United States Presidential Policy Guidance was already mentioned to highlight that on the domestic level it authorised the targeting of suspected terrorists without the knowledge of their full names. In this section, we focus on the role of legal norms in the practices around Skynet and how terrorist suspects are produced.

We need to start by highlighting that in the context of the US drone strikes in Pakistan, the assessment of the legal framework relevant for the selection of terrorist suspects has been contested. This constitutes the first legal indeterminacy. Whereas some considered the strikes to be a form of lawful or justifiable self-defence within the context of the broader United States war with Al-Qaeda in Afghanistan, others argued that these were unlawful extrajudicial killings because the United States did not act in self-defence and did not have permission from the Pakistani government for their engagement. The United Nations Special Rapporteur in 2010 also failed to reach a conclusion on whether the United States was legally engaged in an armed conflict in Pakistan in the years prior.[56] Unsurprisingly, in 2013 the United States administration remained silent about the legal basis that it used to target individuals in Pakistan.[57] However, regardless of the applicable international legal framework (international armed conflict, non-international armed conflict or self-defence), legal indeterminacies are prevalent and often leave a broad margin of discretion that contributes to the identification of terrorists, and even more to the production of terrorist *suspects*. Who is a combatant, who is directly participating in hostilities or whether they pose an imminent threat are all crucial legal questions that are increasingly being decided upon on the basis of behavioural pattern analysis.

[50] "SKYNET: Applying Advanced Cloud-Based Behavior Analytics."
[51] Currier, "U.S. Government."
[52] *Zaidan et al v Trump et al*. Complaint paragraph 61.
[53] Perugini, "Distinction," 1393.
[54] Weber, "Keep Adding."
[55] Aradau, Algorithmic Reason.
[56] Sullivan, The Law of the List.
[57] Amnesty International "Will I Be Next?"

When it comes to targeting in international armed conflicts, legal categories of combatants and civilians (or non-combatants) are already very vague, but emerging socio-technical forms of engagement in violence further challenge these distinctions. Warfare is characterised by what Perugini and Gordon call 'liminal entities' – persons whose engagement in violence lies between the rigid positions assigned by law, such as that of human shields.[58] They are neither civilians nor fully combatants, and thus fall within a legal grey space where they lack adequate legal protection. The changing landscape of warfare, targeting enabled by behaviour pattern recognition technologies but also the legal 'apparatus of distinction', blurs the lines between lawful and unlawful targets, further fostering 'liminality' and obscuring the lines of lawful use of force.

Such liminalities also exist in the context of non-international armed conflicts. One such liminal category is the 'continuous combat function' (CCF). The term was introduced by the ICRC in a report from 2009, which refers to an individual who assumes a continuous function of direct participation in hostilities on behalf of a non-state armed group party to a conflict, and therefore can lawfully be targeted.[59] The definition of CCF, as introduced by the ICRC, effectively expands the category of 'direct participation in hostilities', which requires observable hostile acts. The ICRC does not provide clear criteria on the basis of which CCF is to be determined. In her analysis, Mignot-Mahdavi argues that the CCF is an open-textured term that 'allow[s] for targeting practices beyond areas and moments of active hostilities', and instead opens doors for targeting practices based on *'suspicious behaviour patterns*'.[60] CCF is a fluid legal concept that facilitates counterterrorism interventions on the basis of associations made between behavioural patterns and suspicions of involvement in terrorism.

Similar trends are found when applying the right to self-defence. On some accounts, the United States claimed that in accordance with United Nations Charter Article 51 (when interpreted to include right to pre-emptive self-defence) and due to 'a continuing, imminent threat to US persons', the United States had a legal right to use lethal force in self-defence.[61] However, Amnesty International reported that the United States killed individuals even 'in the absence of any intelligence about a specific planned attack', and stretched the term 'imminent threat' 'beyond its ordinary meaning and established interpretations under the existing international law'.[62] As shown, even in the context of self-defence, an elastic interpretation of the legal terms allowed for the killings of individuals on the basis of incomplete intelligence and algorithmic filtering mechanisms.

This section has discussed the indeterminacy of legal frameworks governing the conduct of hostilities in the context of the United States' engagement in Pakistan, during which Skynet was used to counter Al-Qaeda members. We argued that this legal vagueness has contributed to the possibilities of counter-terrorism interventions. The trial-and-error process whereby Skynet was constantly evolving to include new markers (e.g. Sikh) or behavioural features (e.g. phone usage) until it met the expectations of the users is one example how human labour, stereotyping, the opacity of data-driven algorithms and liminality of legal categories played a role in co-producing terrorist suspects and justified pre-emptive self-defence counter-terrorist interventions.

4. Discussion: Three Concerns in the Co-production of 'Terrorist Suspects'

We draw on our two case studies to illustrate that these are not separate listing instances, but rather there is something fundamental to this practice that challenges traditional meanings and classifications of law. We argue that traditional logics of the law that approach counter-terrorism by classifying measures into legal regimes, separating the domestic from the international, isolating digital infrastructures and dividing terrorists from non-terrorists are insufficient to understand the production of terrorist suspects and counter-terrorism interventions. We propose that it is crucial for researchers to look beyond the legal frameworks and categories and continue to unpack these complex and evolving associations of security assemblages. We highlight three concerns that emerged from the case studies: (1) behavioural patterns and suspicion; (2) the flow of data from one database to another; and (3) the need to rethink law to address the security assemblages facilitated by listing practices.

4.1 Concern 1: Behavioural Patterns and Suspicion

Scholars have reflected on how traditional counter-terrorism practices draw suspicion of involvement in terrorism on the basis of so-called '*guilt by association*'.[63] If you are a brother or a friend of a listed terrorist, even if you are unaware of their terrorist activities and/or that person has not been proven to be a terrorist yet, your familial link to that person may lead to suspicion and your inclusion on a counter-terrorism database. This practice, which has been criticised, is based on an understanding that

[58] Amnesty International "Will I Be Next?"
[59] Melzer, "Interpretive Guidance."
[60] Mignot-Mahdavi, "Rethinking Direct Participation."
[61] Amnesty International, "Will I Be Next?," 52.
[62] Amnesty International, "Will I Be Next?," 52.
[63] Cole, "Secrecy, Guilt."

terrorist organisations 'usually enjoy strong support by the member's immediate environment' and an assumption that this support also indicates a shared religious or ideological motivation.[64]

Yet, our analysis also illustrates that *association*, when produced by algorithms, is not a result of sharing the same family or friend circles as 'guilt by association' is traditionally understood. Instead, the association is digitalised in the form of behavioural patterns and digital maps that redefine terrorist identities: knowing a person suspected of terrorism is not necessary for suspicion and inclusion on the list to materialise. In the new digitalised forms of guilt by association, if you live in the same city, travel by plane in similar frequencies but also, more abstractly, make similar number of calls a day, then your behavioural patterns may be *associated* with the patterns of a listed terrorist leading to the production of knowledge about potential terrorist identity and inclusion on the list. Association in automated listing practices is expanded beyond family ties and more loosely includes a variety of features that indicate life patterns. While these traces have an origin in actual human behaviour, our case studies reveal a similar pattern of disembodiment and post-humanistic visions of a human body as discussed by Perugini and Gordon;[65] those listed identities become more and more digital and detached from the context in which the original behaviour of individuals emerged.

In the case of the Skynet algorithm, abstract patterns of movement, phone usage and calling habits become grounds for inclusion on the list, while in the case of the FSPRT list, a mix of automated decisions and subjective risk indicators, such as watching violent videos or sleeping on the floor, drives inclusion on the list. Similarly, in the case of recently reported automated decision-making system "Lavender" used by the Israeli Defence Forces, the reports indicate that listing individuals as Hamas associates is based on loose associations in patterns of features 'such as being in a WhatsApp group with a known militant, changing cell phone every few months, and changing addresses frequently'.[66]

Emerging list-plus-algorithms facilitate the formation of 'guilt by association' by using *any* data points that are available, many of which are abstract. As shown in the case studies, any type of behaviour can become 'suspicious' if the algorithm identifies it as a proxy for 'association'. Mathematical operations conducted by algorithms draw *correlations* between data points rather than causation. Weber also argues that the association of 'patterns of life and suspicion of terrorism' is arbitrary, because it lacks any 'transparent or consistent line of argument that would justify the criteria and render them coherent'.[67] In other words, the decision that is legal in its effect – to include someone on the terrorist list – is made on the basis of associative claims that do not necessarily amount to substantial evidence about the (suspected) involvement in terrorism.

4.2 Concern 2: From One Database to Another

As behavioural patterns become fundamental in the identification of suspicious threats, it is essential to better understand the broader landscape of digital technologies in which both the FSPRT and the Skynet algorithms operate. The current landscape of terrorist lists and databases is extensive, encompassing a wide range of digital infrastructures – from international criminal databases to domestic medical dossiers. As shown in our research, these lists become connected when data from one database is used to inform characterisation of digital identities stored in another database.[68] Legal frameworks such as domestic surveillance legislation and international obligations to exchange data from watchlists, as well as technical devices, data flows and various actors, are involved in practices of collecting and sharing of data. By zooming out to this global framework, we show that behavioural patterns and risk indicators are not static data points but are shared and reinterpreted across different databases. In doing so, the scope for novel conditions of security interventions widens.

In the case of France, we see that the FSPRT list is associated with various domestic security agencies and legal institutions – for example, intelligence services, police, courts, TRACFIN and the Department of Justice, as well as the databases of EUROPOL.[69] There is also a mention of association with the domestic S-list; however, specific details of how data flow from one list to another are not available. All these lists have different purposes, and the scope of their data collection is significantly different; nonetheless, when connected, these lists can feed into one another and contribute to the level of suspicion. This is

[64] Levanon, "Criminal Prohibitions," 261.
[65] Perugini, "Distinction."
[66] Abraham, "Lavender."
[67] Weber, "Keep Adding."
[68] Here, our understanding of interoperability between these different databases aligns with the concepts presented by Bellanova and Glouftsios, who observe that security infrastructure interoperability in the European context is not achieved by pulling all data into a new single database, but rather by 'designing, implementing and reorganising a series of infrastructural elements that store, match, associate and repurpose data sets stored in already existing systems'. Similarly, we observe how data points travel from one database to another without having necessarily been embedded in a coherent data infrastructure.
[69] See the analysis of the case study above for reference to each database.

particularly problematic when we look at the legal decision of the French government to expand surveillance into medical dossiers through *automated linkages* between terrorism and psychiatric databases. The data flow is made through informal procedures, requiring only a confirmation of identity. Here, data gathered and governed in a medical context become *associated* with terrorist intent.

Both the Skynet program and the FSPRT watchlist are elements of a larger global counter-terrorism trend. The law does not only facilitate the exchange of data on a domestic level but also encourages connections and flows of data between *different* lists, such as watchlists, kill lists and other databases such as the INTERPOL criminal database. Identities of suspected terrorists migrate from one list to another, sometimes with little oversight. For example, the Watchlisting Toolkit indicates that states may include names on their lists received from foreign partners even if 'specific information as to why the individual is in a watchlist' is not provided 'due to national security reasons'.[70] In other words, individuals can be watchlisted, and their data shared, while agencies remain blind to the evidence that led to their inclusion in the first place. Identities are difficult to get off the list and their data points easily migrate from one list to another. In these socio-technical practices, data from different one database travel into another and become entangled in the co-production of knowledge about suspected terrorists.

4.3 Concern 3: Rethinking Law

In this section, we bring forward considerations of the regulatory role of legal instruments, specifically in relation to the provisions of redress and oversight. Redress is an important legal procedure that should be made available to the individuals who are targeted, whose assets are frozen or who cannot cross borders due to their listing as terrorists. It provides individuals with the possibility to challenge their inclusion on the terrorist databases and seek remedy. Legal redress in the context of listing takes a binary approach, whereby one is either innocent or guilty, 'in' or 'off' the list, supported by evidence. The stark line between innocence and guilt, however, is often blurred in the context of pre-emptive security: individuals might not have crossed a legal line but can potentially do so in the future. Our case studies illustrate that the legal options to curtail the power of pre-emptive security logics remain limited, risking leaving databases without oversight and individuals without legal remedy. The example below, which relates to the Skynet program, exemplifies this dynamic.

In 2019, Zaidan and Kareem sought legal remedy from the US government after allegedly being attacked several times by drones while they remained in Syria.[71] Zaidan claimed that at least on five occasions drone attacks were deployed in his close proximity, which made him believe that he was on a US target list. Zaidan and Kareem claimed that their inclusion on the kill list was unsubstantiated and the attempted attacks unlawful, and both sought legal remedy in a US District Court. The plaintiffs, however, restrained from accessing the US kill lists and other databases, and were unable to deliver further evidence of their inclusion on the list beyond the shadow of a doubt. The case was eventually dismissed because of a lack of evidence, despite the fact that the Intercept also reported that Zaidan was already identified as an Al-Qaeda member *before* the drone attacks took place, specifically on 'the Terrorist Identities Datamart Environment, or TIDE, [which] is a U.S. government database of over one million names suspected of a connection to terrorism, which is shared across the U.S. intelligence community'.[72] Nonetheless, no satisfactory evidence was presented to prove how these databases were connected and whether information was shared between them. In the court's analysis, the allegations of Zaidan's inclusion on the list were 'conjectural' and it was not possible to 'allege adequately a link between Skynet and the Kill List'. The observation remained only speculative and associative. While Zaidan and Kareem had ample examples of events that would indicate that they were being actively targeted in Syria, the case was dismissed. Their legal claims met with unsatisfactory results primarily due to the inability of the court to establish *clear links* between the drone attacks, the Skynet program and their possible inclusion on the kill list.[73]

This case illustrates how terrorist databases and lists do not work within the confines of legal categories – pre-emption and algorithmic tools condition counter-terrorism practices to form associations and dynamic interpretations of suspicion. While associations are always part of evidencing guilt or innocence in the context of (de)listing, we observe that individuals are included in extensive databases of which the categories vary according to segments of 'dangerousness', and information is shared between databases combining knowledge on suspected individuals in an automated way. This form of ordering has little to do with the legal categories of 'known terrorists' or 'suspected terrorists', which means redress options are limited. Instead, enabled by algorithmic technologies, these list-plus-algorithms tend to be unstable, which disrupts the traditional legal logics of solid categorisations.

[70] Counterterrorism Watchlisting Toolkit, 31.
[71] *Zaidan et al v Trump et al.* Memorandum Opinion.
[72] Currier, "U.S. Government."
[73] US District Court 'Memorandum Opinion' in Aradau, Others, 87.

5. Conclusion: Regulating Socio-technical Surveillance Assemblages

In this article, we have demonstrated through two empirical case studies how legal frameworks, security logics and surveillance technologies produce a novel form of countering terrorism. Departing from an assemblage approach, we conducted an interdisciplinary analysis of how terrorism lists work in practice, which laws shape them and how data are collected for the purpose of countering terrorism. Our empirical analysis shows that such an approach is essential if we want to understand the complexity of listing practices, particularly in an age where many decisions are becoming more automated. This assemblage approach allows us to distil three critical concerns from our empirical case studies for the role of law and its relationship to algorithmic surveillance for counter-terrorism purposes.

The theoretical argument that we have put forward in this article seeks to question the assumption that algorithmic decision-making to identify terrorist suspects works towards more precise and clear legal definitions. We propose that the logic that drives the list – more precise and better-defined legal options to intervene – is the opposite of what the list produces. The pre-emptive security logic facilitates the creation of terrorist profiles from a combination of irregular data points that, in essence, say very little about terrorism, radicalisation or threat, but when *associated* together and *materialised* through algorithmic ordering can lead to grounds for further surveillance and interventions. Legal frameworks to regulate and govern such practices remain broad and exempt national security matters from strict oversight, thus extending the power of the list rather than curtailing it. Consequently, our analysis concurs with John's argument that 'the associative work that list-plus-algorithms do would entail horizontal inquiry and organising, rather than a preoccupation with vertical relationships and tracing claims back to the feet of one or other perceived puppet-master'.[74]

Our empirical analysis has illustrated that in both case studies, law's focus on binary categories of enlisted/delisted or guilty/innocent is not well equipped to deal with the fluid and complex ways in which data are shared across databases. Furthermore, the empirics illustrate that options for redress are limited due to the automated processes and lack of algorithmic oversight. Thus, further research should focus on how legal frameworks can limit the possibilities of collecting and sharing data, particularly as possibilities for algorithmic surveillance technologies are increasing, in the context of both warfare and national security.

Acknowledgements
The authors are thankful for the generous feedback received at the ESIL IG International Law and Technology working group during the ESIL annual conference in Utrecht in 2022. We are also thankful for the useful comments by our colleagues from the Transnational Legal Studies department at the Vrije Universiteit Amsterdam, and the two anonymous peer reviewers for their insightful comments on earlier drafts of this article.

Klaudia Klonowska's contribution to this article was conducted within the context of the DILEMA Project on Designing International Law and Ethics into Military Artificial Intelligence, funded by the Dutch Research Council (NWO) Platform for Responsible Innovation (NWO-MVI).

[74] Johns, "Global Governance," 143.

Bibliography

Amnesty International. "'Will I Be Next?' US Drone Strikes in Pakistan." Amnesty International, October 21, 2013. https://www.amnestyusa.org/reports/will-i-be-next-us-drone-strikes-in-pakistan.

Amoore, Louise. "The Deep Border." *Political Geography* 109 (2024): 102547. https://doi.org/10.1016/j.polgeo.2021.102547.

Amoore, Louise. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham, NC: Duke University Press, 2020.

Aradau, Claudia and Tobias Blanke. *Algorithmic Reason: The New Government of Self and Other*. Oxford: Oxford University Press, 2022.

Aradau, Claudia and Tobias Blanke. "Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data." *European Journal of Social Theory* 20, no 3 (2017): 373–391.

Blank, Laurie R. and Benjamin R. Farley. "Characterizing US Operations in Pakistan: Is the United States Engaged in an Armed Conflict." *Fordham International Law Journal* 34 (2010): 151. https://ir.lawnet.fordham.edu/ilj/vol34/iss2/2.

Christakis, Theodore. "National Security, Terrorism and the Legality of Secret Surveillance: The Case of France." In *Terrorists' Use of the Internet*, edited by Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald and Lella Nouri, 327–337. Amsterdam: IOS Press, 2017.

Cloatre, Emily. "Law and ANT (and Its Kin): Possibilities, Challenges, and Ways Forward." *Journal of Law and Society* 45 (2018): 646. https://onlinelibrary.wiley.com/doi/pdf/10.1111/jols.12133.

Code de la sécurité intérieure ReplierPartie législative (Articles L111-1 à L898-1). https://www.legifrance.gouv.fr/codes/id/LEGISCTA000030934655.

Cole, David. "Secrecy, Guilt by Association, and the Terrorist Profile." *Journal of Law and Religion* 15 (2001): 197–218. https://www.austlii.edu.au/cgi-bin/viewdoc/au/other/lawreform/ALRCDP/2004/67.pdf.

Conseil d'Etat 27 Mars 2020. Analyse n° 431350. https://www.conseil-etat.fr/fr/arianeweb/CE/analyse/2020-03-27/431350.

Conseil D'état, 13 March 2020. N°s 431350, 431530, 432306, 432329, 432378, 435722. https://www.santementale.fr/medias/userfiles/files/hopsyweb-rejet.pdf.

Currier, George, Glenn Greenwald and Andrew Fishman. "U.S. Government Designated Prominent Al Jazeera Journalist as 'Member of Al Qaeda'." *The Intercept*, May 8, 2015. https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list.

De Goede, Marieke, Anna Leander and Gavin Sullivan. "Introduction: The Politics of the List." *Environment and Planning D: Society and Space* 34, no 1 (2016): 3–13. https://doi.org/10.1177/0263775815624561.

Decree No. 2018-383 of 23 May 2018 authorizing the processing of personal data relating to the follow-up of people in psychiatric care without consent. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036936873.

Décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036936873.

Deliberation no. 2018-354 of December 13, 2018 providing an opinion on a draft decree amending decree no. 23 May 2018 authorizing the processing of personal data relating to the monitoring of people in psychiatric care without consent (request for opinion no. 18020552). https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038445390.

Deliberation No. 2022-046 of 14 April 2022 giving an opinion on a draft decree amending Decree No. 2018-383 of 23 May 2018 authorizing the processing of personal data relating to the follow-up of persons in psychiatric care without consent (request for opinion No. 22005342). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045684637?init=true&page=1&query=caractère+personnel+relatifs+au+suivi+des+personnes+en+soins+psychiatriques+sans+consentement+&searchField=ALL&tab_selection=all.

Downey, Anthony. "Algorithmic Predictions and Pre-emptive Violence: Artificial Intelligence and the Future of Unmanned Aerial Systems." *Digital War* 5, no 1 (2024): 123–133. https://doi.org/10.1057/s42984-023-00068-7.

Fédération Francaise de Psychiatrie. "Affaire Hopsyweb." https://fedepsychiatrie.fr/wp-content/uploads/2022/05/Decret-27042022-SSC-Hopsyweb-1.pdf.

Follorou. « Les failles » de la lutte antiterroriste,' *Le Monde*, November 19, 2015. https://www.lemonde.fr/attaques-a-paris/article/2015/11/19/les-failles-de-la-lutte-antiterroriste_4813166_4809495.html.

Hellmuth, Daniel. "Countering Jihadi Terrorists and Radicals the French Way." *Studies in Conflict & Terrorism* 38, no 12 (2015): 979–997. https://doi.org/10.1080/1057610X.2015.1076277.

Interministerial Committee for the Prevention of Crime and Radicalisation. 11 April 2019. https://www.cipdr.gouv.fr/wp-content/uploads/2019/04/2019-04-11-CIPDR-ANG-V2-2.pdfbat.pdf.

Johns, Fleur. "Global Governance through the Pairing of List and Algorithm." *Environment and Planning D: Society and Space* 34 (2016): 126–147.

Johns, Fleur, *Non-Legality in International Law: Unruly Law*. Cambridge: Cambridge University Press, 2013.

Kassem, Ramzi, Rebecca Mignot-Mahdavi, and Gavin Sullivan. "Watchlisting the World: Digital Security Infrastructures, Informal Law and the 'Global War on Terror'". *Just Security,* October 28, 2021.

https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror.
Kaufmann, Mareile, Simon Egbert and Matthias Leese. "Predictive Policing and the Politics of Patterns." *The British Journal of Criminology* 59, no 3 (2019): 674–692. https://doi.org/10.1093/bjc/azy060.
Le fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) (14-10-2022) Direction Générale de la Sécurité Intérieure. https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents/fichier-de.
Le Parisien. «terrorisme»: plus de 8000 personnes fichées pour radicalisation, annonce Darmanin,' August 31, 2020. https://www.leparisien.fr/faits-divers/terrorisme-plus-de-8000-personnes-fichees-pour-radicalisation-annonce-darmanin-31-08-2020-8375955.php.
Le Parisien. "Radicalisés: Les plus dangereux sont suivis par la DGSI." https://www.leparisien.fr/faits-divers/les-plus-dangereux-sont-suivis-par-la-dgsi-25-01-2017-6614685.php/.
Leander, Anna. "Technological Agency in the Co-Constitution of Legal Expertise and the US Drone Program." *Leiden Journal of International Law*, 26, no 4, (2013): 811–834.
Levi, Ron and Mariana Valverde. "Studying Law by Association: Bruno Latour Goes to the Conseil d'Etat." *Law & Social Inquiry* 33, no. 3 (2008): 805–825. https://doi.org/10.1111/j.1747-4469.2008.00122.x.
LOI n° 2015-912 du 24 juillet 2015 relative au renseignement (1).
Melzer, Nils. *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. Geneva: International Committee of the Red Cross, 2009.
Mignot-Mahdavi, Rebecca. *Rethinking Direct Participation in Hostilities and Continuous Combat Function in Light of Targeting Members of Terrorist Groups*. Manchester: *University of Manchester,* 2021.
Mignot-Mahdavi, Rebecca. "All About Forms: Global Security Governance and International Law." Paper presented at the European Society of International Law Research Forum in Glasgow, 31 March 2022.
Ní Aoláin, Fionnuala. "Soft Law, Informal Lawmaking and 'New Institutions' in the Global Counter-Terrorism Architecture." *European Journal of International Law* 32, no 3 (2021): 919–942. https://doi.org/10.1093/ejil/chab071.
Perugini, Nicola and Neve Gordon. "Distinction and the Ethics of Violence: On the Legal Construction of Liminal Subjects and Spaces." *Antipode* 49, no 5 (2017): 1385–1405. https://doi.org/10.1111/anti.12343.
Puar, Jasbir K. *Terrorist Assemblages: Homonationalism in Queer Times*. Durham, NC: Duke University Press, 2018.
Smith, Adam. "Drones as Techno-Legal Assemblages." *Law, Technology and Humans* 4, no 2 (2022): 152–165. https://doi.org/10.5204/lthj.2333.
Sullivan, Gavin. "Law, Technology, and Data-Driven Security: Infra-Legalities as Method Assemblage." *Journal of Law and Society* 49 (2022): S31–S50. https://doi.org/10.1111/jols.12352.
Sullivan, Gavin and Marieke De Goede. "Between Law and the Exception: The UN 1267 Ombudsperson as a Hybrid Model of Legal Expertise." *Leiden Journal of International Law* 26 (2013): 833–854. https://doi.org/10.1017/S0922156513000435.
Sullivan, Gavin. *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law*. Cambridge: Cambridge University Press, 2020.
The Intercept. "Skynet: Applying Advanced Cloud-Based Behavior Analytics." May 8, 2015. https://theintercept.com/document/2015/05/08/skynet-applying-advanced-cloud-based-behavior-analytics.
Interministerial Committee for the Prevention of Crime and Radicalisation. *The State, Territorial Authorities, and Society: A Chain of Protection Against Radicalisation.* February 23, 2018–April 11, 2019. https://www.cipdr.gouv.fr/wp-content/uploads/2019/07/2019-04-11-CIPDR-ANG-V2-2.pdfbat.pdf.
Weber, Jutta. "Keep Adding. On Kill Lists, Drone Warfare and the Politics of Databases." *Environment and Planning D: Society and Space* 34, no 1 (2016): 107–125. https://doi.org/10.1177/0263775815623537.
Zaidan et al v Trump et al. Memorandum Opinion (District Court 2019). https://law.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2017cv00581/185403/29.