The Politics of Security Lists

de Goede, M.; Sullivan, G.

DOI
10.1177/0263775815599309
Publication date
2016
Document Version
Final published version
Published in
Environment and Planning D - Society & Space

Article

Society and Space

Environment and Planning D: Society and Space
2016, Vol. 34(1) 67–88

DOI: 10.1177/0263775815599309
epd.sagepub.com
SAGE

The politics of security lists

Marieke de Goede
University of Amsterdam, the Netherlands

Gavin Sullivan
University of Kent, UK

Abstract
The List, one of the most archaic means of written enumeration and classification, has made a forceful recurrence in the post-9/11 global security landscape. From terrorist sanctions lists and No-Fly lists to "kill-lists" for drone warfare; from the privately compiled lists of risky banking clients to the regulatory lists of untrustworthy or incompliant companies, the list seems to proliferate as a contemporary technology of security and regulation. How and why are lists becoming newly embedded in security practices? What work do lists perform as specific techniques of government and forms of normative ordering? And what consequences follow for how problems of legal accountability and political responsibility are currently understood and addressed? This paper frames security lists as inscription devices that are heterogeneous, unpredictable and *productive* in unforeseen ways. It draws attention to the ways they materialise the categories they purport to describe, and how they enact novel forms of knowledge, jurisdiction and targeting. We suggest that critiques could be strengthened by making visible and contesting the fragmented and diffuse conditions through which security lists are produced.

Keywords
Lists, devices, law, security, technology

> "The material culture of bureaucracy and empire is not found in pomp and circumstance, nor even in the first instance at the point of a gun, but rather at the point of a list." (Bowker and Star, 1999: 137).

Introduction: The revival of the list

The List, one of the most archaic means of written enumeration and classification, has made a forceful recurrence in the post-9/11 global security landscape. From No-Fly lists to "kill-lists" for drone warfare; from the privately compiled lists of risky banking clients to the regulatory lists of untrustworthy or incompliant companies, the list seems to proliferate as a

The authors contributed equally to the paper

Corresponding author:
Marieke de Goede, Department of Political Science, University of Amsterdam, Postbus 15578, 1001NB Amsterdam, the Netherlands.
Email: m.degoede@uva.nl

contemporary technology of security and regulation. At the same time, lists appear as technical instruments that order the world in relatively straightforward ways and are considered to be fairly innocuous by the security professionals who use them. Within critical security studies, lists have not nearly generated as much critical debate as other technologically-driven security practices like extraordinary rendition or algorithmic datamining (e.g. Amoore, 2013; Bellanova and González Fuster, 2013; Blakely, 2007; Leese, 2014).

Probably the most well-known and controversial list in contemporary security is the secret kill lists used by the US authorities for their targeted killing program. It is well known that US drones and special-op task forces carry out targeted killings operations in Pakistan, Yemen, Somalia and elsewhere on the basis of lists designating suspected terrorists or "high-value targets" for capture or killing. Nominations for listing and processes of targeting are acknowledged to be contentious and subjective. According to one former Chief of Staff interviewed in the *New York Times* (NYT) those involved recognise that "this isn't science, this is judgments made off of, most of the time, human intelligence" (cited in Becker and Shane, 2012). Listing involves a continuous process of discussion, inclusion and replacement of names. "One guy gets knocked off, and the guy's driver, who's No. 21, becomes 20?" one interviewee of the NYT said, "At what point are you just filling the bucket with numbers?" (cited in Becker and Shane, 2012). At the same time, killing listed individuals is primarily undertaken on the basis of metadata analysis and geolocational phone tracking technology, suggesting the emergence of more complex ensembles of kill-lists, technical objects and targets (Scahill and Greenwald, 2014). As one former drone operator from the US military's Joint Special Operations Command (JSOC) put it: "People get hung up that there's a targeted list of people . . . [but] it's really like we're targeting a cell phone. We're not going after people – we're going after their phones, in the hopes that the person on the other end . . . is the bad guy" (cited in Scahill and Greenwald, 2014).

Whilst kill-lists are the most lethal variety, other forms of contemporary security listing affect larger (and ever-increasing) numbers of individuals. The Terrorist Identities Datamart Environment (TIDE), for example, maintained by the US National Counterterrorism Center (NCC), is a classified "master database" that includes over 1.1 million entries since August 2014 (Bennett, 2008; Handeyside, 2014). An unclassified extracted version of TIDE is fed into the US Department of Homeland Security Terrorist Screening Database (TSDB), containing about 680,000 names related to suspected terrorism. The TSDB provides the basis for both the Federal Bureau of Investigation's (FBI's) "No-Fly" list used by frontline officials to bar individuals from boarding planes travelling to, from or over the US and a "Selectee list" that identifies passengers for more intensive security screening and questioning. Cumulatively, these aviation lists contained 119,000 names in 2006 (American Civil Liberties Union (ACLU), 2006), a number which is likely to have grown substantially since. Listed individuals have no formal means to find out if or why they are listed, and instructions to front-line staff are to "neither [confirm] nor [deny] whether an individual is on the Terror Watchlist" (NCC, 2013: 54). Whilst officials receive *pro forma* instructions on how to handle potential encounters with listed parties, no background information or grounds for listing are contained in the database or otherwise made available for operational use. As we discuss below, US counterterrorism lists rely on a functional "division of evaluative labour" whereby different actors and institutional agencies work in a heterogeneous ensemble to "set the predictive criteria, make the prediction, validate it, and use it" (Bernstein, 2013: 484).

By comparison, an estimated 214 financial sanctions list worldwide prohibit the provision of support to the individuals and entities that they target. Many of these lists apply

extraterritorially, or are enforceable by states in relation to non-citizens acting outside that state's boundaries. Banks, other financial institutions and NGOs working in risky environments are increasingly required to monitor not just the lists that operate globally (such as the various UN targeted sanctions regimes) or in their home countries, but those operating extraterritorially across multiple jurisdictions. As regulatory requirements flowing from sanctions have become increasingly complex, private companies like World-Check have emerged to consolidate and translate the different lists into saleable and searchable compliance products. However, World-Check – a leading provider of compliance software for the financial services – does not simply compile pre-existing sanctions lists data. As we will discuss in this paper, they also "add value" during the list compilation process by providing their own open-source intelligence and risk-analysis.

From the vantage point of risk-based security cultures oriented pre-emptively toward catastrophic futures, this resurgence of the list is puzzling (Amoore, 2013; Aradau and van Munster, 2011). How is it – in a world marked by radical uncertainty, complex algorithmic datamining and sophisticated colour-coded visualisations of danger – that the "lowly, dull [and] mechanical" knowledge-practice of listing has made such a comeback (Bowker and Star, 1999: 137)? As Urs Staeheli (2012: 233) points out, the list is one of the 'oldest' modes of knowledge and communication; it promises order as well as open-endedness, exhaustiveness as well as infinite addition. How and why are lists becoming newly embedded in countering terrorism, fighting fraud, managing borders, protecting customers and other security practices? What work do lists perform as specific techniques of government and forms of normative ordering? And what consequences follow for how problems of legal accountability and political responsibility are understood and addressed?

This paper analyses how security lists operate as knowledge practices and modes of (legal) ordering. Our purpose is not to suggest that existing (juridical) analyses of the problems surrounding blacklists are wrong, but to *shift perspective:* what do we see when we start with the question of the power and the form of the list? What are the implications of putting the lists itself centre stage in critical research on blacklisting? It is important to understand that the list as a knowledge form has the capacity to *do* things – as Law and Mol (2002: 7) point out for example, lists "assemble elements that that do not necessarily fit together into some larger scheme." This paper endeavours to "remain in the register of the list" (Johns, this issue), in order to analyse security lists' capacities for knowing, ordering and connecting. We do so by approaching security lists as inscription devices. For John Law and Evelyn Ruppert, "devices" are functional and strategic: "devices *do* things" (emphasis in original). However, this "doing" is not just programmatic, because devices are heterogeneous and unpredictable. Lists are *productive* in unforeseen ways (Law and Ruppert, 2013: 230; also Amicelle et al., 2015). This approach expands our understanding of listing practices to encompass their collateral realities and internal tensions.

Whilst we aim to contribute to broader discussions concerning the list as a governance device, the empirical focus of this paper is on security lists – including counterterrorism watchlists, targeted sanctions blacklists and private risk management databases. We start by developing the framework of device, to show how it provokes a different set of questions about how security lists enact novel forms of knowledge, jurisdiction and targeting. The paper then analyses the key themes of criteria, consolidation and critique. We suggest that challenges to security lists could be strengthened by relying not only on due process principles but also making visible and more forcefully contesting the fragmented and diffuse juridical disconnections/connections produced through lists.

From instruments to devices

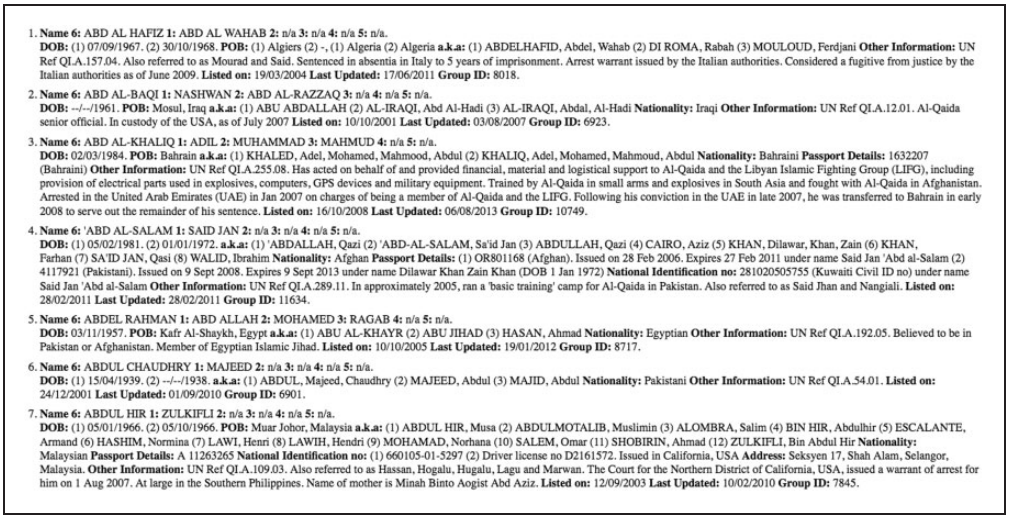
Our starting point is a departure from the instrumental view that lists simply compile or represent pre-existing information. Instead, we understand Lists as "inscription devices" that *produce* specific material, political and legal effects (Latour, 1986; Latour and Woolgar, 1986; Law and Ruppert, 2013) Research on security listing remains dominated by two interrelated schools of thought – international relations scholarship on targeted sanctions and counterterrorism financing policies (Biersteker and Eckert, 2007; Giumelli, 2011), and legal scholarship highlighting the ways that sanctions lists generate conflict between the UN, EU and national legal orders (de Búrca, 2010; Isiksel, 2010). Both approaches tend to be positivist in outlook, normative in focus and primarily concerned with questions of political or legal authority. Security lists are broadly considered as either "information repositories" or "neutral backdrop[s] of impartial information . . . [that] have no effects on the world themselves" (Bernstein, 2013: 485, 464). These approaches have been very important in pushing the political problems of security lists to the surface, including their secrecy and use of intelligence. However, they often frame the key problem as one of *balancing* the competing demands of international security and human rights.

Using the lens of the device to examine security lists opens up a different mode of analysis and critique. It involves analysing the productive capacities of lists, and asking:

> . . . where and how they happen, who and what they are attached to and relations they forge, how they get assembled, where they travel, their multiple arrangements and mobilizations and . . . their instabilities, durabilities and how they . . . get disaggregated (Law and Ruppert, 2013: 32).

Concretely, we identify four analytical shifts rendered possible through the lens of understanding security lists as devices. First, framing security lists as devices draws attention to their specific ordering qualities. As forms of inscription, lists privilege over-generalised schema through de-contexualisation and the use of simplified formatting (Goody, 1977: 105–106). Lists promise order by providing concrete inventories of items in a given category, and they flatten complexity by drawing disparate items into abstract, commensurate relation. They function as particular technologies of ordering and homogenisation. In their analysis of credit retail industry listing, Andrew Leyshon and Nigel Thrift (1999) coin the phrase "lists come alive" to capture the power of banking retail software as a repository of knowledge that came to slowly replace the experience and judgment of bank's managers. This draws attention to the "liveliness" of lists – both in term's of their mutability and the ways they actively constitute and shape political and professional relations.

Consider the example of Consolidated List of Financial Sanctions Targets as shown in Figure 1, which incorporates the UN Al Qaeda sanctions list into UK law. It has a simple nomenclature that appears unremarkable and a far cry from the sophisticated aesthetics of catastrophe governing (Aradau and van Munster, 2011: 85–106). List entries are arranged alphabetically and are standardised both in format and in their visualisation of biographic information. Yet the "collateral reality" (Law, 2012) of this list is that it connects and homogenises widely diverse entries associated with localised political violence and historically embedded (Islamist) movements – from Egypt to Indonesia, from Palestine to Somalia – into abstract relation. This list does more than compile and classify pre-existing elements from an entity called "al Qaeda". It "comes alive" as an actant, constituting al Qaeda itself as a more or less coherent global terrorist network to be countered. But just as quantification creates metrical relations between disparate things whilst obscuring the



1. **Name 6:** ABD AL HAFIZ **1:** ABD AL WAHAB **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: (1) 07/09/1967. (2) 30/10/1968. **POB:** (1) Algiers (2) -, (1) Algeria (2) Algeria **a.k.a:** (1) ABDELHAFID, Abdel, Wahab (2) DI ROMA, Rabah (3) MOULOUD, Ferdjani **Other Information:** UN Ref QI.A.157.04. Also referred to as Mourad and Said. Sentenced in absentia in Italy to 5 years of imprisonment. Arrest warrant issued by the Italian authorities. Considered a fugitive from justice by the Italian authorities as of June 2009. **Listed on:** 19/03/2004 **Last Updated:** 17/06/2011 **Group ID:** 8018.

2. **Name 6:** ABD AL-BAQI **1:** NASHWAN **2:** ABD AL-RAZZAQ **3:** n/a **4:** n/a **5:** n/a.
DOB: --/--/1961. **POB:** Mosul, Iraq **a.k.a:** (1) ABU ABDALLAH (2) AL-IRAQI, Abd Al-Hadi (3) AL-IRAQI, Abdal, Al-Hadi **Nationality:** Iraqi **Other Information:** UN Ref QI.A.12.01. Al-Qaida senior official. In custody of the USA, as of July 2007 **Listed on:** 10/10/2001 **Last Updated:** 03/08/2007 **Group ID:** 6923.

3. **Name 6:** ABD AL-KHALIQ **1:** ADIL **2:** MUHAMMAD **3:** MAHMUD **4:** n/a **5:** n/a.
DOB: 02/03/1984. **POB:** Bahrain **a.k.a:** (1) KHALED, Adel, Mohamed, Mahmood, Abdul (2) KHALIQ, Adel, Mohamed, Mahmoud, Abdul **Nationality:** Bahraini **Passport Details:** 1632207 (Bahraini) **Other Information:** UN Ref QI.A.255.08. Has acted on behalf of and provided financial, material and logistical support to Al-Qaida and the Libyan Islamic Fighting Group (LIFG), including provision of electrical parts used in explosives, computers, GPS devices and military equipment. Trained by Al-Qaida in small arms and explosives in South Asia and fought with Al-Qaida in Afghanistan. Arrested in the United Arab Emirates (UAE) in Jan 2007 on charges of being a member of Al-Qaida and the LIFG. Following his conviction in the UAE in late 2007, he was transferred to Bahrain in early 2008 to serve out the remainder of his sentence. **Listed on:** 16/10/2008 **Last Updated:** 06/08/2013 **Group ID:** 10749.

4. **Name 6:** 'ABD AL-SALAM **1:** SAID JAN **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: (1) 05/02/1981. (2) 01/01/1972. **a.k.a:** (1) 'ABDALLAH, Qazi (2) 'ABD-AL-SALAM, Sa'id Jan (3) ABDULLAH, Qazi (4) CAIRO, Aziz (5) KHAN, Dilawar, Khan, Zain (6) KHAN, Farhan (7) SA'ID JAN, Qasi (8) WALID, Ibrahim **Nationality:** Afghan **Passport Details:** (1) OR801168 (Afghan). Issued on 28 Feb 2006. Expires 27 Feb 2011 under name Said Jan 'Abd al-Salam (2) 4117921 (Pakistani). Issued on 9 Sept 2008. Expires 9 Sept 2013 under name Dilawar Khan Zain Khan (DOB 1 Jan 1972) **National Identification no:** 281020505755 (Kuwaiti Civil ID no) under name Said Jan 'Abd al-Salam **Other Information:** UN Ref QI.A.289.11. In approximately 2005, ran a 'basic training' camp for Al-Qaida in Pakistan. Also referred to as Said Jhan and Nangiali. **Listed on:** 28/02/2011 **Last Updated:** 28/02/2011 **Group ID:** 11634.

5. **Name 6:** ABDEL RAHMAN **1:** ABD ALLAH **2:** MOHAMED **3:** RAGAB **4:** n/a **5:** n/a.
DOB: 03/11/1957. **POB:** Kafr Al-Shaykh, Egypt **a.k.a:** (1) ABU AL-KHAYR (2) ABU JIHAD (3) HASAN, Ahmad **Nationality:** Egyptian **Other Information:** UN Ref QI.A.192.05. Believed to be in Pakistan or Afghanistan. Member of Egyptian Islamic Jihad. **Listed on:** 10/10/2005 **Last Updated:** 19/01/2012 **Group ID:** 8717.

6. **Name 6:** ABDUL CHAUDHRY **1:** MAJEED **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: (1) 15/04/1939. (2) --/--/1938. **a.k.a:** (1) ABDUL, Majeed, Chaudhry (2) MAJEED, Abdul (3) MAJID, Abdul **Nationality:** Pakistani **Other Information:** UN Ref QI.A.54.01. **Listed on:** 24/12/2001 **Last Updated:** 01/09/2010 **Group ID:** 6901.

7. **Name 6:** ABDUL HIR **1:** ZULKIFLI **2:** n/a **3:** n/a **4:** n/a **5:** n/a.
DOB: (1) 05/01/1966. (2) 05/10/1966. **POB:** Muar Johor, Malaysia **a.k.a:** (1) ABDUL HIR, Musa (2) ABDULMOTALIB, Muslimin (3) ALOMBRA, Salim (4) BIN HIR, Abdulhir (5) ESCALANTE, Armand (6) HASHIM, Normina (7) LAWI, Henri (8) LAWIH, Hendri (9) MOHAMAD, Norhana (10) SALEM, Omar (11) SHOBIRIN, Ahmad (12) ZULKIFLI, Bin Abdul Hir **Nationality:** Malaysian **Passport Details:** A 11263265 **National Identification no:** (1) 660105-01-5297 (2) Driver license no D2161572. Issued in California, USA **Address:** Seksyen 17, Shah Alam, Selangor, Malaysia. **Other Information:** UN Ref QI.A.109.03. Also referred to as Hassan, Hogalu, Hugalu, Lagu and Marwan. The Court for the Northern District of California, USA, issued a warrant of arrest for him on 1 Aug 2007. At large in the Southern Philippines. Name of mother is Minah Binto Aogist Abd Aziz. **Listed on:** 12/09/2003 **Last Updated:** 10/02/2010 **Group ID:** 7845.

Figure 1. Consolidated list of financial sanctions targets in the UK, available at: http://bit.ly/1jFLBSj (Contains public sector information licensed under the Open Government Licence v2.0. Reprinted with permission from the UK National Archives).

contingency of the quantification process itself (Espeland and Stevens, 2008: 422), the list's arrangement as delocalised, technical and depoliticised helps to enclose its creative effects and the politics of commensurability it enables.

Second, understanding lists as devices draws attention to their strategic functionality – or what Ertuk et al. call their ''contrivance'' (2013: 340). The purpose of security lists – such as blacklists and targeted sanctions – is one of pre-emption. They are novel modes of targeting that enable security intervention in advance of conventional judicial processes and before any dangerous act has occurred (de Goede, 2011; Sullivan and Hayes, 2011). Security lists are therefore best understood as forms 'pre-crime', targeting potential threats at an early stage (Zedner, 2007; Krassman 2012). They provide advantage to the executive by carving out of novel logics of inclusion and exclusion and enabling accelerated security governance on the basis of malleable criteria. Omitting this temporal dimension from the study of security lists, as much of the existing literature does, means missing their key organising logic.

Third, our shift in perspective – remaining in the register of the list – draws attention to the distributed forms of agency at work in and through security lists, and how lists work to enact novel forms of ''transnational legal assemblage'' (Sullivan, 2014). When lists are understood as instruments they tend to remain tethered to the institutional actors that deploy them and the circumscribed jurisdictions they operate in. What this approach leaves out is ''the more prosaic, mundane, routine ways in which human action is moulded in the context of non-human and non-symbolic artefacts'' (Walters, 2002: 92). When analysed as devices, the interconnections, translations and transnational dynamics of lists are more readily brought to the surface. This provides a better empirical map of the fragmented forms of post-national jurisdiction that lists help to enact. Thus it becomes possible to rethink problems of accountability in relation to more dispersed forms of global security governance (Krisch, 2015: 7).

Due process litigation, for example, has proven to be a crucially important means for providing legal redress to individuals targeted by security lists. But judicial review presupposes an executive actor taking a singular decision that can be legally contested in court. Most security lists, however, operate by way of a ''diffusion of evaluative labour,'' where the predictive work of actors from a plethora of different executive agencies and institutions (e.g. police, border guards, intelligence agencies, banks, airlines) is continually intersected with variable algorithmic assessments to produce contingent knowledge about threats through processes of ''cumulative judgment'' (Bernstein, 2013: 485). Listing, in this sense, is much more than an exercise of executive power. It is also a materially heterogeneous arrangement fostering novel connections across jurisdictions and across public/private divides, as will be further explored in this paper.

Fourth, analysing the agency and liveliness of security lists has important consequences for the way that relations between lists, law and power are conceived. Law is ordinarily conceived as something normatively abstract and immaterial. In this view, security lists are relatively benign objects of legal representation, similar in style and format to Executive Regulations. As with other legal materials like documents and files, lists are effectively forced to ''remain ... below the perception threshold of the law'' (Vismann, 2008: 11). Situating the materiality of the listing process at the centre of analysis helps to bring the specific legal ordering capabilities of lists – that is, the ways they work to *constitute* law and establish new modes of legal transmission – into clearer view. It brings into better focus the (documentary) work *behind* or below formal legal decisions and contestations: the guidelines, reports and private sector standards that play an important role in effectively writing the list's criteria (also for example, Cloatre 2013).

Approaching lists as devices thus invites us to think differently about how diffuse security powers are created, expanded and sustained. It eschews rigid assumptions concerning scales of governance and levels of authority. For Latour (1986, 19–20), inscription devices enable advantage because they are characteristically mobile, immutable, flat, reproducible, multi-scalar, readily recombinable and geometrically measurable. What's important are not these particular features *per se* but rather how they are materially assembled in specific domains ''to increase either the mobility or immutability of traces'' (1986: 10). In this sense, analysing the productive work that inscription devices *do* is to ''place the practical means of achieving power'' and the ''material'' that makes macro-actors ''macro,'' at the centre of empirical enquiry (1986: 27–28). That is, the analytic of the device can help us understand how 'global' sites that make security lists are not *a priori* larger than the 'local' sites that implement them, but are made so (at least in part) by the material artefacts used and the ways these artefacts facilitate control through the ''multiple connections, groupings and hybridizations of different understandings of the world and order'' they enable (Bueger, 2015: 7 - 8). This paper hones in on consolidations and (dis)connections of security lists, in order to explore in detail their global dynamics and local appropriations.

Security lists are often thought to work through the use of ''fixed disciplinary criteria'' and ''techniques of prohibition, enclosure and stopping'', in seeming contrast to more algorithmically modulated security practices (Amoore, 2013: 89–90). But they are fast becoming more flexible knowledge technologies than their traditional appearance as binary classification mechanisms suggests. Lists and databases increasingly exist in symbiotic relation within contemporary political ecologies. ''Flat'' lists become more lively, processual and contingent as they are made interoperable with biometric data and Advanced Passenger Information (API) systems. Security lists are made able to contain ''quite heterogeneous items'' and are potentially infinite in nature (Staeheli, 2012: 234). They are capable of bringing binary logics of ''and ... and ... and'' together with

algorithmic logics of "if . . . and . . . then" in particular ensembles (Amoore, 2011, 2013). In this way, security lists function as complex amalgams by combining predictive and possibilistic knowledge techniques, diverse forms of agency and digital and analogue modes of information processing. Understanding their operation requires concrete, empirical analyses within the specific domains that lists circulate and perform their security work.

Rather than looking for political agency *behind* the list, or measuring security lists against pre-given normative standards, this paper shifts perspective and analyses lists for what they *do* rather than what they *lack* (also Johns, this issue). Focusing on key contemporary security lists, the remainder of this paper is structured around questions of criteria, consolidation and critique. First, the section on criteria shows how the work of lists consists not simply of executing decisions made through pre-defined criteria, but of writing criteria and enacting novel quasi-legal categories. Second, the section on consolidation analyses how lists intersect, translate, connect and disconnect. It is precisely through such situated (dis)connections across public/private spheres, that some of the most powerful (and disconcerting) effects of lists operate. Finally, the section on critique asks how security lists might come to be challenged in novel and productive ways.

Criteria

TSDB and the standard of derogatory information

The knowledge registers of security lists entail their own protocols for selection, nomination and inclusion. If we understand lists as security devices, it becomes clear that selection criteria do not necessarily *pre-exist* the list, and so demanding transparency concerning criteria can only partly challenge the work that lists do. As Staeheli (2012: 237) points out, lists are inherently ambivalent, and "criteria of selection are not fixed . . . but evolve during the list's use." It is clear that the evolving and flexible criteria of security lists depart from established procedures and classifications of suspicion as codified in criminal law in important ways. Pre-emptive security lists function as relatively novel forms of administrative law and pre-crime modes of targeting. Because they are deemed to be preventative rather than punitive in nature, these lists can operate outside the scope of conventional criminal justice standards and protections. Furthermore, list inclusion criteria and content are relatively malleable. There is a need to better understand the multi-sited activities of creating, expanding and regulating lists, developing protocols, discussing nominations and removing entries.

With many contemporary examples of security listing, however, these protocols and forms of designation criteria are simply not known. Here, the empirical analysis of lists as security devices becomes necessarily shrouded in the "fog of secrecy" surrounding national security issues (Best and Walters, 2013: 346). William Walters analyses the obstacles and question that arise when "actor network theory-type" research is directed at security questions: "How do we 'follow the actors' when they operate under cover of national security? How do we study public controversies when public disclosure is the exception and secrecy is the norm?" (2014: 105). For Walters, the answer lies partly in dynamics of "absent presence" and acknowledgment that "quite often an object will shape public understanding and a dynamic of a controversy not by virtue of its immediate presence . . . but through its trace, shadow, rumour or phantom" (2014: 112). But it also lies partly in the complex work of generating visibility and here the use of Freedom of Information mechanisms and leaked documentation are becoming increasingly important sources of research enquiry.

Paradoxically, UN Security Council blacklists have been the most secret kind of security list – relying as they do, on classified intelligence – *and* the most explicitly subject to political

debate and legal challenge. Debate on the quasi-regulatory effects of No-fly lists, privately compiled lists and commercial 'white lists' is just beginning. The use of various Counterterrorism watchlists and No-fly lists by the US Terrorist Screening Center (TSC) has been a rumour or "shadow" within US security debates since at least 2003, when it appeared that Senator Edward M Kennedy had been listed by mistake (Goo, 2004). Yet it is only recently that US debate on this issue has accelerated following the disclosure of detailed information about how these lists work into the public domain. When it became clear that the name of the failed 2009 "Christmas day" bomber (Umar Farouk Abdulmutallab) had been listed in the TCS database but *not* transposed onto the No-fly list, the number of US citizens on the No-fly list apparently almost doubled (Sullivan, 2012). As a consequence, in 2011, the Electronic Privacy Information Center (EPIC) filed *Freedom of Information* Act requests for disclosure of the criteria used to place individuals in the TSDB, and the criteria for transposing entries from the (broad) TSDB to the (more narrow) No-Fly or Selectee List.[1] In response, the FBI released a partial and initial cache of redacted documentation concerning their watchlisting protocols, criteria and guidelines. In July 2013, the entire 166-page *National Counter Terrorism Center Watchlisting Guidance* (NCC, 2013, hereafter, "Watchlisting Guidance") was leaked via the investigative journalism website, *The Intercept*. These leaked and redacted documents are the primary materials on which our following discussions are based.

We now know that the US TIDE, which lists 1.1 million individual names, is expanded daily and feeds the TSDB and the No-fly lists (Handeyside, 2014). It has developed elaborate protocols for nomination and inclusion (see Figure 2). The TIDE master database (tightly protected and subject to intense secrecy), managed by the little known Directorate of Terrorist Identities (DTI), is formed on the basis of national and international intelligence information from FBI, CIA and Interpol and also includes material from foreign security

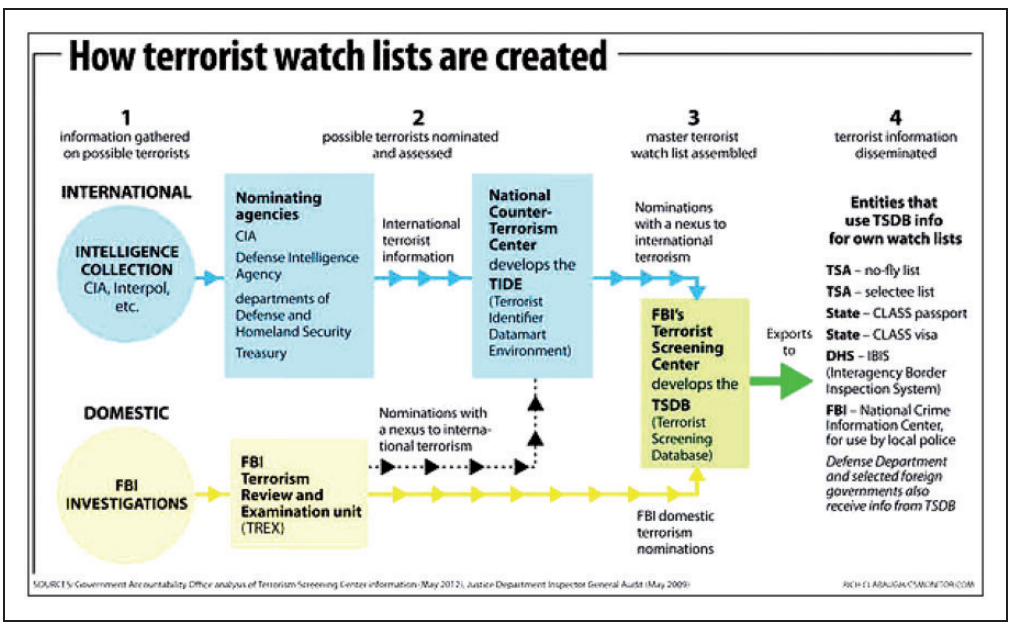


Figure 2. How watchlists are created? Available at: http://bit.ly/1ErhV4M (Reprinted with permission from Christian Science Monitor).

services and information collected by Embassies. The grounds for inclusion in TIDE include preparation of international terrorist activity, gathering information on potential targets, soliciting membership in an international terrorist organisation, or providing material support – including communications, funds or transportation – for terrorism (Government Accountability Office (GAO), 2012: 36). However, more than 40% of those are known to have "no recognised terrorist group affiliation" (Handeyside, 2014). TIDE entries are made on the basis of so-called "derogatory information". This term originates from the practice of credit scoring where it refers to credit risk information – such as foreclosures, bankruptcy and tax arrear history – that can justify the refusal of loans. It is an explicitly *risk-based* rather than strictly evidence-based category. Whilst the precise meaning of the "derogatory information" operationalized by TIDE is left unclear in the available information, it likely extends to include fragments of intelligence that suggesting a "nexus" to international terrorism (Amoore, 2011). "Christmas Day bomber" Abdulmutallab had been listed in TIDE, for example, on the basis of his alleged associations with Yemeni-based extremists (Travers, 2010). But with more than 1.1 million people listed here, compared with just over 200 individuals listed as Al Qaeda associates by the UN Security Council, it is clear that the TIDE standard of derogatory information is vastly broader and more flexible than the known or suspected associations with terrorism considered by the UN Security Council.

Because the TIDE list contains classified material from agencies such as the CIA and US military sources worldwide, it cannot be directly accessed by US border agents and other security professionals operating in the field. Yet 680,000 of TIDE records have been included in the TSDB list, managed by the FBI's Terrorist Screening Center, that is shared much more broadly with US federal agencies, law enforcement bodies, foreign governments and private security contractors. The TSDB list interconnects in turn with the No-Fly list (of individuals prohibited from flying) and Selectee List (of individuals thought to require further questioning before boarding a plane) maintained by the US Department of Homeland Security's Transportation Security Authority (TSA) (see Figure 2). These lists differ from TIDE both in size and in scope, including names and basic identifying data but not the complete record of derogatory information (Clayton, 2013; GAO, 2012). Although the No-Fly List and Selectee Lists are derivatives of the much larger TIDE database, they are said to be "unique" for applying more stringent inclusion standards, though the precise listing criteria used remains unknown.[2]

The selection of records from TIDE and TSDB for inclusion in the lists maintained by the TSA is governed by a standard of "reasonable suspicion" and must contain "particularized derogatory information" (NCC, 2013: 33; Travers, 2010). This standard is defined as:

> . . . articulable intelligence . . . which, based on the totality of the facts and taken together with rational inferences from those facts, reasonably warrants a determination that the subject is known or suspected to be . . . knowingly engaged in . . . preparation for, in aid of, or related to terrorism or terrorist activities (FBI, 2010: 3).

In other words, as revealed by the documents leaked through *The Intercept,* the novel category of "particularised derogatory information" requires factual information concerning specific behaviours and associations. But "irrefutable evidence or concrete facts are not necessary" for this reasonable suspicion standard to be met because inferences can readily be drawn "based on the totality of circumstances" (NCC, 2013: 33–34).

This determination of reasonable suspicion is partly done on the basis of open source information which is acknowledged to "involve some level of subjectivity" (GAO, 2012: 38). It can include postings on social media and other so called "write-in" information. Whilst

nominators of list entries are encouraged to record the "uncorroborated" nature of such information, it is not automatically discounted (NCC, 2013: 34). As is clear from the leaked guidance documents, the TSDB extends to include individuals deemed to be "associates or affiliates" of "known terrorists". However, the category of "known terrorists" is defined to include those on the UN Security Council's Al Qaeda sanctions list and the US Specially Designated Global Terrorist (SDGT) List. Both of these lists work pre-emptively to include those merely suspected of association with suspected members of global terrorist networks. In this way the TSDB creates its list of "known terrorists" not from those who are convicted of terrorism offences (as the name might suggest), but from disparate pool of potential suspects already enrolled into other security lists on the basis of secret, fragmentary and speculative material. Thus, the criteria applied by the TSDB translates "suspected" terrorists into "known" terrorists, widening the field of intervention to those who have repeated contact with listed individuals (including their spouses and underage children). In effect, this constitutes an additional list *below* or *around the* UN 1267 and US SDGT lists. We understand TSDB list therefore as a form of productive power that articulates novel quasi-legal targeting categories. Whilst it claims to speak in the familiar legal language of "reasonable suspicion", the particular knowledge practices it deploys redefine how such suspicion is to be generated. It functions, in short, as an inscription device rather than a mere instrument of security or law.

World-Check and the logic of infinite addition

Compared to the TIDE and TSDB lists, the protocols for inclusion into the database of financial data-provider World-Check operate both more visibly and more opaquely. World-Check relies on open source information in its subjective processes for data compilation and validation. World-Check (now part of Thompson Reuters) is a data company that collects, collates and sells listing information and due diligence compliance solutions to clients within (and beyond) the financial industries. Its main rationale is to compile into one master database the more than 400 sanctions lists, counterterrorism watchlists, regulatory and law enforcement lists in existence worldwide. In the contemporary environment, list-checking has proven to be more complicated than it sounds. As security lists have proliferated and the formal requirements for financial companies to avoid dealing with heightened-risk clients have expanded, so has the need for professional services and software packages to assist risk-mitigation and compliance with this process (Amicelle and Favarel-Garrigues, 2012; de Goede, 2012).

However, World-Check does not only compile pre-existing list entries. It also "value-adds" by adding their *own* nominations of heightened risk banking clients – including, for example, persons indicted for fraud or terrorism and persons otherwise publicly associated with, but not necessarily convicted of, such offenses. Inclusion in the World-Check database is based on open-source information research performed by multi-lingual teams around the world. In this process, web-based sources, public indictment records, newspaper articles and other publicly available information of very diverse quality – including blogs, news sites and online photographs – are reviewed for possible connections to "financial crime, narcotics trafficking, money laundering, gambling and internet fraud [and] those types of things."[3] Protocols for database inclusion are recognised to be subjective and listing categories are flexible and overlapping. In-house discussions take place on the need to include or exclude borderline cases, of for example employee fraud, from the database. World-Check, in this sense, operates at the intersection of legal requirement and commercial innovation. On the one hand, the company stresses that its inclusions are based on publicly available, legally-

obtained information that is often grounded in criminal convictions rather than gleaned from speculative entries on blacklists. On the other hand, World-Check have acknowledged that their standards for "declaring someone a high risk to engage in financial impropriety" are lower than "[those applied by] most governments" (Lichtblau, 2004) and their database is expressly marketed on the basis that it "go[es] far beyond official sources."[4]

A number of observers have emphasised that lists are "plastic, flexible" structures (Belknap, 2000: 35) that operate according to "logic[s] of possibly infinite addition" (Staeheli, 2012: 234). Security lists like TIDE and World-Check are commonly presented as a means of "targeted intervention" in an increasingly dispersed fight against terrorism. Yet it is telling that the DTI, which maintains TIDE, celebrated its one-millionth list entry (in June 2013) as a milestone in its "strategic accomplishment" report, and wrote: "While [the Directorate] seeks to create only as many person records as are necessary for our nation's counterterrorism mission, this number is a testament to DTFs hard work and dedication over the past 2.5 years" (DTI, 2013). Even more so than TIDE, the operative logic of World-Check is one of infinite addition. In 2009 the World-Check database included 1.2 million records, and it is updated daily. The company does not foresee a need for formal delisting procedures but may, on the basis of individual requests, engage in an in-house, subjective discussion on possible entry removal.

As these examples show, the knowledge registers of security lists work through suspicion, pre-emption and association. Both the TSDB list and the World-Check database are means of rendering intelligence actionable. It is unsurprising that criteria and standards applied in this domain have been a consistent focus of critiques and legal challenges to security listing regimes. Fundamental rights and due process litigation has certainly opened up discursive cracks and fissures where the legitimacy of listing measures have been subjected to judicial and political scrutiny. At the same time, however, such legal challenges have themselves played a productive role in generating new quasi-legal standards and criteria for security listing. Take the curious genre of the "Narrative Summary of Reasons for Listing" that the UN 1267 Sanctions Committee have released since 2009 concerning individuals included on the Al Qaida targeted sanctions list (example shown in Figure 3). This novel criterion emerged as a direct response to EU legal challenges against this list and the absence of accusatory information being made available to those targeted. Pressed to render their procedure more transparent, but reluctant to divulge classified intelligence, the genre of "narrative summaries" was invented and rendered public for each list entry. This record includes a short narrative statement concerning the date of listing, the groups that the individual is thought to be associated with, their alleged but usually unspecified terrorist activity, and their criminal convictions, if they have any. The point here is not to debate the question of whether this procedural innovation sufficiently addresses the critique of the UN listing process, but to show how processes of critique and litigation play an important role in procedurally advancing the particular knowledge regimes of security listing. Put differently: whilst legal challenges can certainly provide much-needed redress to targeted individuals, they can carve out new procedures that neither overturn pre-emption nor leave it intact, thus fortifying the broader security work that listing devices perform (see also Sullivan and de Goede, 2013).

Consolidation: "Lists Come Alive"

Our examples of the operation of TIDE and World-Check show not only how listing standards are flexible and evolving, but they also show that different security lists intersect,

Figure 3. Narrative summary of reasons for listing, UN1267 Sanctions Committee. Available at: http://bit.ly/1MrDeLm. (© (2015) United Nations. Reprinted with permission from the United Nations).

feed into each other, become consolidated, disseminated, stretched and translated. The TIDE master database, for example, feeds the TSDB list, from which the No-Fly and Selectee Lists are drawn. TIDE list entries are also supplemented with biometric identifying information obtained by the DTI's Biometric Analysis Branch and drawn largely from drivers' licenses maintained by US state motor vehicular departments. In a different process, (inter)national blacklists, including UN targeted sanctions lists, feed the databases of World-Check, and become intermingled with other records including ledgers of Politically Exposed Persons and heightened risk banking clients. In this process, the narrative summaries of suspected al-Qaida operatives from around the world become intermingled and, to some extent, homogenised with local drug dealers and individuals convicted of fraud offences. Whilst about 10–20% of World-Check's records are based on formal security lists, for example, the remaining 80% is drawn from court records and other open-source information.[5]

These examples suggest that we need to be attentive to the ways in which lists intersect and interconnect; how they are moved, transcribed and consolidated, or, in important cases, *dis*connected (Opitz and Tellmann, 2012). With each of these moves, a translation takes place. Moving records from one list/database to another – for example, from the UN Al Qaeda list to the World-Check database – does not just change the "context" in which the information is used. It changes the information itself: its technical appearance, the meaning it is inscribed with, the elements it is associated with, and the effects it is able to have. Translation, in this sense, is a "form of modification" (Barry, 2013: 414). The case of would-be bomber Abdulmutallab reveals some of the complexities of list's disconnections and (failed) translations. Abdulmutallab's name was included in TIDE after his father reported suspicions of his associations with Yemeni terrorists to the US embassy in Abuja, Nigeria. However, this list entry was *not* transposed to the TSDB because "the associated derogatory information" of Abdulmutallab's record was not deemed sufficient or "particularized" enough to meet the "reasonable suspicion" standards of the No-Fly list (GAO, 2012: 9; Travers, 201). As a consequence, Abdulmutallab's name was not transposed to the No-Fly list, and was able to board a US-bound plane without problems.

The importance of processes of list translation, interconnection and (dis)connection can be illustrated with other recent examples. In 2010 the Security Council appointed an Ombudsperson to receive delisting requests from individuals and groups targeted by sanctions against Al Qaeda and make recommendations about whether they should remain on, or be removed from, the targeting list. Between 2010 and July 2014, 34 individuals and 27 entities have successfully petitioned for delisting on recommendation of the Ombudsperson.[6] However, these delisting decisions are not automatically taken into account by World-Check, nor would they be regarded as a reason for removal from their database. A delisted individual formerly associated with terrorism would still be considered a "heightened risk" banking client, – as company representatives have put it.[7] As a consequence, hard-won UN delisting proceedings are only partially able to restore an individual's life to normality. As long as their record remains on World-Check and/or they remain targeted by the US terrorism lists, former suspects will continue having difficulty opening bank accounts, transferring money, acquiring loans and travelling freely without interrogation. Once enlisted, it is extraordinarily difficult to become delisted, due to the fragmented and interconnected nature of the global security list environment.

Rahinah Ibrahim's case further exemplifies the problems and power at work through lists' partial disconnections/connections. Ibrahim, a Malaysian national and former Stanford University architecture student, was the first person to successfully challenge inclusion on the US No-Fly list in January 2014, after more than eight years of protracted litigation. During trial it emerged that the FBI listed Ibrahim as a result of human error and that the US government did not actually consider her a security threat. After succeeding in court and finally being removed from the No-Fly list, Ms Ibrahim attempted to return the US but was still unable to travel. Her US student visa had been revoked due to inclusion in another security list – the Consular Lookout and Support System (CLASS), maintained by the US State Department – on the grounds that she was suspected terrorist. As it turned out, this CLASS listing had been made on the basis of the original and erroneous No-Fly list entry, since discredited and overturned by the court. Whilst US intelligence and law enforcement agencies can populate the CLASS database with derogatory information, only US State Department officials can remove it. And when list entries are moved from the No-Fly list to the CLASS list, all of the (potentially sensitive) substance is removed to leave only stripped-back, basic identifying information (e.g. name) and numerical visa refusal class (e.g. "212(a) (3)(B): terrorist activities" or "212(f): Individual who is detrimental to US

interests'').[8] That is, in moving an entry from one list to another a certain translation, and novel means of exclusion, is effected. Despite being cleared from the No-Fly list, Ibrahim is nonetheless still prevented from travelling to the US and her attempt to challenge the government's refusal of visa have been dismissed by the courts.

The political geometry of the list, here, is neither global nor local, but rather something that effects novel reconnections between local professional practices – including local police and private banking – and forms of global organization. For Staeheli, the list is a ''technique of the global''. It does not simply ''[channel] and [control] global flows of communication'' but has the capacity to ''do the global'' by homogenizing across local particularities (Staeheli, 2012: 233–234; also this issue). Lists like the TSDB are national in appearance, but apply extraterritorially. They seek to standardise bureaucratic practices whilst opening up new domains, problems and grounds for further list intervention. In the case of the No-fly lists, for example, the US NCC prescribes particular ''Encounter Management Actions'' for homeland security personnel, border agency workers and local police who ''encounter known or suspected terrorists'' in their daily routines (NCC, 2013: 69). Noting clearly that list placement ''is not a legal basis to detain'' (2013: 60), the Guidance encourages security professionals to use encounters to generate ''additional or new information'' about suspects. The Guidance specifies a plethora of different types of potentially valuable security information that might be acquired through encounters – including ''Resumes; Conference Literature; Telephone data; Biometrics; Prior travel; Financial information.including bank statements, salary slips; Photos [and] Email addresses'' (NCC, 2013: 74–76). In this way, the List Guidance aims to standardise local encounters across time and space, whilst feeding further information into the list that may otherwise not be legally obtainable, and that may end up producing new networks of association for targeting.

In this sense, it is helpful to understand the list as a ''boundary object'' as discussed by Bowker and Star (see also Leander, in this issue). For Bowker and Star (1999: 139), lists are an ''attempt at universal standardization,'' cutting across time and space and seeking to standardize bureaucratic functions. Yet the standardizing ambitions of lists exist in ''permanent tension'' with ''the local circumstances of those using them'' (Bowker and Star, 1999: 139). Lists are boundary objects that navigate between the local and the global, and that enact the connections between them. ''Boundary objects are both plastic enough to adapt to local needs ... yet robust enough to maintain a common identity across sites'' (1999: 297). The boundary work of security listing traverses not only global and local scales but also public and private settings. Public security lists become reconfigured into private, commercial applications that ultimately assist mid-level banking bureaucrats in relation to transactions monitoring and asset-freezing decisions. The list's technological appearance and commercial value change from being a publicly accessible (yet cumbersome) online dataset, to becoming a privately-owned, highly commercialized and largely invisible pool of names. Annual subscriptions to World-Check's databases, for example, can cost up to €1 million. The way in which lists cut across public/private space is not just a matter of *enlisting* private actors in the fight against terror. It also entails an authorization of private participants to make security decisions and become ''petty sovereigns'' (Butler, 2004), rendering the global listing field both more diffuse and heterogeneous as a result.

As our examples show, the new political geometry of lists is not unidirectional nor does it always foster *connections*. Some of the most powerful effects of security lists operate not through global connectivity, but through disjunctures and *disconnections* – as when a hard-won UN delisting does not affect the World-Check database, or when Ibrahim's victory in a

US lawsuit turns out to be insufficient to re-enter the country. Translating public lists into private database entries "distances the subject from legal centres" (Opitz and Tellmann, 2012: 274). It makes the issue of redress for targeted individuals more complex because there is no forum where a World-Check listing decision can be formally contested. The collateral realities of lists-as-devices, then, include the fostering of novel global security patterns, including forms of cooperation and disjunction (Law and Ruppert, 2013: 232).

Matters of critique

Much of the work of security lists, as suggested in this paper, is performed through differentiation, interconnection, translation and the production of globally fragmented jurisdictions. Following Fleur Johns, we have argued that it is at best, "tethered here and there, to defined legal ground" (Johns, 2013: 2).

Whilst conventional forms of legal challenge can certainly provide listed individuals with redress, it is ill equipped to challenge the distributed processes of cumulative judgment made possible through security listing dynamics. For example, recent litigation brought by the ACLU obtained a modicum of due process protections for citizens and permanent residents on the US No-Fly list.[9] Yet 95% of those listed in the TSDB database (from which the No-Fly list derives) are foreign nationals who fall outside the scope of the US constitutional framework altogether (Pincus, 2009). Despite limited judicial victories, most targets of US counterterrorism lists still have no real possibility for legal redress. This kind of asymmetry between the global connectivities of security lists and the processes of legal accountability that remain tied to traditional jurisdictions is, of course, not specific to the technology of the list. When power and authority are diffused across post-national space, "judicial review often suffer[s] from the lack of a suitable target: when there is no one point of decision-making, but instead a continuous social process in which standards are made and remade by different actors, [it]... often fail[s] to produce relevant effects" (Krisch, 2015: 16).

How, then, might issues of critique and accountability be productively reposed in relation to the dispersed security listing arrangements we have outlined? What can examining lists-as-devices help bring to the ways political problems are framed and addressed? For us, the perspective of the list-as-device is not just a way of rendering visible what security lists do – politically and juridically, in terms of drawing together items and working across jurisdictions. Rendering visible the distributed agency at work through lists is also important because it broadens the scope of what and where we understand the political to be (Braun and Whatmore, 2010; Latour and Weibel, 2005: 15). We seek to enable a 'diffraction' of security lists, an "interference" that repoliticises them (Law and Ruppert, 2013: 235, drawing on Haraway). Such an interference proceeds not only by denouncing normative errors (that is, by identifying what lists *lack* in relation to existing legal standards) but also by exposing what they *produce,* "bring[ing] to light the conditions that ha[ve] to be met" for listing arrangements "to be made possible" (Foucault, 2008: 36). In closing, we highlight two avenues for repoliticizing security lists, in an attempt to move outside the strict parameters of existing juridical contestations, whilst acknowledging their continued importance.

First, thinking how lists might be made *otherwise* "requires understanding what existing technical knowledge does, what it achieves and what latent possibilities it might hold" (Riles, 2011: 224). A first diffraction of security lists entails reopening the domain of technical expertise to critical political scrutiny. The list is an incessantly depoliticising technology of government as Anna Leander's paper in this issue also reminds us. Its boundary work is vitally important precisely because it is here that the operation of listing is rendered into a

'technical' problem, rather than a political one (Aalberts and Leander, 2013). Once listing problems are made technical, they elevate relevant security expertise around questions of practical implementation, effective calibration and practical interoperability. Technicality does not so much dissolve political questions (for example, how suspects are targeted pre-emptively through exceptional listing mechanisms), however, it buries such questions within registers of expertise. The use of force to counter global security threats is always subject to vociferous debate, for example, because going to war (or not) is understood as a necessarily political question. Yet debates around security lists (if there are any) concern technical, expert-led issues about who to target and how to ensure lists are properly implemented to maximize their intended effects. Here, the form of the list makes a difference, by helping to fold political questions of pre-emptive warfare back into less contentious, technical questions of expert administration. To analyse lists-as-devices, then, is to start disentangling such processes and revaluing the technicalities of the list for the profoundly political practices that they are.

A second avenue for critique opened up through diffracting the list, draws attention to its inherently speculative and unstable nature. As we have argued, lists have the capacity to arrange disparate items into a coherent semantic field, rendering them presentable as a particular kind of objective order. This objectivity function can, in turn, further serve to stretch and extend the list's specific depoliticizing qualities. Take the UN1267 targeted sanctions list, for example, which presents the individuals it targets as 'known' members or associates of A1 Qaeda, operationally connected with other terrorists designated as list entries. What eludes this formatting is the fact that many of those listed are not so much known terrorists, but rather individual suspects pre-emptively targeted, usually on the basis of unseen intelligence material, for potential terrorist association. The contingencies and uncertainties underpinning individual listing decisions based on speculative security grounds (de Goede, 2012), however, are removed from the equation when formatted in the medium of a list. In this way, global lists function in a comparable manner to global indicators, enabling ''outcomes [to] appear as forms of knowledge rather than particular representations of a methodology and particular political decisions about what to measure and what to call it'' (Merry, 2011: S88).

Whilst both security listing and data profiling are practices grounded in speculative logics and processes, profiling is criticized for being discriminatory and conjectural but listing is ordinarily not. The difference lies in the fact that they format their suspicions differently. Because lists repose their speculative assessments as seemingly stable knowledge claims, they avoid the political controversies that constrain the spread of other pre-emptive security technologies, like profiling. Whilst security datamining is regularly challenged for breaching the rights of privacy and non-discrimination, such challenges are much harder to direct toward the list, whose objectively formatted suspicion seems to relieve its targets of their rights.

The speculative knowledge claims of security listing can be rendered visible and challenged with the help of Bowker and Star's concept of 'torque,' which denotes the tension between classification and *life*. Torque does not just signal to the fact that lived life always exceeds the boundaries of classification, but also to the complicated ''trajectories [and]... threads'' that tie people to categories to insitutions (Bowker and Star, 1999: 195). There are multiple ''tensions and twists'' in the alignment between body and classification, as they are mediated through institutions and expertise. Rendering visible the contested trajectories and personalised micro-stories of how suspects become listed and how tenuous the connections are between individual lives and listing orders is one way of questioning and critiquing the list's blunt homogenisations.

We conclude by offering two brief examples of torque, illustrating how lived life can be rendered visible again *contra* the abstracted and depoliticised form of the list. These examples help show how the abstraction and disruption that security lists effect might be otherwise contested. When Abousfian Abdelrazik was placed on the UN1267 targeted sanctions list by the US government in 2006, he was left unable to travel from Sudan back to his home in Canada. After his passport expired and the Canadian government refused to issue him with further travel documents, Abdelrazik was effectively made subject to political exile. To counter this travel ban, and in direct defiance of the laws prohibiting association with, and support of, listed persons, more than 100 people – including former government officials and university professors – made donations to help purchase a return flight to Canada. After Abdelrazik was finally allowed to return on order from the Canadian Federal Court, a coalition of Canadian trade unions publicly announced that they would each be hiring Abdelrazik "to document his story, so that other Canadians can be made aware of the impact of the security agenda on innocent people" (People's Commission Network, 2010). Such a simple act of defiance (providing financial support and lending political support) is made powerful here not only because it provides those listed with a chance to represent their story. It is also a representational act that makes visible the severe coercive effects of this list whilst at the same time openly confronting its disruptive rationale by "associating with" the enlistedand effecting a "strategy of rupture" (Christodoulidis, 2009).

The New World Summit, a Dutch art organisation led by Jonas Staal, similarly tries to challenge the boundaries of association drawn by security listing practices. The summit was first organised during the Berlin Biennale of 2012 as an 'alternative parliament' to give voice and visibility to those excluded by being designated on international terrorism lists. It brought

Figure 4. Jonas Staal, Design of the parliament of the first New World Summit, Berlin, surrounded by flags of organizations currently dealing with terrorist blacklisting. In collaboration with Paul Kuipers (Event-Architecture). Reprinted with permission of Jonas Staal.

representatives from listed groups and the lawyers of those targeted together with academics and artists, to interrogate logics of listing and offer a ''platform for the shadow side'' of the current security system (Staal, 2012: 26). The staging, design and publications accompanying this summit give visibility to the banned icons and symbols of listed organisations (Figure 4) and aim to create an archive of the very diverse histories, aims and symbols of blacklisted organisations (Staal, 2012). The project is designed to operate at the limit of laws prohibiting support to listed groups and individuals and, in so doing, make those laws visible as something politically contingent and contestable. Most importantly, however, it provides immanent terrain for the enlisted to connect and think through their co-placement on security lists together and how their list-borne association might be repurposed otherwise.

Concluding remarks

Framing security lists as inscription devices helps turn attention towards the collateral realities and diffuse material conditions through which lists are produced, sustained, interconnected and transformed. Nonhuman materials like lists are usually excluded as irrelevant in political and legal thinking by being relegated ''to the status of resources or tools'' (Braun and Whatmore, 2010: xv). By bringing renewed focus to the material conditions through which lists are produced the idea of the device brings nonhuman agency or 'liveliness' back in, urging us to think carefully about how listing technologies make a difference in, or are *constitutive* of, particular security arrangements. For Law (2012), collateral realities differ from 'collateral damage' because they are not to be understood as unintended side-effects but as integral to the practice. We have shown how lists have the capacity to enact their own criteria. We have analysed the fragmented space of global list disconnectivities/connectivities as a collateral reality with powerful effects on individual lives.

Our approach is intended to help facilitate critical approaches to law grounded in ''the agency of technocratic legal form,'' and imagine multidirectional, rather than unidirectional, processes of legal change (Riles, 2005–2006, 980). This can help us better understand how legal measures introduced in response to a given problem are made expansive and mobile to annex an increasing number of other problem areas without need for further recourse to formal legal or political decision-making processes. This paper, and the special issue of which it is part, is intended as a first step in 'diffracting' security lists, and questioning them differently.

Authors' note

Earlier versions of the paper were presented to workshops within the COST Action IS1003, 'International Law between Constitutionalization and Fragmentation', the Law and Society Association (LSA) conference in Minneapolis in 2014, the European International Studies Association (EISA) meeting in Izmir in 2014, at Kent Law School in February 2014, and at the School of Global Studies in Gothenburg in January 2015, where it received many helpful comments from colleagues.

Acknowledgements

The authors would like to express their thanks to the editors of Society & Space, and to three anonymous reviewers who offered very helpful comments on an earlier draft of this paper.

Declaration of conflicting interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Dutch Council for Scientific Research (NWO), through the VIDI-grant European Security Culture, award number 452-09-016.

Notes

1. Request available at: http://epic.org/privacy/airtravel/EPIC_No_Fly_List_Criteria_FOIA_Request.pdf
2. http://www.oig.dhs.gov/assets/Mgmt/OIGr_09-64_Jul09.pdf (at 9).
3. Interview with representatives of World-Check, London, 18 March 2010.
4. See: http://accelus.thomsonreuters.com/products/world-check
5. Interview with representatives of World-Check, London, 18 March 2010.
6. http://www.un.org/ga/search/view_doc.asp?symbol=S/2014/553, p. 1
7. Interview with representatives of World-Check, London, 18 March 2010.
8. s. 212, Immigration and Nationality Act (INA). See: http://travel.state.gov/content/visas/english/general/ineligibilities.html
9. *Latif v Holder et al* (Case 3:10-cv-00750-BR)

References

Aalberts T and Leander A (2013) Introduction: The Co-Constitution of Legal Expertise and International Security. *Leiden Journal of International Law* 26(4): 783–792.

American Civil Liberties Union (ACLU) (2006) Available at: https://www.aclu.org/national-security/aclu-calls-overhaul-aviation-watch-lists-wake-60-minutes-report (last accessed 12 August 2015).

Amicelle A and Favarel-Garrigues G (2012) Financial surveillance: who cares?. *Journal of Cultural Economy* 5(1): 105–124.

Amicelle A, Aradau C and Jeandesboz J (2015) Questioning security devices: Performativity, resistance, politics. *Security Dialogue* 46(4): 293–306.

Amoore L (2011) Data derivatives: On the emergence of a security risk calculus of our times. *Theory, Culture and Society* 28(6): 24–43.

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC: Duke University Press.

Amoore L (2014) Security and the claim to privacy. *International Political Sociology* 8(1): 108–112.

Aradau C and van Munster R (2011) *Politics of Catastrophe: Genealogies of the Unknown*. London: Routledge.

Barry A (2013) The translation zone: Between actor-network theory and international relations. *Millennium* 41(3): 413–429.

Becker J and Shane S (2012) Secret 'kill list' proves a test of Obama's principles and will. *The New York Times* 29: A1.

Belknap R (2000) The literary list: A survey of its uses and deployments. *Literary Imagination* 2(1): 35–54.

Bellanova R and González Fuster G (2013) Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices. *International Political Sociology* 7(2): 188–209.

Bennett CJ (2008) Unsafe at any altitude: The comparative politics of no-fly lists. In: Salter M (ed.) *Politics at the Airport*. Minneapolis: University of Minnesota Press.

Bernstein A (2013) The hidden costs of terrorist watch lists. *Buffalo Law Review* 61(3): 461–535.

Best J and Walters W (eds) (2013) Forum: Actor-network theory and international relationality. *International Political Sociology* 7(3): 332–349.

Biersteker, TJ and SE Eckert (eds) (2007) *Countering the Financing of Terrorism*. London: Routledge.

Blakely R (2007) Why torture?. *Review of International Studies* 33(3): 373–394.

Bowker GC and Star SL (1999) *Sorting Things Out: Classification and Its Consequences*. Cambridge: The MIT Press.

Braun B and Whatmore S (2010) The stuff of politics: An introduction. In: Braun and Whatmore (eds) *Political Matter: Technoscience, Democracy, and Public Life*. Minneapolis: University of Minnesota Press.

Bueger, C (2015) Making Things Known: Epistemic Practices, the United Nations, and the Translation of Piracy. *International Political Sociology* 9(1): 1–18.

Butler J (2004) *Precarious Life: The Powers of Mourning and Violence*. London: Verso.

Christodoulidis E (2009) Strategies of rupture. *Law and Critique* 20(1): 3–26.

Clayton M (2013) Terrorist watch lists: Are they working as they should? *Christian Science Monitor* 22 May.

Cloatre E (2013) *Pills for the Poorest: An Exploration of TRIPS and Access to Medication in sub-Saharan Africa*. London: Palgrave MacMillan.

de Búrca G (2010) European court of justice and the international legal order after Kadi. *Harvard International Law Journal* 51(1): 1–49.

de Goede M (2011) Blacklisting and the ban: Contesting targeted sanctions in Europe. *Security Dialogue* 42(6): 499–515.

de Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press.

Directorate of Terrorist Identities (DTI) (2013) Strategic accomplishments, August 5 2014. *The Intercept*. Available at: https://firstlook.org/theintercept/document/2014/08/05/directorate-terrorist-identities-dti-strategic-accomplishments-2013/

Ertuk I, Froud J, Johal S, et al. (2013) (How) do devices matter in finance?. *Journal of Cultural Economy* 6(3): 336–352.

Espeland WN and Stevens ML (2008) A sociology of quantification. *European Journal of Sociology* 49(3): 401–436.

Federal Bureau of Investigation (FBI) (2010) *Counterterrorism Program Guidance: Watchlisting*. December 2010.

Foster LA (2014) Critical cultural translation: A socio-legal framework for regulatory orders. *Indiana Journal of Global Legal Studies* 21(1): 79–105.

Foucault M (2008) *The Birth of Biopolitics: Lectures at the College de France*. London: Palgrave Macmillan.

Giumelli F (2011) *Coercing, constraining and signalling: explaining UN and EU sanctions after the Cold War*. Colchester: ECPR Press.

Government Accountability Office (GAO) (2012) *Terrorist Watchlist: Routinely Assessing Impacts of Agency Actions since to December 25, 2009, Attempted Attack Could Help Inform Future Efforts*. Report to Congress, Washington, May.

Goo SK (2004) Faulty 'No Fly' system detailed. *Washington Post* A01.

Goody J (1977) *The Domestication of the Savage Mind*. Cambridge: Cambridge University Press.

Handeyside H (2014) Numbers tell the story of our government's watchlisting binge. *ACLU Blog of Rights* 6 August.

Isiksel NT (2010) Fundamental rights in the EU after Kadi and Al Barakaat. *European Law Journal* 16(5): 551–577.

Johns F (2013) *Non-legality in international law: unruly law*. Cambridge University Press: Cambridge.

Krassman S (2012) Law's knowledge. On the susceptibility and resistance of legal practices to security matters. *Theoretical Criminology* 16(4): 379–394.

Krisch N (2015) The structure of postnational authority. SSRN 2564579.

Latour B (1986) Visualization and cognition: Drawing things together. *Knowledge and Society* 6: 1–40.

Latour B and Woolgar S (1986) *Laboratory Life: The Construction of Scientific Facts*. Princeton: Princeton University Press.

Latour B and P Weibel (eds) (2005) *Making Things Public: Atmospheres of Democracy*. Cambridge MS: MIT Press.

Law J, 2012, "Collateral Realities", in *The Politics of Knowledge* Eds F Domínguez Rubio, P Baert (London: Routledge) pp. 156–178.
Law J and Mol A (eds) (2002) Complexities: An introduction. In: Law J and Mol A (eds) *Complexities: Social Studies of Knowledge Practices*. Durham: Duke University Press.
Law J and Ruppert E (2013) The social life of methods: Devices. *Journal of Cultural Economy* 6(3): 229–240.
Leese M (2014) The new profiling. *Security Dialogue* 45(5): 494–511.
Leyshon A and Thrift N (1999) "Lists come alive": Electronic systems of knowledge and the rise of credit scoring in retail banking. *Economy and Society* 28(3): 434–466.
Lichtblau E (2004) Homeland Security Department experiments with new tool to track financial crime. *New York Times* 12.
Merry SE (2011) Measuring the world: Indicators, Human Rights, and Global Governance. *Current Anthropology* 52.S3: S83–S95.
National Counterterrorism Center (NCC) (2013) *Watchlisting Guidance*. March 2013.
Opitz S and Tellmann U (2012) Global territories: Zones of economic and legal dis/connectivity. *Distinktion* 13(3): 261–282.
Pincus W (2009) 1600 are suggested daily for FBI's list. *The Washington Post* 1.
People's Commission Network (2010) "Supporting Abdelrazik, Striking Down the '1267 List'". *Pacific Free Press*19 May. Available at: http://www.pacificfreepress.com/rss/6234-supportingabdelrazik-striking-down-the-1267-list.html.
Riles, A. (2005–2006) A new agenda for the cultural study of law: Taking on the technicalities. *Buffalo Law Review* 53: 973–1033.
Riles A (2011) *Collateral Knowledge: Legal Reasoning in the Global Financial Markets*. London: University of Chicago Press.
Scahill J and Greenwald G (2014) The NSA's secret role in the US assassination program. *The Intercept* 10.
Staal J (2012) Art in defense of democracy. In: *New World Summit*, Museum De Lakenhal.
Staeheli U (2012) Listing the global: dis/connectivity beyond representation?. *Distinktion: Scandinavian Journal of Social Theory* 13(3): 233–246.
Sullivan E (2012) No-fly list of suspected terrorists more than doubled in the past year. *Huffington Post*. 2 February. Available at: http://www.huffingtonpost.com/2012/02/02/no-fly-listdoubles_n_1249014.html (last accessed 12 August 2015).
Sullivan G (2014) Transnational legal assemblages and global security law: topologies and temporalities of the list. *Transnational Legal Theory* 5(1): 81–127.
Sullivan G and Hayes B (2011) *Blacklisted: Targeted Sanctions, Preemptive Security and Fundamental Rights*. Berlin: ECCHR.
Travers R (2010) "Statement for the Record of Mr. Russell Travers," before the US House of Representatives Hearing on *Sharing and Analyzing Information to Prevent Terrorism*, Washington, 24 March.
Vismann C (2008) *Files: Law and Media Technology*. Stanford: Stanford University Press.
Walters W (2002) The power of inscription: Beyond social construction and deconstruction in European integration studies. *Millennium* 31(1): 83–108.
Walters W (2014) Drone Strikes, Dingpolitik and beyond: Furthering the debate on materiality and security. *Security Dialogue* 45(2): 101–118.
Zedner L (2007) Pre-crime and post-criminology? *Theoretical Criminology* 11(2): 261–281.

Marieke de Goede is professor of political science at the University of Amsterdam. She has published widely on the intersection between finance and security. She is author of Speculative Security: the Politics of Pursuing Terrorist Monies (2012) and Virtue, Fortune

and Faith: A Genealogy of Finance (2005). De Goede is Associate Editor of Security Dialogue (e-mail: m.degoede@uva.nl).

Gavin Sullivan is a solicitor and Lecturer in Law at the University of Kent. His research and practice focuses on counterterrorism, peacebuilding, human rights and the politics of global security law. He is the coordinator of the Transnational Listing Project – a global law clinic providing representation to people targeted by different security lists around the world – and is an editor of the journal Transnational Legal Theory (e-mail: g.sullivan@kent.ac.uk).