The algorithmic regulation of security: An infrastructural perspective

Bellanova, R.; de Goede, M.

DOI
10.1111/rego.12338

Publication date
2022

Document Version
Final published version

Published in
Regulation & Governance

License
CC BY-NC

Link to publication

Citation for published version (APA):
Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, *16*(1), 102-118. https://doi.org/10.1111/rego.12338

Regulation & Governance

Regulation & Governance (2022) 16, 102–118 doi:10.1111/rego.12338

The algorithmic regulation of security: An infrastructural perspective

Rocco Bellanova and Marieke de Goede

Department of Political Science, University of Amsterdam (UvA), Amsterdam, The Netherlands

Abstract

This article contributes to debates on algorithmic regulation by focusing on the domain of security. It develops an *infrastructural* perspective, by analyzing how algorithmic regulation is enacted through the custom-built transatlantic data infrastructures of the EU-U.S. Passenger Name Records and Terrorism Financing Tracking Program programs. Concerning regulation *through* algorithms, this approach analyzes how specific, commercial data are rendered transferable and meaningful in a security context. Concerning the regulation *of* algorithms, an infrastructural perspective examines how public values like privacy and accountability are built into international data infrastructures. The creation of data infrastructures affects existing modes of governance and fosters novel power relations among public and private actors. We highlight *emergent* modes of standard setting, thus enriching Yeung's (2018) taxonomy, and question the practical effects of operationalizing public values through infrastructural choices. Ultimately, the article offers a critical reading of algorithmic security, and how it materially, legally, and politically supports specific ways of doing security.

Keywords: algorithmic regulation, data, infrastructure, PNR, security, TFTP.

1. Introduction: Algorithmic security

Contemporary security policies and practices are increasingly data-driven and thus provide an important domain for what Yeung (2018) has called "algorithmic regulation" (also Hildebrandt 2018; Johns 2016). For example, since 2001, the United States' (U.S.) Treasury and CIA have captured and analyzed financial transactions data from the Society of Worldwide Interbank Transfer (SWIFT) as part of the Terrorism Financing Tracking Program (TFTP), which aims to map terrorist networks and generate police leads. By comparison, border policing uses airline passenger data (Passenger Name Records [PNR] data), to analyze, predict, and pre-empt "suspicious" passengers before they present themselves at a physical border.1 These programs rely on large amounts of digital data and computing power to govern populations through algorithmic analyses. They process information extracted from multiple – often commercial – databases, to inform security decisions in a endless cybernetic-like loop of data extraction, knowledge generation, and regulation. These algorithmic security systems eventually provide actionable knowledge to law enforcement and border officials, enabling preemptive decisions to stop, deter, freeze, or detain (Yeung 2018, p. 509; Amoore & de Goede 2008).

Security programs such as the ones based on PNR and SWIFT data entail practices and challenges of algorithmic regulation in a dual sense – they are both a "tool" and a "target" of regulation (Brownsword & Yeung 2008). On the one hand, they are a *tool* of algorithmic regulation – they govern contemporary populations through "algorithmic decision making," as they "track and intervene in the behaviour of … an entire population" (Yeung 2018, p. 509). They do so by redeploying commercial datasets for security purposes, with the aim of algorithmically identifying unknown suspects and emerging threats. Thus, they constitute important examples of the regulation of populations *through* algorithms, whereby algorithms are a tool. On the other hand, these programs are themselves a *target* of novel forms of algorithmic regulation. Socio-legal features that regulate and condition these security programs – including limitations concerning system access and privacy safeguards – have become built into their architectures. Interfaces, especially software systems, regulate who can access and share specific

Correspondence: Rocco Bellanova and Marieke de Goede, Department of Political Science, University of Amsterdam (UvA), Nieuwe Achtergracht 166, 1018WV Amsterdam, The Netherlands. Email: r.bellanova@uva.nl; m.degoede@uva.nl

Accepted for publication 9 June 2020.

datasets, and under what conditions. Thus, these security programs are important examples of novel types of regulation *of* algorithms, whereby algorithms are a *target* of regulation.

This article explores the dual nature of algorithmic regulation as a tool and a target in data-led security programs. It contributes to the debate on algorithmic regulation by focusing on the domain of security, and by fostering a dialogue with the rich literature that has critically analyzed security algorithms (Amoore 2011; Jacobsen 2015; Amoore & Raley 2017; Wilcox 2017; Aradau & Blanke 2018). In particular, we focus on algorithmic regulation *through* and *of* security systems that use commercial passenger and financial data to enable *possibilistic* transatlantic security decisions, based on anticipatory assessments of transactional behavior (Amoore 2013). Our empirical focus is on two major transatlantic security programs – the EU-U.S. PNR system and the EU-U.S. TFTP program. Public authorities from the United States, several European countries and others including Canada and Australia have deployed multiple algorithmic security programs with a global ambition and an appetite for commercial data (Bauman *et al.* 2014). Yet, the PNR and TFTP systems stand out because, contrary to other international mass-surveillance initiatives (for example those of the so-called Five Eyes, cf. Bigo 2019), authorities on both sides of the Atlantic have progressively institutionalized PNR and TFTP infrastructures by making them publicly accountable and seemingly privacy-friendly. Political authorities consider them part of an acceptable repertoire of data-driven security tools, if not examples of a good governance of algorithmic security (Clarke *et al.* 2013). While the political and legal negotiations surrounding these programs have been well documented (Papakonstantinou & De Hert 2009; Mitsilegas 2014), little is known about their algorithmic regulation in the dual sense outlined above. Conversely, the literature on algorithmic regulation has yet to focus on the specific domain of security, and to fully connect to the considerable academic literature that critically analyzes security algorithms (but see Ulbricht 2018).

Specifically, this article develops an *infrastructural* perspective on algorithmic regulation. It analyzes how regulation through and of algorithms in the domain of security is enacted through custom-built transatlantic data infrastructures. The infrastructural approach to algorithmic regulation contributes to debates by focusing attention on the architectures of data analysis and data transfer, thus unpacking how seemingly technical solutions make algorithmic regulation possible across national, organizational, and legal boundaries. Infrastructures are not neutral vehicles for the enactment of regulation, but play an important role in shaping and enabling particular regulatory actions and functions. Concerning regulation *through* algorithms, for example, this approach raises questions concerning the "production of data points" (Eyert *et al.* 2022, p. 14), and how specific, commercial data are rendered transferable and meaningful in a security context. How are commercial datasets carved off and rendered mobile? How is the mass of unwieldy data points ordered into a neat transatlantic flow? Concerning the regulation *of* algorithms on the other hand, an infrastructural approach examines how public values like privacy and accountability are built into transatlantic data infrastructures in specific ways. These programs entail specific operationalizations of values that are inscribed into security infrastructures as "architectural constraints" (Eyert *et al.* 2022, p. 24; Berlin Script Collective 2017).

Ultimately, this article offers a critical reading of algorithmic security, and how it materially, legally, and politically supports specific ways of doing security. We demonstrate how transatlantic data infrastructures affect existing modes of governance and foster novel power relations among public and private actors. Notably, the creation of new semi-autonomous databases facilitates the political acceptance of the algorithmic regulation of security. Our findings show how security programs challenge and broaden Yeung's (2018) taxonomy of algorithmic regulation. For instance, we suggest adding "emergent" as a mode of standard setting, because in the security domain, the objectives of algorithmic regulation are not always prespecified and publicly known. Our research also reveals that algorithmic security decisions are dispersed and difficult to contest, even when formal redress procedures are in place. There is a need to better understand how emergent forms of algorithmic regulation redesign security governance, and what the practical effects are of operationalizing values of privacy, dignity, and fairness through infrastructural choices.

This article is structured as follows. The first section makes the case for a dialogue between literatures on algorithmic regulation and on security studies. The second section develops an infrastructural perspective on algorithmic regulation, to bring into focus how algorithmic regulation is enacted and what work is carried out to make data flow across the Atlantic, and from private companies to state agencies. This allows us to examine how algorithmic security regulation functions in practice, and what security visions and ambitions it promotes. The third section sets out the key elements and methods for our empirical analysis. We focus on how datasets are curated to facilitate their circulation from commercial to public databases (data structuring), how legal obligations and values are inscribed into socio-technical systems (architectural constraints), and how decisions about what datasets security officers can and should use are enforced (interfaces). Our empirical analysis is based on a close reading of "Joint Review" reports, which are documents released by U.S. and European authorities in compliance with the terms of the EU-U.S. PNR and TFTP Agreements. The fourth section presents a close reading of how PNR and TFTP infrastructures make possible the algorithmic regulation of transatlantic security. In the conclusions, we reflect on how the focus on data infrastructures has implications for thinking about algorithmic fairness.

2. The algorithmic regulation of security

Yeung (2018) has proposed the notion of "algorithmic regulation" to enable a critical interrogation of how the use of algorithms comes to affect modes and targets of regulation in new and often problematic ways. In her conceptual framing, algorithms contribute to the creation of environments where deviations from given standards and objectives can be detected and corrected in a way that has never been possible before. Yeung's invitation is twofold: to attend to the specificity of each instantiation of algorithmic regulation, and to critically interrogate algorithm-driven governance. Her taxonomy of algorithmic regulation draws attention to algorithms' increasing capacity to enact the "variable adaptation of behavioural standards" and the "instantaneous" identification of deviating behavior (2018, p. 509). In this sense, algorithmic regulation is more immediate than conventional (pre-digital) types of regulation and sanctioning. Its adaptive and automated capacities entail a particularly powerful type of "architectural constraint" (2018, p. 509). The danger of complex adaptive standard setting and real-time predictive sanctioning systems is that meaningful deliberations and contestations of regulatory enforcements are excluded from this cybernetic-like environment (Amoore 2011; Supiot 2017).

The literature on algorithmic regulation has yet to fully connect to analyses in Critical Security Studies that have also focused on the role of algorithms and automated decisions in security governance, and that share some of Yeung's concerns (Amoore & Raley 2017; Leese 2014). This literature has pointed out that "the modern history of security is saturated with the methods and technologies of computation," and that "[t]o secure with algorithms … is to reorient the embodied relation to uncertainty" (Amoore & Raley 2017, pp. 3–4). Critical studies of algorithmic security regulation have facilitated growing attention for the role of non-human actors and technicalities (Aradau 2010; Salter 2015). This has paved the way for more granular analyses of the inner workings of security technologies and their political dimensions (Bourne *et al.* 2015; Shah 2017; Hoijtink & Leese 2019), which cast a light on how algorithms challenge the democratic governance of security (Huysmans 2014). Algorithms do not simply implement pre-established security visions. Rather, their use is "generative"; that is, security algorithms "abductively generate the threats and targets via the recognition of patterns in vast volumes of data" (Amoore & Raley 2017, p. 6). This means that algorithmic security affects what public and private actors perceive as security-relevant. Security algorithms may offer no clear evidence about why a given transaction or traveller may be suspicious. However, their capacity to crunch vast amounts of data seems to offer a mechanical knowledge that can justify speculative security decisions (de Goede 2012).

This body of literature can enrich efforts to better understand algorithmic regulation as proposed by Yeung and others. At least two themes are relevant. First, Critical Security Studies has extensively discussed how algorithmic security systems are targeted at "*future* action or behaviour based on algorithmic identification of unexpected correlations" (Yeung 2018, p. 509, emphasis added). This is not strictly an objective of "prediction" (Yeung 2018, p. 509), but has been analyzed as a process of precaution or preemption (Aradau & van Munster 2007; Anderson 2010). Preemptive security practices acknowledge that statistical predictions concerning future suspect behavior and deviation cannot reliably be calculated. At the same time, they seize upon these knowledge limits to use speculative inferences and correlations, drawn from a mass of data points, to creatively and pre-emptively identify possible future suspects. This is what Louise Amoore has called a "politics of possibility," which:

> *acts not strictly to* prevent *the playing out of a particular course of events on the basis of past data tracked forward into probable futures but to* preempt *an unfolding and emergent event in relation to an array of possible projected futures. (201, p. 9, emphasis in original)*

As this literature shows, algorithmic security is not strictly *predictive*, but works through speculative inferences to identify *potential* futures and suspicions. This has implications for the mechanisms and processes of algorithmic regulation.

Secondly, this literature problematizes the notion of regulation "as intentional activity directed at achieving a prespecified goal" (Yeung 2018, p. 507). In algorithmic security, the goal of securing is often not clearly articulated or prespecified. Broad ambitions like preventing attacks or intercepting suspicious money and people are formulated across this policy domain, and are assumed to be largely self-explanatory. However, the precise objectives of security programs – like the PNR or TFTP – remain under articulated. Their standard setting is not just adaptive (Yeung 2018, p. 508), but *emergent* and often secretive. The objectives of algorithmic security are emergent in the sense that they are "informed by the data … instead of being informed by legal experts" (Hildebrandt 2018, p. 3). Johns (2016, p. 131) identifies three different ways in which algorithms function as a "conduit between legal orders [and] sites of legal decision." Algorithmic governance can *refine, optimize*, or *substitute* lawful authority, in Johns' reading. The latter relation, whereby an algorithm does "legal work in its own right," is most prevalent in the domain of security, for example in relation to the creation of No-fly lists and other "catalogues of persons, entities, and things invested with risk" (Johns 2016, p. 133; see also de Goede & Sullivan 2016). "In this mode," writes Johns (2016, p. 133), an algorithm "operates as a structuring or background-conditioning device for an array of regulatory initiatives and legal interactions."

Moreover, security algorithms work through what Weber (2016, p. 116) describes as "systematized tinkering … the use of trial and error [and] bottom-up search heuristics" (2015, p. 116). "Anomaly," in this context, is different from statistical abnormality: instead of articulating a societal norm or standard to which regulation aspires, "anomaly detection" emerges processually from "the existence of variation in data" (Aradau & Blanke 2018, p. 12). As Amoore (2013, p. 66) shows, algorithmic security does not work with prespecified normative objectives, but with what she calls a "mobile norm" – that is, "a norm that is itself modulated and aleatory, governed not by normalcy and deviations but by differential curves of normality." In sum, the literature on security algorithms problematizes the notion of regulation as an intentional standard-setting activity aimed at a prespecified goal, and emphasizes its aleatory and inductive nature. What implications does this have for our understandings of the shape and politics of algorithmic regulation?

In Yeung's taxonomy (2018, p. 508), security algorithmic systems that use SWIFT and PNR data are closest to what she calls "complex predictive sanctioning systems" and "complex predictive recommender systems." These systems govern populations through "preemptive violation prediction" that act as powerful ways of social ordering (Yeung 2018, p. 508). However, insights from literature in Critical Security Studies also challenge and expand Yeung's taxonomy of algorithmic regulation in specific ways. They show that algorithmic security is typified by a lack of prespecified and publicly known regulatory objectives, coupled with new practices of emergent and secretive mobile norms. The security sphere also problematizes Yeung's distinction between sanctioning and recommending, in the sense that the outcome of security algorithms is to flag and recommend travellers or transactions for additional scrutiny. However, "flags" are "not stable expressions" like more traditional forms of coercive power (Crawford & Gillespie 2016, p. 411). Instead, they occupy the ground between recommendations on the one hand, and sanctions on the other. A flag is a recommendation for additional scrutiny (e.g. of the traveller at the airport, or of the financial transaction en route to a conflict zone), and so in itself a sanction in the sense that it causes delay and anxiety. As mechanisms of governance, flags are often uncertain, "their meaning unclear" and their operation secretive (Crawford & Gillespie 2016, p. 411). Taken together, the emergent standard setting of security algorithms, and the obfuscated operation of flagging as a regulatory mechanism, enrich Yeung's taxonomy of algorithmic regulation.

3. An infrastructural perspective

This paper develops an *infrastructural* perspective which aims to analyze algorithmic security practices in their wider socio-material context. As Ziewitz (2016, pp. 5–6) has argued, literatures usually understand algorithms as "consequential actors," opaque but powerful. We often tend to see algorithms as "black boxes" that need to be unpacked or opened up. In contrast to this "algorithmic drama," Ziewitz (2016, p. 2) suggests resituating the analysis of security algorithms into their broader workflows and digital infrastructures (Straube 2019).

Algorithms, in their original meaning of "a decision procedure," comprise far more than machine learning code (Amoore & Piotukh 2016, p. 2). They need instructions concerning risk appetites, patterns, and thresholds; technical platforms that render data mobile; and interfaces to enable access, use and functionality.

Building upon Science and Technology Studies, a growing body of literature draws attention to how infrastructures are not so much a "background or stage" for political life, but more "a domain through which relations are made" (Lancione & McFarlane 2016, p. 48; also Aradau 2010; Opitz & Tellmann 2015). Infrastructures are recognized to be "lively," contested, and the material embodiment of "complex rationalities of government" (McCormack 2016, p. 420; also Amin 2014). Susan Leigh Star's pioneering work on infrastructure in particular helps focus on the socio-material processes of standardization that are required for complex social processes to function across technical and legal differences, and temporal and cultural distances (Bowker & Star 1999; Star & Ruhleder 1996). Infrastructures do "not grow de novo," but are incremental and path-dependent (Star 1999, p. 383). They require encoding, standardizing, tinkering, and tailoring (Grommé 2016; Weber 2016). In this spirit, Fuller and Goffey (2012, p. 105) draw attention to the "tools, techniques and technologies" that enable digital workflows. They reintroduce attentiveness to the "relations of force" that underpin workflows, and they critically interrogate the formalizations, codifications, and scripts that enable algorithmic work to appear as a "seamless" flow despite its inherent "stickiness" (Fuller & Goffey 2012, pp. 106–108 & 109).

In terms of understanding algorithms as a *tool* of security governance, the notions of infrastructure and workflow focus attention on concrete data trajectories, and reintroduce notions of sequencing, movement and ordering into the algorithmic sense-making order. This approach helps unpack the manifold "friction[s]" that have to be overcome or silenced to make data flow (Edwards 2010, p. 84), for example, from airline companies to border security agents. Our objective is to unearth the hard work involved in making data points materialize, and making data transportable. Data flows are not inherently fluid and automated (Lupton 2015, p. 106), but rather something that need to be put in place and kept under scrutiny. As Latour (2011, p. 802) has put it: "smooth continuity is the hardest thing to get." Both the PNR and TFTP programs promise to continuously feed public authorities' security algorithms with fresh data, thus allowing them to govern a population algorithmically. In practice, this ambition takes the form of complex "programs of action" (Akrich & Latour 1992, p. 260), elaborated by European and U.S. institutions, in order to generate seemingly smooth data flows, thus making security algorithms work in the everyday world. The result is an often convoluted transatlantic data architecture, showing how much these security projects are beset with challenges, fissures, failures, and tentative fixes.

In terms of understanding algorithms as a *target* of security governing, our approach focuses on how the infrastructures of transatlantic data sharing inscribe legal and regulatory values in specific ways. As Hellberg and Grönlund (2013, p. 161) show, the "operationalization" of basic values – privacy, data protection, and accountability – does not precede the building of data infrastructures, but is "negotiated" through concrete "practical achievements" on how these values become part of new data practices. These achievements allow negotiators to claim that the essence of values has "been maintained," while concrete data flows are enabled, and institutional, political, and legal contestations are deflected (Hellberg & Grönlund 2013, p. 161). This suggests that juridical protections are not discursive supra-layers on top of data infrastructures, but co-constitutive of how technical systems are designed, built, used and audited. Data protection, for example, is both more and less than an ethico-juridical principle – it comes to route data flows in particular ways, and operates as a rationality of control over emergent forms of algorithmic regulation (Bellanova 2017).

4. Elements and methods in analyzing algorithmic security regulation

4.1. Three elements

Our argument is that an infrastructural approach brings into better focus key aspects of algorithmic regulation that deserve further scholarly attention. The empirical discussion that follows – focusing on the EU-U.S. PNR and TFTP programs – uses three key concepts arising from this approach to resituate (security) algorithms into their socio-technical infrastructures, and to focus the analysis on three of their core elements. These concepts inform the three empirical parts of the article (4.1, 4.2 and 4.3).

First, concerning algorithms as a *tool* of security regulation, there is a need to better understand how data are *structured*. Data structuring can be understood as the ways "of storing and arranging data" that allow algorithms to operate *on* something (Fuller & Goffey 2012, p. 83; Helmond 2015). As also emphasized by Eyert *et al.* (2022, p. 14), it is important to develop a greater understanding of the ways that knowledge is assembled in algorithmic systems, including the "actual production of data points … as the result of sometimes complicated socio-technical networks." This brings to the forefront the work required in managing digital data, which are never "raw" (Gitelman & Jackson 2013). Data need to be "collected, readied for the algorithm, and sometimes excluded or demoted" before feeding the algorithmic machine (Gillespie 2014, p. 169). This involves numerous tensions around "language, categorizations, update frequency, [and] granularity of values," among other issues (Pelizza 2016, p. 39). Thus, in our work, data structuring refers to the practices that curate, arrange and transport datasets, selecting and readying them for machinic processing, and to the "social processes" that facilitate the acquisition and movement of datasets (Goffey 2008, pp. 18–19).

Second, concerning security algorithm as a *target* of regulation, there is a need for greater understanding of how the operationalization and legal enforcement of values – such as privacy and accountability – take place in and through data architectures. Eyert *et al.* (2022, p. 17) propose the term "architectural constraint" to theorize how material conditions and computer programs make certain "courses of action practically *impossible* – which is quite different from making them *unattractive*" (*Idem*, emphasis in original; also Yeung 2019). There are different modes and degrees of "technologically mediated influence," as classified by the Berlin Script Collective (2017). Here, we are interested in "technologically mediated coercion" in the form of, for example, digital boxes to be ticked or filled out before an analyst can access data in a system, or particular routings of data flows so that they are rendered (in)visible to institutional participants in a security program (Berlin Script Collective 2017, p. 11). Accordingly, we examine how data protection and juridical accountability are *inscribed into* the socio-technical infrastructures of transatlantic security workflows (Hanseth & Monteiro 1997). Such socio-legal infrastructures and architectural constraints are crucial to how data are rendered mobile, encoded, digested, and enriched, in order to become meaningful as the basis for security interventions.

Third, the notion of *interface* helps analyze how data are accessed, interpreted, and acted upon in the algorithmic security programs under scrutiny. As Cramer and Fuller (2008, p. 149) note, "[i]n computing, interfaces link software and hardware to each other and to their human users or other sources of data," thus facilitating not only users-hardware and users-software relations, but also hardware-hardware, software-hardware, and software-software (e.g. application programming interfaces) relations. Galloway (2012, p. 30) suggests studying an interface "not [as] something that appears before you but rather [as] a gateway that opens up and allows passage to some place beyond." From this perspective, interfaces are "processes" that regulate the interaction between officials and their datasets, through which relations of power are negotiated (Hookway 2014). For instance, O'Grady (2015, p. 132) shows that interfaces bring human and non-human participants together for specific governmental goals, like making sense of risk. While any algorithmic system relies on several and diverse interfaces, here we focus on those interfaces that affect the interactions between security officials and black-boxed datasets. On the one hand, the interface relates to the operation of algorithmic regulation as a *tool* of security, because interfaces structure how data are accessed, interpreted, and visualized, and how they produce flags that are relevant to security decisions. On the other hand, interface relates to security algorithm as a *target* of regulation, because interfaces determine who can access data, when, how, and under what conditions. Only validated data requests lead to interfaced access to particular data or datasets.

4.2. A note on method

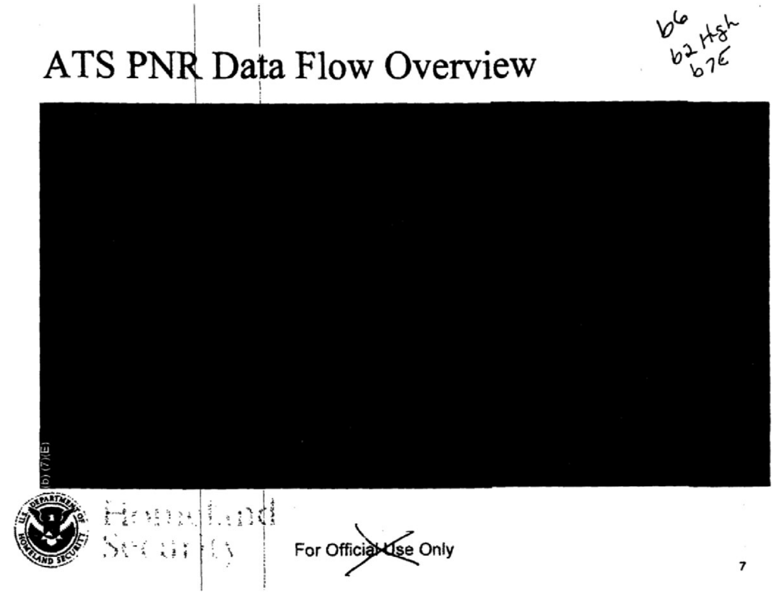
This article heeds the call to "examine algorithmic devices in situ" (Amoore & Piotukh 2016, p. 3). As the Snowden revelations highlighted, state authorities across multiple countries are engaged in mass-surveillance schemes – harvesting data from commercial databases, sharing them with agencies from other countries, and relying on algorithms to process vast amounts of digital transactions (Lyon 2014). In this geopolitical context of data-driven security workflows, the PNR and TFTP programs are among the most institutionalized systems. Their institutionalization is the fruit of several years of controversies and negotiations, which offer us a promising vantage point to study algorithmic regulation as both a tool and a target.

In this article, we focus on the Joint Reviews of these programs and other accountability documents as crucial research sites. Both the PNR and TFTP programs are subject to regular review exercises, as required by their respective agreements.2 The ad hoc review teams are composed of European and U.S. officials from various public authorities and units, mainly working on law enforcement, data protection, privacy, and international cooperation.3 The agreements define the goal of these exercises, namely to examine whether the programs comply with the technical, legal and organizational requirements set out in the Agreements themselves. Since their respective entry into force in 2010 and 2012, the EU and U.S. authorities have carried out five reviews of the TFTP Agreement and two reviews of the PNR Agreement.4 As part of the review process, the evaluation teams visit technical sites, collect statistical data, and report publicly.

Given the sensitive and secretive nature of data-led security practices, Joint Reviews offer information that would be difficult to collect otherwise. Granted, they only provide a partial account of these systems: the scope of the reviews is intrinsically limited, and teams refrain from advancing any criticism that may be read as a "political judgment" (EC 2011, p. 4). Memos, minutes, and other documents used during Joint Reviews are not publicly released. However, Joint Reviews are available publicly, and are accompanied by several reports and assessments carried out by European and U.S. authorities. By comparing these accountability documents with the heavily redacted material occasionally disclosed in response to freedom of information requests (cf. Fig. 1 below), their informative potential becomes evident. When their limitations are acknowledged and taken into consideration, this kind of accountability documents provides a situated but promising point of entry into otherwise secretive security practices (Walters 2019, pp. 167–170).

Moreover, Joint Reviews are valuable sources for studying the infrastructures of algorithmic regulation. Just as cable infrastructures become most visible when they break down (Starosielski 2015, p. 40), data infrastructures are rendered visible through their breakdowns and controversies over, for example, accountability and data protection (Bellanova & Fuster 2013; Neyland 2016). Joint Reviews seek to smooth over multiple political, legal, and technical frictions. However, they retain the imprint of these frictions, and they offer precious insights into the work needed to make commercial datasets become security data points.

In the sections that follow, we offer a close reading of the Joint Reviews, with a particular focus on how frictions are identified and (temporarily) resolved. Through these documents, we see that security agencies and companies are busy solving manifold infrastructural issues: the definition of appropriate technical and organizational systems to transfer data, the curation of data in view of their algorithmic analyses, the design of interfaces, etc. Throughout our analysis, we note when components of the programs remain secret, formally classified or beyond the reach of the review exercises. These classifications can themselves be relevant for understanding the political dimension of security data workflows.



ATS PNR Data Flow Overview

b6
b2 Hgh
b7E

[redacted]

(b)(7)(E)

Homeland Security

For Offici~~al Use~~ Only

7

Figure 1 Redacted slide presenting the "ATS PNR Data Flow Overview" (available at: https://www.eff.org/files/filenode/dhs_pass_data/20071207_euusphr.pdf, last accessed on 5 June 5 2020).

5. An infrastructural perspective on the EU-U.S. PNR and TFTP agreements

5.1. Data structuring

First, we examine how datasets are generated, curated, and selected. As explained, this relates to the way in which security programs function as a *tool* of algorithmic governance, in the sense that they produce and aggregate data to govern populations. Contrary to what is often thought, commercial datasets rarely exist in a form that is directly accessible by security officials, but need to be pre-processed, carved off, and rendered mobile. This section focuses on *data structuring*, understood as the work required to make (security) data materialize, and render them mobile, sharable, transportable, and ultimately actionable (also Flyverbom & Murray 2018).

In the case of PNR data, the first step of data structuring starts when data are extracted from the commercial ecosystem. Private companies actively participate in this process. Air carriers are obliged to systematically transfer PNR data on passengers on U.S.-bound flights 96 hours before takeoff, and then again at given intervals. PNR data are directly stored in the Passenger module of the Automated Targeting System (ATS-P), which is both a database and a computing system operated by U.S. Customs (US DHS Privacy Office 2007, 2012). Private companies use digital formats that they have negotiated with state authorities in the framework of PNRGOV working groups, hosted by the International Air Transport Association (IATA 2013). Other enterprises provide technological solutions to facilitate the transfer of PNR data (e.g. SITA 2020). The initial ambition of U.S. authorities to gain direct access to airlines' databases has not materialized as such. This first step of data structuring shows how private companies were able to shape algorithmic security by both regulating how data should circulate and defining international standards for data formats. The second step consists of masking sensitive data. An automated system looks for "codes and terms" that are deemed to reveal sensitive information about passengers, by filtering these data out (EC 2017a, p. 13). However, the analysts retain the possibility of manually overriding the filtering systems when they believe that data have been erroneously excluded – for example, when they consider that the airline system did not send data with a "nexus" to the United States. Moreover, U.S. Customs officers can gain direct access to air-carrier databases if there is a technical problem that prevents data transmission. This "ad hoc pull" system can be used "in order to respond to a specific, urgent and serious threat" (EC 2013b, p. 18). This infrastructure aims at defining the "right population" to be algorithmically governed. Software regulates the private-public data transfer, limiting companies' liability. However, the scope of data collection remains wide enough to facilitate security algorithms' emergent standard setting, and public officials retain the ultimate power to override technical solutions and assert security needs.

Data structuring accompanies the entire lifecycle of PNR data. The whole socio-technical system aims at making sure that PNR data can become data points usable for border and immigration controls, counter terrorism and law enforcement. Once "loaded" into the ATS-P, datasets may be updated in response to modifications concerning passengers' reservations or the flight itself (EC 2013b). PNR data are curated at least three more times. First, datasets are depersonalized after six months: all information that may link a PNR to an individual passenger is masked. These datasets are still processed in an "active database," where U.S. Customs officers process them to detect patterns and profiles, and, under strict administrative supervision, they can be re-personalized when a law enforcement operation requires the identification of a given passenger (EC 2013b, p. 10). Five years after their initial ingestion, PNR data are moved into a "dormant database," where processing, access and repersonalization are subject to stricter conditions, that is, "only in response to an identifiable case, threat, or risk" (EC 2017a, p. 33). Finally, after 10 years in the dormant database, PNR data have to be "fully anonymized," that is, curated so that it is impossible to "repersonalize" them (EC 2013b, p. 33). Even when their connections to identifiable passengers are removed, they are endowed with an intrinsic security value. Their structuring as anonymous data ensures their store-ability, making them computable and actionable for the foreseeable future. They are indexed and thus retrievable for further queries, and valuable for what they may tell as part of informational "mosaic[s]" (Amoore 2013, p. 85). PNR data are means of real-time "speculative security" (de Goede 2012), *and* sources for future algorithmic regulation.

The TFTP algorithmically governs populations by capturing financial wire-transfer datasets held by SWIFT, and analyzing them to identify possible connections to terrorism financing and facilitation (broadly defined). Capturing and curating these datasets, and rendering them transportable across jurisdictions, has taken considerable regulatory and infrastructural work. With the exception of a brief moment immediately after 9/11, SWIFT has not allowed security authorities direct access to its database. Instead, the security datasets that are transported to U.S. Treasury have to be curated and rendered mobile. SWIFT itself plays an important role in algorithmic regulation, by shaping how datasets are carved off from the source database and made transportable. In the current form of the TFTP, the curation of the dataset operates through monthly data requests from the U.S. Treasury to SWIFT, for a batch of wire-transfer data suspected of a possible "nexus" with terrorism. At the same time, the U.S. Treasury sends a copy of the request, including supporting documents, to the EU agency Europol. These data requests cover a specific timeframe, and specify "the geographical sphere and lists the required data categories" (JSB 2012, p. 3).

The U.S. Treasury data requests have to "include recent specific and concrete examples of terrorist threats and vulnerabilities" relating to the (geographical) scope of the dataset requested (EC 2012, p. 6). Upon receiving the U.S. Treasury data request, and after the approval of this request by Europol, SWIFT curates the database to be transferred to the U.S. Treasury. This dataset is encrypted – or black-boxed, in SWIFT's words. The size of these (monthly) datasets is unknown: prior to 2012, it was estimated that millions of records were transferred annually (Belgian Privacy Commission 2006). Since the entry into force of the TFTP Agreement, however, the amount of data transferred to the U.S. Treasury is classified, because it is argued that "too detailed information on data volumes would in fact provide indications [about] message types and geographical regions sought" to adversaries (EC 2012, p. 5). Taken together, data requests now "essentially cover a continuous time-period" (JSB 2012, p. 2). This infrastructure of algorithmic regulation in the TFTP has been established through difficult political and juridical negotiations over data request protocols, formatting and encryption. By stabilizing this infrastructure, a heated political controversy was turned into a relatively smooth and continuous transatlantic data flow.

5.2. Architectural constraints

This second section examines those socio-legal infrastructures of the PNR and TFTP programs that function as architectural constraints in algorithmic regulation. These are the technical practices and juridical arrangements that render data mobile across jurisdictions, under particular conditions. We focus on how data mobility is established and enabled: what are the conditions that allow data to flow, and what role does data protection play?5 Once captured and re-structured from their commercial source, how are data made to flow, and what trajectory do they carve out? We focus on the material operationalization of values, how a "legitimate flow" is enabled, what shape it takes, what technologies it requires, and how it becomes juridically blocked, routed or fixed. Here, the focus is on the infrastructures as a target of algorithmic regulation.

The socio-legal infrastructures that make the PNR security workflow possible are the offspring of a decade of negotiations. The introduction of a system able to automatically assess all passengers became a political priority for the U.S. government after 9/11 (US DHS 2003), but setting up a transatlantic socio-legal infrastructure proved challenging from technical, juridical, and political perspectives (Papakonstantinou & De Hert 2009). Notably, the initial ambition of U.S. authorities to gain unfettered direct access to air carriers' databases created an important fissure in the transatlantic workflow. Besides the adoption of a system whereby data are automatically pushed to authorities (EC 2017b), the main architectural solution was to adopt the same storage and protection rules for all PNR data collected by U.S. Customs. Legal constraints are thus inscribed in the security workflow as architectural constraints concerning how data should be transferred from airlines to public authorities, and by making PNR data part of a separate, EU data protection-friendly database within the ATS-P (US DHS Privacy Office 2017).

Other architectural constraints condition the circulation of PNR data among public authorities. U.S. Customs may share PNR data and related analytical information with domestic and foreign law enforcement agencies if standards concerning their safeguards are met. Access to PNR data is also granted to initiatives focusing on migration and border controls. These forms of distribution and data fusion are either based on ad hoc dispatching or discrete access to the PNR database. The overall transatlantic regulative framework of PNR data slightly complicates domestic exchange and processing. Probably in response to these socio-legal constraints, U.S. Customs now "copie[s]" all PNR data into the *DHS Data Framework*, a "classified database [which] is used exclusively for counter-terrorism purposes" (EC 2017a, p. 12). This is both a technical and legal operation. It allows U.S. authorities to index PNR datasets and make then discoverable to classified queries without having to reopen transatlantic negotiations. The European review team recognizes that "this change should be acknowledged in the review," but it does not question this new data architecture, limiting itself to assessing this infrastructural operation from a legal compliance perspective (EC 2017a, p. 12).

Introduced in 2007, the *DHS Traveler Redress Inquiry Program* is an online tool for individuals to request access to their travel information, including their PNR data. It is a sort of addendum to the other socio-legal infrastructures, but it has gained a central role in the operationalization of values. Through it, U.S. authorities responded to criticism concerning privacy and judicial redress rights of non-U.S. citizens, who are granted limited rights by relevant statutory laws. It served as a legal requirement to introduce an extra form of accountability in the security practice (also Kosta 2022). However, this tool is barely used by EU citizens, and the number of PNR-related requests is paltry (EC 2017b, pp. 16–17). At the same time, this (limited) form of data protection compliance stabilizes the overall functioning of the PNR system as a mass-surveillance program. In response to data access requests, U.S. authorities do not release information about how security decisions may have been informed by PNR-fed algorithms, nor about the risk assessment logics used. Rather, the mere presence of this online tool deflects legal contestations and has allowed a major transatlantic dispute to be overcome. In sum, data protection takes a material form which puts limited constraints on security workflows.

The socio-legal infrastructures of the TFTP were similarly built through a series of transatlantic negotiations that slowly grafted particular modes of accountability and legality onto an ad-hoc and secretive post-9/11 security program. Safeguarding the dataflow became cast as a top priority in transatlantic security in 2010, after Members of the European Parliament threatened to stop the data transfers in the interests of the privacy of European citizens.

Eventually, continued data flow was enabled through the establishment of particular architectural constraints that inscribed privacy and redress onto this pre-existing security program. This speaks to how TFTP became a target of algorithmic regulation, by building juridical protections into the transatlantic infrastructure. The 2010 TFTP Agreement designs a new socio-legal infrastructure in which rights of access and rectification for data subjects were incorporated at the insistence of the European Parliament. Figure 2 shows how data protection is built into the data infrastructure, and comes to route TFTP data in particular ways. Data requested from SWIFT (the "designated provider" at the bottom of the image) are sent in encrypted and black-boxed form to a special server inside the U.S. Treasury. Access to this "standalone" server is regulated through successive EU-U.S. negotiations and agreements: the dataset as curated and black-boxed by SWIFT remains formally inaccessible to Treasury officials until they perform a search, as discussed in the next section.

Moreover, two Overseers – one on behalf of SWIFT, and one on behalf of the EU – work inside the U.S. Treasury and contribute to the TFTP workflow. The Overseers have the authority to assess the compliance of TFTP searches with the Agreement's provisions, and to block them in real time. The TFTP Agreement, moreover, grants an EU citizen the right to "seek the rectification, erasure, or blocking of his or her personal data processed by the U.S. Treasury Department" (Articles 15 and 16). During the last review period for which a report is available, three requests for data access were made, and during the lifetime of the Agreement no requests for data rectification have been made at all (EC 2017b, pp. 17–18). Indeed, one of the fissures in the TFTP workflow is that the rights to access and rectification *cannot* effectively be exercised. The first Joint Review of 2011 explains that data in the "standalone server" (Fig. 2) can be accessed only to perform a terrorism-related search, and not to ascertain whether a subject's data are held, or to correct such data, because all searches require a "demonstrable nexus to terrorism" (EC 2011, p. 12). What could be understood as a serious flaw in the proper functioning of the TFTP workflow, however, is reduced to a glitch in the Review report, which notes: "Although this may seem unsatisfactory to the individual … the EU review team is of the opinion that this procedure is a correct implementation of the Agreement" (EC 2011, p. 12). The socio-legal infrastructure of citizen protection was indispensable to making data flow across the Atlantic, but its malfunctioning in terms of providing actual redress is reduced to an afterthought.

5.3. Interfacing

This final empirical section deploys the notion of interface to explore the everyday processes through which security professionals interact with data – pertaining to algorithmic regulation as both a tool and a target. Here,

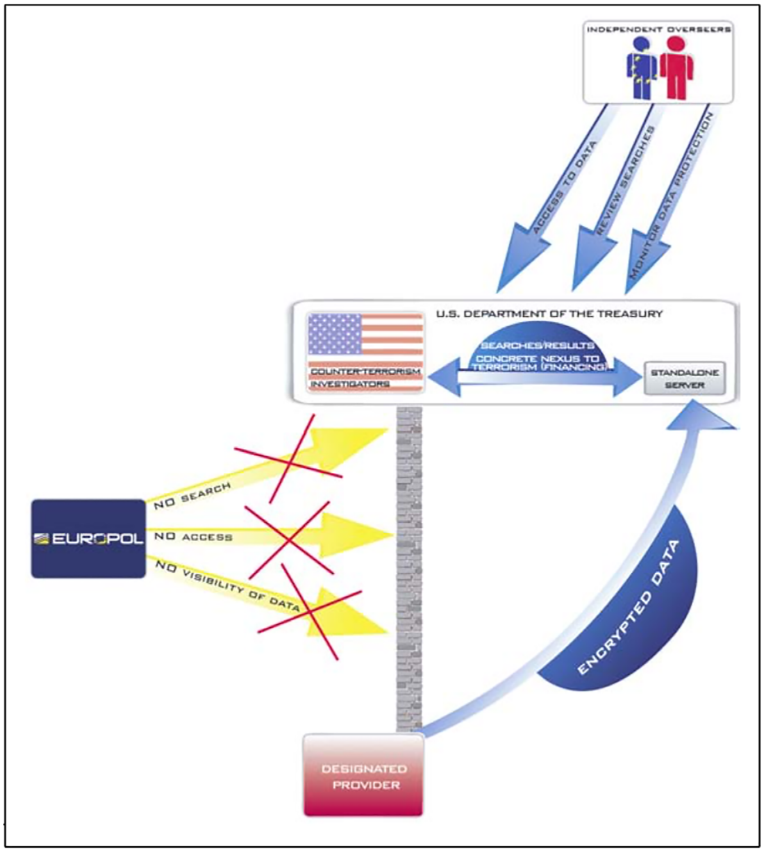


Figure 2 TFTP workflow: from commercial database to security decision (Europol 2011, p. 4).

interfaces affect how data are made productive for algorithmic security decisions. But interfaces also condition who can access data, when, and how. Attending to the modes of interfacing encourages an analysis of how data are combined, interpreted, and shared – that is, processed – to generate flags. Data processing is co-constituted, and interfaces can tell us something about the terms under which diverse elements come together and how operations of algorithmic sense-making become possible.

Once ingested by the ATS-P, PNR data are processed in several ways. They are run against other law enforcement and immigration-control databases, and uploaded in other data systems (mainly for counter terrorism purposes). Besides their processing in the ATS-P and the National Targeting Centre, PNR data are also shared with frontline officers making decisions concerning further screening, boarding or even admission of travellers. In May 2015, U.S. authorities declared to the EU team that "14,414 [Department of Homeland Security] users have access to PNR in the 'active' PNR database" (EC 2017a, p. 27). Even if many officers have "just" the possibility to "view" a limited portion of stored PNR data (EC 2017a, p. 13), the increasing diffusion of this mode of interfacing is becoming a fissure in the transatlantic workflow. While limiting the datasets available to most frontline officers, the same interface multiplies the possibilities of accessing the PNR database. The European Commission voiced requests about the need to "monitor the number of staff with access rights to PNR data to ensure that only those with an operational need to use and view the data can do so" (EC 2017c, p. 4). In fact, this interface foregrounds the idea that PNR data may prove useful across many security policies, running against the European discourse about the need to limit and target PNR data processing.

According to its Privacy Impact Assessment, the data run through the ATS provide "decision support" in three main ways. PNR data are compared with other databases and with risk-based rules. They are made available to "federated queries," and are the object of "search across many different databases and systems" (US DHS Privacy Office 2012, p. 2). These processing operations create spaces where security officials and PNR data interface. However, these spaces are themselves a byproduct of other processes of interfacing – where hardware relates to other hardware and software, and software relates to other software. Details about how analysts can act upon PNR data are codified in a dedicated document, the *CBP PNR Directive*, which, however, is not included in the Joint Review documentation. This "directive" is accessible to the EU review team under strict conditions: only a paper version can be consulted, and for a limited time (EC 2017a, p. 15). In the context of algorithmic regulation, all these processes are essential to produce flags, which here should be understood as algorithmic knowledge that informs analysts and frontline officers about whom further security action should be directed toward (secondary screening, refusing entry, etc.).

Securing the participation of humans is key to the success of the PNR processing operations. This is mainly done via the ATS graphical user interface, which claims to "improve the user experience" and apply "technical security and privacy safeguards associated with the underlying systems" (US DHS Privacy Office 2007, p. 3). Joint Reviews do not provide detailed information about this user interface, but they note that specific training and technological and organizational supervision are used to further discipline ATS-P users (EC 2017a). For instance, analysts can override an automated decision of the filtering system, but the software will automatically flag the human decision to a supervisor. This interface has both an operational and legal function. Data-mining and profiling systems require analysts capable of generating flags out of vast amounts of data across multiple databases. By bringing together analysts and PNR data, the user interface facilitates knowledge generation and thus regulation through algorithms. Moreover, user interfaces enable emergent approaches to data analysis. "Updates" to the ATS Privacy Impact Assessment show that changes to the user interface permit the application of "risk-based rules centered around CBP [Customs and Border Protection] Officer experience," and cross-matching with several other databases (US DHS Privacy Office 2017, pp. 10 & 24). This interface also guarantees the presence of a "human in the loop," which is essential to ensure the legality of any profiling system from an EU perspective (Jones 2017). There is a general prohibition of decisions "based solely on the automated processing and use of PNR" (EC 2017a, p. 34). The presence of humans shields a crucial site of security decision-making from institutional enquiry. Indeed, compliance with this requirement has satisfied the Review Team's inspection. The team has neither investigated the risk assessment logic adopted nor the security decisions *supported* by PNR automated processing.

The interface between SWIFT data and U.S. Treasury officials is configured through the notion of *nexus*, which regulates the conditions under which data may be accessed. It has been formally stipulated that each TFTP data search has to have a "nexus to terrorism or its financing" (Article 5, TFTP Agreement). This requirement to record a nexus to terrorism (financing) is one site through which the regulation of security algorithm is shaped. The nexus has to be documented and entered into the system, and "no search can take place without the entry of information on the terrorism nexus of the search" (EC 2012, p. 8). The nexus is assessed by the Overseers who work inside the U.S. Treasury on behalf of both SWIFT and the EU, and who have the power to request additional information and to block searches in real time (EC 2012, p. 9).

However, it remains difficult to assess what this nexus means, and how it operates as an interface between human and machinic sense-making. The nexus is never formally (i.e. legally) defined; it is a broad and flexible conditionality. It may entail tentative or speculative connections to suspected terrorism or its financing. Recognizing a nexus is said to require "intensive" intelligence "training on the job" (EC 2012, p. 8), that is, the intuitive and experienced assessment of an intelligence professional. In the words of a senior EU official, a terrorism nexus "is something that has to be decided by the [Overseers] in the light of their own professional experience… [T]his is why it is …not suitable and appropriate to put the data protection guy in this function because … they don't [know] the mod[us] operandi [of terrorists]."6

A nexus, in any case, must be a broad and flexible category – broader than the established juridical threshold of a reasonable suspicion. We know that there were 31,797 searches in the first 20 months of the TFTP program (EC 2012, p. 5), and 27,095 searches in the 22 months covered by a more recent review (EC 2017b, p. 9). An average of 1,200–1,300 searches were performed per month in the different review periods (EC 2017b, p. 9). In this manner, the U.S. Treasury curates its own dataset out of the black-boxed SWIFT data: data extracted through searches become part of internal U.S. Treasury databases and enter a different data protection regime with different retention periods (governed by U.S. law). In addition, extracted data, in the U.S. Treasurylogic, are no longer governed by the protections of redress and rectification as stipulated in the 2010 EU-U.S. Agreement. More than 11,000 TFTP-derived "leads" were shared between the U.S. Treasury and European police authorities in

2014–2015 in the context of counter terrorism investigations, including "account numbers, names, addresses, transaction amounts, dates, branch locations" (EC 2017b, p. 41). Once shared with European police forces, however, it becomes impossible to follow these leads, as agencies receiving them will not be informed that they are TFTP-derived.

6. Conclusion: An infrastructural perspective on algorithmic security regulation

This article has examined data-led security programs as both a tool and a target for algorithmic regulation. We suggested that an infrastructural perspective offers a useful way of thinking about algorithmic regulation, and how it concretely takes shape in the security domain. Focusing on the convoluted and controversy-driven data infrastructures of the EU-U.S. PNR and TFTP agreements, we have analyzed how data structuring, architectural constraints and interfacing organize and enable security workflows. We have shown how datasets are transferred from private to public databases, how data are rendered mobile across institutional and juridical boundaries, and how interfaces function to facilitate algorithmic sense-making on risk. Data flows are generated through complex legal and political negotiations over right formats, visibilities, and protections.

Data infrastructures are not neutral, as they materially, legally, and politically support specific ways of doing security. In the transatlantic data flows under consideration, we observed a redistribution of competences (Europol acquiring an important role in legitimizing the transfer of sensitive commercial data); a shifting boundary between public and private (airlines and SWIFT acting as data sources *and* shaping how data circulate); the introduction of new actors (like the Washington-based EU Overseer for the TFTP program); and the creation of sui generis databases and servers (in both security workflows). The technical operation of dataflow, then, has implications for structures of governance and the appearance of novel power relations among actors – not the least for those individuals who are "flagged" or who wish to exercise data-access and redress rights. Importantly, the progressive institutionalization of these data infrastructures has contributed to evacuating political and legal controversies. This has not been achieved easily, nor are the solutions merely cosmetic. As we highlighted throughout the analysis, the creation of these infrastructures requires time and the design of sophisticated technologies. Notably, the carving out of new, semi-autonomous databases – with specific rules for storage and protection – was pivotal in the institutionalization of both security workflows as properly regulated, and thus legitimate, security algorithms.

We showed how these security programs challenge and expand Yeung's taxonomy of algorithmic regulation in specific ways. The security sphere adds "emergent" as a mode of standard setting to Yeung's taxonomy, alongside "fixed" and "adaptive." Emergent standard setting is typified by an uncertainty and malleability of goals and interventions. In addition, flagging is an important mode of intervention in the taxonomy of algorithmic regulation – it holds ground between recommending and sanctioning, and operates with dispersed and often secretive effects. As Yeung (2018, p. 519) argues, algorithmic regulation raises questions that go beyond "informational privacy," and that touch upon "core legal and constitutional principles that are ultimately rooted in the liberal commitment to treat individuals with fairness and dignity." In conclusion, we suggest that our examination of PNR and TFTP data infrastructures has several implications for thinking about algorithmic regulation and its broader implications for fairness.

First, we have drawn out how – in the security domain – the objectives of algorithmic regulation are not always prespecified and publicly known. As Johns (2016) also argues in relation to security and existential threats, algorithmic systems have the capacity to do regulatory work in their own right. Our infrastructural approach shows how such emergent, regulatory work is done in the cases of EU-U.S. PNR and TFTP programs. The data infrastructures generated through these two Agreements stitch together regulatory spaces across the Atlantic and across public-private spheres in novel ways. As stated in a Joint Review report, they allow a "close cooperation between the U.S. authorities, Europol and EU counter terrorism authorities in assessing and communicating on terrorism-related threats" (EC 2017b, p. 21). Importantly, in the case of the TFTP, they provide speedy access to financial data without formal data extradition requests or other legal formalities. For example, one day after Anders Breivik's attacks in Norway in July 2011, the U.S. Treasury provided 35 TFTP-derived leads to Europol "detailing Breivik's extensive financial activities and network that spanned nearly a dozen countries," some of which were related to "financial transactions conducted between four and eight years prior to the attacks"

(EC 2013a, p. 14). The significance of these dataflows is not so much their ability to *prevent* attacks – clearly, in the Breivik case, they did not – but how these security spaces allow security authorities to have unprecedented and swift access to transaction data without interference by a judge or necessary recourse to extra-jurisdictional data requests. More broadly, this contributes to the literature on algorithmic regulation by (i) drawing attention to types of regulation that are not clearly goal-driven or prespecified, and (ii) showing how infrastructures play important roles in enacting algorithmic regulation in particular ways.

Second, and related to Yeung's emphasis on principles of "fairness and dignity" (2018, p. 519), our cases show how security data infrastructures uphold a practice where regulatory decisions are dispersed and difficult to contest, even when formal redress procedures are in place. This pertains both to algorithmic regulation as a tool (whereby the algorithmic programs based on PNR and SWIFT data govern populations) and as a target (whereby values like privacy are built into the infrastructures). The architectural constraints and interfaces structuring the processing of PNR and TFTP data show how diffuse algorithmic security has become, and how challenging it is to pinpoint where and how discrete security decisions are made. The inscription of specific values into the workflow, where privacy is mostly reduced to data security or accountability fixes, has a double channeling purpose. While it participates in defining appropriate routes and routines for data processing, it largely deflects more radical questions concerning the fairness and necessity of mass-surveillance programs, and reduces value failures to minor technical issues in otherwise functioning systems. Crucially, the particular design of PNR and TFTP security workflows has contributed to rooting a transatlantic political imaginary where privacy-friendly algorithmic surveillance is achievable. Their infrastructural choices resonate with increasing emphasis on engineering data protection in the technical and organization design of data practices – be they in the security domain or elsewhere (Bellanova 2017). For instance, European institutions adopted an EU-wide scheme for PNR use in 2016, on the grounds of its presumed added value for counter terrorism and high standards of data protection (Ulbricht 2018). In this respect, the cases we studied can be read as cautionary tales – they highlight how architectural constraints aiming at operationalizing values rarely leave enough space to assess algorithmic logics, or to contest their regulative effects on individuals or populations.

Acknowledgments

Many thanks to the special issue editors, Lena Ulbricht and Karen Yeung, for their support of this paper. Comments by three anonymous reviewers for *Regulation & Governance* were incredibly detailed and helpful. We thank Annalisa Pelizza and Mark B. Salter for their feedback on previous versions of this article, and all members of the FOLLOW team for help and suggestions. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (research project "FOLLOW: Following the Money from Transaction to Trial", Grant No. ERC-2015-CoG 682317).

Endnotes

[1] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *OJ* L195/5, 27.07.2010; and Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, *OJ* L215/5, 11.08.2012.

[2] Cf. Article 23 PNR Agreement and Article 13 TFTP Agreement.

[3] For instance, the 2017 EU-U.S. PNR Joint Review teams included officials from the European Commission and the EU Delegation to the U.S., a data protection expert from the French Data Protection Authority, a border and aviation security expert from the U.K. Home Office, as well as 17 U.S. officials from the Department of Homeland Security, and Customs and Border Protection, ranging from the Privacy Office to the National Targeting Centre and the Immigration & Customs Enforcement (EC 2017c: 44–45). The 2019 E.U.-U.S. TFTP Joint Review teams included two officials from the European Commission, two representatives of European data protection authorities and seven U.S. officials, from the Departments of Justice and Treasury, and from the Office of the Director of National Intelligence (Civil Liberties Protection Officer) (EC 2019: 21).

[4] Before the adoption of the 2012 PNR Agreement, EU and U.S. authorities had carried out two Joint Reviews (2005 and 2010) as foreseen by the previous agreements. These Joint Reviews are not part of our corpus.

[5] The PNR and TFTP Agreements pre-date the adoption of the 2016 European data protection reform, that includes the General Data Protection Regulation (GDPR) and the Police and Judicial Authorities Data Protection Directive. As legal scholars have shown, the two Agreements, and their specific data protection regimes, are also the offspring of tensions with the then overall European data protection legislative framework (Mitsilegas 2014). A 2017 EU Court of Justice's opinion on the draft EU-Canada PNR Agreement suggests that, if these security workflows were to be renegotiated, their conformity with current European data protection legislation and jurisprudence would be matter for legal debates (Tambou 2018).

[6] Interview, senior EU official, DG Home, Brussels, January 2013.

References

Akrich M, Latour B (1992) A Summary of a Convenient Vocabulary for Semiotics of Human and Nonhuman Assemblies. In: Bijker W, Law J (eds) *Shaping Technology/Building Society*, pp. 259–264. MIT Press, Cambridge, MA.

Amin A (2014) Lively Infrastructure. *Theory, Culture and Society* 31(7/8), 137–161.

Amoore L (2011) Data Derivatives. *Theory, Culture and Society* 28(6), 24–43.

Amoore L (2013) *The Politics of Possibility*. Duke University Press, Durham.

Amoore L, de Goede M (eds) (2008) *Risk and the War on Terror*. Routledge, London.

Amoore L, Piotukh V (2016) Introduction. In: Amoore L, Piotukh V (eds) *Algorithmic Life*, pp. 1–18. Routledge, London.

Amoore L, Raley R (2017) Securing with Algorithms. *Security Dialogue* 48(1), 3–10.

Anderson B (2010) Preemption, Precaution, Preparedness. *Progress in Human Geography* 34, 777–798.

Aradau C (2010) Security that Matters. *Security Dialogue* 41(5), 491–514.

Aradau C, Blanke T (2018) Governing Others: Anomaly and the Algorithmic Subject of Security. *European Journal of International Security* 3(1), 1–21.

Aradau C, van Munster R (2007) Governing Terrorism through Risk. *European Journal of International Relations* 13(1), 89–115.

Bauman Z, Bigo D, Esteves P *et al.* (2014) After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8(2), 121–144.

Belgian Privacy Commission 2006. *Advies nr 37*, *27 september*. Brussels: Commissie voor de Bescherming van de Persoonlijke Levenssfeer.

Bellanova R (2017) Digital, Politics, and Algorithms. Governing Digital Data through the Lens of Data Protection. *European Journal of Social Theory* 20(3), 329–347.

Bellanova R, Fuster GG (2013) Politics of Disappearance. Scanners and (Unobserved) Bodies as Mediators of Security Practices. *International Political Sociology* 7(2), 188–209.

Berlin Script Collective (2017) *Comparing Scripts and Scripting Comparisons. Toward a Systematic Analysis of Technologically Mediated Influence*. Technical University, Berlin.

Bigo D (2019) Beyond National Security, the Emergence of a Digital Reason of State(s) Led by Transnational Guilds of Sensitive Information: The Case of the Five Eyes Plus Network. In: Wagner B, Kettemann MC, Vieth K (eds) *Research Handbook on Human Rights and Digital Technology*, pp. 33–52. Edward Elgar, Cheltenham.

Bourne M, Johnson H, Lisle D (2015) Laboratizing the Border. *Security Dialogue* 46(4), 307–325.

Bowker GC, Star SL (1999) *Sorting Things out*. MIT Press, Cambridge, MA.

Brownsword R, Yeung K (2008) *Regulating Technologies*. Hart, Oxford.

Clarke RA, Morell M, Stone G, Sunstein C, Swire P (2013) *Liberty and Security in a Changing World. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*. The White House, Washington.

Cramer F, Fuller M (2008) Interface. In: Fuller M (ed) *Software Studies. A Lexicon*, pp. 149–153. MIT Press, Cambridge, MA.

Crawford K, Gillespie T (2016) What is a flag for? Social media reporting tools and the vocabulary of complaint. *New Media & Society* 18(3), 410–428.

EC (2011) *Commission Report on the TFTP Joint Review*. European Commission, Brussels.

EC (2012) *Commission Report on the TFTP Joint Review*. European Commission, Brussels.

EC (2013a) *TFTP Joint Report*. European Commission, Brussels.

EC (2013b) *PNR Joint Review*. European Commission, Brussels.

EC (2017a) *PNR Joint Review*. European Commission, Brussels.

EC (2017b) *Commission Report on the TFTP Joint Review*. European Commission, Brussels.

EC (2017c) *Commission Report on the PNR Joint Review*. European Commission, Brussels.

EC (2019) *Commission Report on the TFTP Joint Review*. European Commission, Brussels.

Edwards PN (2010) *A Vast Machine. Computer Models, Climate Data, and the Politics of Global Warming*. Cambridge, MA: MIT Press.

Europol (2011) *Information Note to the European Parliament*. Europol, The Hague.

Eyert F, Irgmaier F, Ulbricht L (2022) Extending the Framework of Algorithmic Regulation. The Uber Case. *Regulation & Governance* 16(1), 23–24.

Flyverbom M, Murray J (2018) Datastructuring. *Big Data & Society* 5(2), 1–12.

Fuller M, Goffey A (2012) *Evil Media*. MIT Press, Cambridge, MA.

Galloway A (2012) *The Interface Effect*. Polity, Cambridge.

Gillespie T (2014) The Relevance of Algorithms. In: Gillespie T, Boczkowski PJ, Foot KA (eds) *Media Technologies*, pp. 167–193. MIT Press, Cambridge, MA.

Gitelman L, Jackson V (2013) Introduction. In: Gitelman L (ed) *"Raw Data" Is an Oxymoron*, pp. 1–14. MIT Press, Cambridge, MA.

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

de Goede M, Sullivan G (2016) The Politics of Security Lists. *Environment and Planning D* 34(1), 67–88.

Goffey A (2008) Algorithm. In: Fuller M (ed) *Software Studies. A Lexicon*, pp. 15–20. MIT Press, Cambridge, MA.

Grommé F (2016) Provocation: Technology, Resistance and Surveillance in Public Space. *Environment and Planning D* 34(6), 1007–1024.

Hanseth O, Monteiro E (1997) Inscribing Behaviour in Information Infrastructure Standards. *Accounting, Management and Information Technologies* 7(4), 183–211.

Hellberg A-S, Grönlund Å (2013) Conflicts in Implementing Interoperability. *Government Information Quarterly* 30(2), 154–162.

Helmond A (2015) The Platformization of the Web: Making Web Data Platform Ready. *Social Media + Society* 1(2), 1–11.

Hildebrandt M (2018) Algorithmic Regulation and the Rule of Law. *Philosophical Transactions of the Royal Society A* 376 (2128), 1–11.

Hoijtink M, Leese M (eds) (2019) *Technology and Agency in International Relations*. Routledge, London.

Hookway B (2014) *Interface*. MIT Press, Cambridge, MA.

Huysmans J (2014) *Security Unbound*. Routledge, London.

IATA (2013) *Passenger and Airport Data Interchange Standards*. International Air Transport Association, Montreal.

Jacobsen KL (2015) Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees. *Security Dialogue* 46(2), 144–164.

Johns F (2016) Global Governance through the Pairing of List and Algorithm. *Environment and Planning D* 34(1), 126–149.

Jones ML (2017) The Right to a Human in the Loop. *Social Studies of Science* 47(2), 216–239.

JSB (2012) *Europol JSB Public Statement*. Europol Joint Supervisory Body, The Hague.

Kosta E (2022) Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights. *Regulation & Governance* 16(1), 212–224.

Lancione M, McFarlane C (2016) Infrastructural Becoming. In: Blok A, Farias I (eds) *Urban Cosmopolitics*, pp. 45–62. Routledge, London.

Latour B (2011) Networks, Societies, Spheres. *International Journal of Communication* 5, 796–810.

Leese M (2014) The New Profiling. *Security Dialogue* 45(5), 494–511.

Lupton D (2015) *Digital Sociology*. Routledge, London.

Lyon D (2014) Surveillance, Snowden, and Big Data. *Big Data & Society* 1(2), 1–13.

McCormack D (2016) Elemental Infrastructures for Atmospheric Media. *Environment and Planning D* 35(3), 418–437.

Mitsilegas V (2014) Transatlantic Counterterrorism Cooperation and European Values. In: Curtin D, Fahey E (eds) *A Transatlantic Community of Law*, pp. 289–315. Cambridge University Press, Cambridge.

Neyland D (2016) Bearing Account-Able Witness to the Ethical Algorithmic System. *Science, Technology & Human Values* 41 (1), 50–76.

O'Grady N (2015) Data, Interface, Security. *Geoforum* 64, 130–137.

Opitz S, Tellmann U (2015) Europe as Infrastructure. *South Atlantic Quarterly* 114(1), 171–190.

Papakonstantinou V, De Hert P (2009) The PNR Agreement and Transatlantic Anti-Terrorism Cooperation. *Common Market Law Review* 46(3), 885–919.

Pelizza A (2016) Disciplining Change, Displacing Frictions. *Tecnoscienza* 7(2), 35–60.

Salter MB (ed) (2015) *Making Things International 1*. University of Minnesota Press, Minneapolis.

Shah N (2017) Gunning for War. *Critical Studies on Security* 5(1), 81–104.

SITA (2020) SITA API PNR Gateway. Available at: https://www.sita.aero/solutions-and-services/solutions/sita-api-pnr-gateway (last accessed 18 June 2020).

Star SL (1999) The Ethnography of Infrastructure. *American Behavioral Scientist* 43(3), 377–391.

Star SL, Ruhleder K (1996) Steps toward an Ecology of Infrastructure. *Information Systems Research* 7(1), 111–134.

Starosielski N (2015) *The Undersea Network*. Duke University Press, Durham.

Straube T (2019) The Black Box and its Dis/Contents. In: de Goede M, Bosma E, Pallister-Wilkins P (eds) *Secrecy and Method in Security Research*. Routledge, London.

Supiot A (2017) *Governance by Numbers*. Hart Publishing, London.

Tambou O (2018) Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement. *European Foreign Affairs Review* 23(2), 187–202.

Ulbricht L (2018) When Big Data Meet Securitization. *European Journal for Security Research* 3(2), 139–161.

US DHS Privacy Office (2007) *Privacy Impact Assessment for the ATS*. Department of Homeland Security, Washington.

US DHS Privacy Office (2012) *Privacy Impact Assessment for the ATS*. Department of Homeland Security, Washington.

US DHS Privacy Office (2017) *Privacy Impact Assessment Update for the ATS*. Department of Homeland Security, Washington.

US DHS TSA (2003) Transportation Security Administration. Privacy Act of 1974: System of Records. *Passenger and Aviation Security Screening Records [148]*. Federal Register, Washington.

Walters W (2019) The Microphysics of Deportation. A Critical Reading of Return Flight Monitoring Reports. In: Hoesch M, Laube L (eds.) Proceedings of the 2018 ZiF Workshop, p. 161–185. Münster: ULB.

Weber J (2016) Keep Adding. On Kill Lists, Drone Warfare and the Politics of Databases. *Environment and Planning D* 34(1), 107–125.

Wilcox L (2017) Embodying Algorithmic War. *Security Dialogue* 48(1), 11–28.

Yeung K (2018) Algorithmic Regulation: A Critical Interrogation. *Regulation & Governance* 12(4), 505–523.

Yeung K (2019) Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law. *The Modern Law Review* 82, 207–223.

Ziewitz M (2016) Governing Algorithms. *Science, Technology & Human Values* 41(1), 3–16.