12

SENSING EUROPEAN ALTERITY: AN ANALOGY BETWEEN SENSORS AND HOTSPOTS IN TRANSNATIONAL SECURITY NETWORKS

Annalisa Pelizza and Wouter Van Rossem

INTRODUCTION

The topic of this book carves a distinctive space in a promising dialogue between sensor technologies and the performativity of security devices. On the one hand, literature on the design of sensor networks has pointed out how it challenges established features of traditional computer networks. Sensing networks require *ad hoc* architectures to respond to at least two key requirements: support for large numbers of unattended autonomous sensor points and adaptation to environmental conditions (Estrin et al. 1999; Dargie and Poellabauer 2010). Such requirements shape not only the technical infrastructure, but also divisions of labour across nodes.

On the other hand, the recent debate between Security Studies and Science and Technology Studies (STS) has produced accounts proposing an 'analytics of security devices' (Amicelle et al. 2015), questioning identification techniques as sociotechnologies of insecurity production (Suchman et al. 2017), wondering

how surveillance and security systems shape power and regulatory dynamics (Vogel et al. 2017), investigating how systems shape legal expertise (Leander 2013). Security Studies scholars most actively engaged in a dialogue with STS have embraced the notion of performativity to challenge the naturalness of security actors and of stabilized enunciating subjects (Aradau 2010; de Goede et al. 2014). Such achievements have made sense of security as sociotechnical agency being shaped but also shaping institutional orders and organizations (Dijstelbloem and Pelizza 2019). Security devices, in particular, (de)stabilize 'the power balance between organizational segments by altering communication patterns, roles relationships, the division of labor, established formats for organizational communication, and taken-for-granted routines' (Manning 1996: 54, quoted in Amicelle et al. 2015: 302).

The attempt to launch a dialogue between the sensor and security scholarships has thus the merit of focusing attention on the entrenchments between the performativity of infrastructures for data production and the alleged obduracy of institutionalized agency. With a few exceptions (e.g., Pelizza 2016; Witjes and Olbrich 2017), the interplay between data infrastructures and order institutionalized through laws has received ambivalent consideration in Science and Technology Studies. The spotlight on security sensing infrastructures thus allows recovering an interest in how sociotechnical orders crystallized in laws and regulations can mutate. Sensors can provoke institutional tensions (see Chapters 4 and 5 in this book). They can trigger changes in nation states and international organizations. These, in turn, can shape knowledge production by stabilizing sensing practices.

Following similar concerns, this chapter aims to conduct an experiment. The experiment is finalized to test the tension between the performativity of data infrastructures and the obduracy of institutionalized agency by adopting the rhetorical figure of analogy. Such rhetorical experiments are not new to the history of technology (Agar 2003), and we wish to extend them to current affairs. As it is known, analogy does not require a full overlap between items to be compared. It does not claim that they are *ontologically* equivalent. Less pretentiously, it singles out some common features of the two elements to be compared and *opportunistically* explores the extent to which such comparison

can reveal new aspects of the second item, before reaching the limits of the analogy itself.

The experiment we propose to conduct in this chapter explores the extent to which an analogy between architectures of sensor networks and trans-national security orders can have heuristic consequences and reveal new aspects of the latter term of comparison. As Ian Hacking (1983) has recalled, experiments' goal does not pertain to the realm of discovery, but to that of creation. To what extent can an analogy between data and institutional architectures provide new insights for inquiry?

The two elements of the proposed analogy are sensor data infrastructures and trans-national security networks for migration management. Not only do security networks rely upon data infrastructures, they also articulate trans-national orders which 'hit the ground' at distinctive, state-bound locales. One type of such locales are the 'Hotspots': migrant registration and identification centres set up at the external borders of Europe in 2015, in replacement of former, less technologically equipped centres (European Commission 2015b). Following literature on sensor architectures, we propose to consider four relevant features in order to unfold the analogy: the topological position of sensors as input devices, their ability to produce knowledge that would not otherwise exist, separation of concern and data reduction as design criteria.

In conducing this experiment, we also propose a methodological and epistemological challenge. Most sociologists who feel the pressure to imitate the natural sciences might find a textual experiment – a book chapter, in this case – unorthodox. However, such scholars would be at risk of overseeing two issues. First, they would confuse an objectivist style with an analysis that allows objects to *object* about what is said about them (Latour 2005). This is exactly what we do in the last part of this chapter, where the proposed analogy is followed to the point of reaching its own limits. Second, they would underestimate the insight that 'textual accounts are the social scientist's laboratory' (Latour 2005: 127). A well written text is a laboratory in that it makes the production of realism and objectivity progressively more complicated by constantly listening to the objections exerted by humans and artefacts.

Such 'listening to objections' has taken place through the analysis of regulation, through the collection of data during fieldwork at Hotspots in the Hellenic Republic in 2018, as well as through the analysis of information systems and technical documents developed by Hellenic and European authorities. In particular, the data analysed in this chapter have been collected from March to October 2018 during a multi-sited ethnography at four registration and identification facilities (i.e., three 'Hotspots' on the Hellenic islands and one identification centre on the Hellenic-Turkish border) through observation of border crossers identification procedures, in-situ interviews with officers from the Hellenic Asylum Service, the Hellenic Police and the Hellenic Reception Service, further off-site interviews – including with European officers, analysis of web interfaces of the Hellenic Register of Foreigners, procurement calls issued by the Hellenic Government, analysis of European regulation and other technical documents made available by both Hellenic and European authorities.

As a result of such 'listening', we suggest that migrant registration and identification centres can be understood as 'sensing nodes of equivalence'. On one hand, they might be conceived of as 'sensors' of European infrastructures for the 'processing of alterity' (Pelizza 2019). Hotspots have been designed by European agendas and practices as input devices for data collection and risk detection, producing information that wouldn't otherwise exist. On the other hand, registration and identification centres are not only input 'points' of European migration management architectures: they are also 'nodes' of equivalence in global security networks.[1] We suggest that Hotspots are nodes tasked with making non-European standards and procedures linguistically and materially equivalent to national ones.

In what follows we discuss how furthering an analogy of Hotspots as sensors (section 2) allows making sense of specific divisions of labour across organizational roles (section 3) and European authorities (section 4). However, we also test the limits of such analogy and suggest that the role of registration and identification centres cannot be only that of input *points* in European alterity processing networks. They also implement global security standards and practices that have become dominant worldwide (section 5). As such, we argue, Hotspots constitute *nodes* at which European data infrastructures

and transnational security networks not only metaphorically, but materially intersect.

All in all, testing the analogy of Hotspots as sensing nodes of equivalence allows opening incursions in current debates about the materiality of security regimes. Such understanding suggests new questions and research directions both to an emergent strand in Science and Technology Studies concerned with sociotechnologies of insecurity and to Security Studies proposing an analytics of security devices.

TWO EARLY FEATURES OF SENSOR NETWORKS

Sensor networks present characteristics that partially distinguish them from traditional computer networks. First, sensors are usually deployed in large numbers in peripheral or otherwise unreachable areas. Second, their deployment is unattended, and sensors are subjected to the caprices of weather, hostile animals (including hostile humans), energy shortages, disasters. Third, sensing devices interact with the physical environment and therefore experience a significant range of task dynamics (Estrin et al. 1999).

These characteristics have suggested distinctive architectures for sensor networks. Early architectures for sensor networks were based on a centralized model, with individual sensors communicating their data to 'a central node, which then performs the computation required for the application' (Estrin et al. 1999: 265). As scholars have stressed, 'most deployed sensor networks involve relatively small numbers of sensors, wired to a central processing unit where all of the signal processing is performed' (Estrin et al. 2001: 2033). More recently, however, the key requirement to assure energy efficiency has prompted different architectures, in which high-level pre-processed information – instead of raw data – is transferred (Elson and Estrin 2004).

These recent architectural developments will be discussed in more details in Sections 3 and 4; now we would like to stress two features of early sensor devices. First, sensors are input devices, tasked with measuring phenomena and encoding information that is then transferred to centres of calculation (Latour

1987). As such, sensors tend to occupy a distinctive position in the topology of measurement networks, namely a peripheral one. This division of labour between input devices and centres of calculation is allowed by the distinctive characteristic of sensors: the ability to operate unmanned and unattended. Sensors are delegated the task of replacing human beings in conducting measurements which would otherwise be limited in time and/or in space. Given these features, in early architectures sensors were conceived as input *points* – black boxed units for data collection, without processing power. Points are distinguished from nodes – unfolded sociotechnical assemblages whose inner working is accessible. This distinction will turn out useful in Section 5.

Sensors' capability to operate unattended introduces the second feature. Sensing devices are first and foremost tasked with producing information of phenomena that would otherwise remain invisible and unknown. In remote desert areas, on mountain peaks or on a 24h shift, human ability to know depends on sensing artefacts. In such situations, data would not only remain invisible: they *would not exist without sensors*. Such performative ability can find an echo in recent work about sensors as individuating devices: 'sensors can be described as engaged in processes of individuating by creating resonances within a milieu, where individual units or variables of temperature and light levels, for instance, are also operationalizing environments in order to become computable' (Gabrys 2016: 11, see also Gabrys 2019).

Hotspots as European sensors

Elaborating on the above-mentioned early features of sensing devices, we wonder to what extent Hotspots can by analogy be compared to sensors in European networks for alterity processing. While to our knowledge we are the first to propose such an analogy, we do not claim that we are 'discovering' it. Rather, as any analogy, it is a heuristic act of arbitrary association by the authors, that is nevertheless expected to open new research questions and directions.

Let's look at the first technical feature of sensors: they act as peripheral input points in sensing networks. Centres tasked with migrant reception and

management functions had been established already in the 1990s at the external borders of Europe. They proliferated as a consequence of the adoption of the Schengen Convention in combination with subsequent European treaties addressing 'irregular migration' and asylum (Balch and Geddes 2011). Being established at the external borders of Europe, such centres were geographically peripheral with respect to the rest of the Schengen Area.

However, informational input functions became a priority especially with the introduction of the 'Hotspot approach' (Pelizza 2019). In spring 2015, the European Commission issued a European Agenda on Migration, which announced the introduction of 'Hotspots' as an immediate action to address the challenges faced by frontline Member States (i.e., Member States at the external European border) involved in the increasing arrival of migrants (European Commission 2015a). The 'Hotspot approach' tackled primarily informational needs: 'The operational support provided under the Hotspot approach, will concentrate on registration, identification, fingerprinting and debriefing of asylum seekers' (European Commission 2015b: 1). The goal of the new approach was indeed 'to swiftly identify, register and fingerprint incoming migrants' (European Commission 2015a: 6). To achieve such goal, the approach foresaw the secondment to frontline countries of European officers from the European Asylum Support Office (EASO, with asylum support functions), European Border and Coast Guard Agency (Frontex, with policing and screening functions), Europol and Eurojust (with policing functions). Frontex and Europol are tasked with conducting mainly risk detection activities. Frontex's debriefing interviews, for example, are aimed at identifying trafficking networks and other risks.

Hotspots' characterization as informational input points emerged even during our multi-sited ethnography.[2] At Hotspots, people on the move are registered and identified against a plethora of national and European information systems utilized to verify previous asylum requests (Eurodac system), check previous criminal activities (SIS II system), establish identity, family relations, health conditions and other events (various national and international databases). Their data are inputted by national and European officers according to a strict division of labour (see next Section). Data on European systems are then accessible by European and national authorities Europe-wide.

Such data architecture shapes a distinctive division of labour. Hotspots can be seen acting as input points, 'sensors' tasked with data collection and risk detection functions. On the other hand, European and national asylum and police agencies act as centres of calculation, users of data collected at the border. As a consequence of this division of labour, Hotspots are peripheral, but not only in the geographical sense.[3] Hotspots are *topologically* peripheral because in the European migration data network they are tasked only with inputting functions and no processing power.[4] As such, they lie at the periphery of the security network.

The second technical feature of sensors is their ability to produce knowledge that would not otherwise exist. Here, too, the analogy seems to hold. As we have just seen by means of the regulation, the introduction of Hotspots was mainly aimed at improving data collection, thanks to the support of European officers. The European Commission rationale was that frontline states did not consistently comply with European regulations in the field of identification and registration. As a matter of fact, in 2015 the European Commission adopted measures against frontline states (European Commission 2015c).

Under similar circumstances, border crossers did not formally exist for European authorities and non-frontline member states, as their data did not exist on European databases. It was thanks to the introduction of Hotspots – with their personnel seconded by European agencies – that information could be produced, which would have otherwise remained unknown to centres of calculation. This is another sense in which Hotspots can be conceived of as sensors producing information that wouldn't exist without them.

Having suggested an analogy between sensing architectures and European networks for alterity processing, in the following two sections we further test the consistency and heuristic usefulness of the analogy by discussing two design criteria proper of sensor networks: separation of concern and data reduction. We also analyse the consequences of adopting those design criteria in the deployment of Hotspots for the division of labour in institutional security orders.

SEPARATION OF CONCERNS AS DESIGN CRITERION

Separation of concerns is a well-established design criterion within software engineering. It emphasizes a modular way of designing software by separating and encapsulating different functions of a system (i.e., 'concerns'), as a type of 'divide and conquer' strategy to manage the complexity of software development (Laplante 2007). We may find examples of separation of concerns in the way data produced by a sensor network are stored and processed.

Gibbons (2018) distinguishes three approaches for storing data in a sensor network, each of which has its own trade-offs. Data can be stored locally at production nodes in the sensor network, externally at points outside of the sensor network, or at other nodes. Storing data at a site external to the sensor network has historically been the most chosen option. This approach is an example of the separation of concerns, since it allows separating data collection from storage and processing functions carried on at external points. This form of separation is desirable because, while the sensor network is good at collecting data, points outside the sensor network usually have more resources available for storage and processing. Transmitting raw data outside the sensing network, on the other hand, has also some downsides. In the next section we will see how this issue factors into our analogy through the design criterion of data reduction.

System components designed according to separation of concerns are said to be 'modular'. Modules are self-contained, as they encapsulate their functions and data, so they can work independently and become interchangeable (Taylor 2009). In a sensor network, this modularity makes it possible for nodes to independently manage the processes for capturing data, and for external nodes to use the data without knowing how they were captured (Yick et al. 2008: 2293).

Separation of concerns at the Hellenic Hotspots

To what extent can we observe separation of concerns in the organization of Hotspots? What could be the heuristic consequences? Observations of practices of use of the Hellenic Register of Foreigners at the Hellenic Hotspots suggest

that the analogy between sensor architectures and security networks could hold even in this case. Notably, parts of the registration and identification procedure work in a similar way as 'software modules' which encapsulate functions and data addressing specific concerns. This is revealed more clearly once we compare the front and back-end designs of the Hellenic Register of Foreigners.

The Hellenic Register of Foreigners[5] was developed between 2011 and 2013 by the Hellenic Police and is used to identify and register persons who arrive at the border and other control points in Greece. As emerged during interviews with officers and observation of registration and identification practices mediated by the Register, different personnel roles – such as police, administrative clerks and asylum officers – use the system to input and retrieve migrants' personal and biometric data. Each personnel role has restricted access to data, according to their functions. These restrictions materialize in the graphical user interfaces used for registration and identification, in the form of tabs and fields available for some personnel and not others (Figs 12.1 and 12.2).

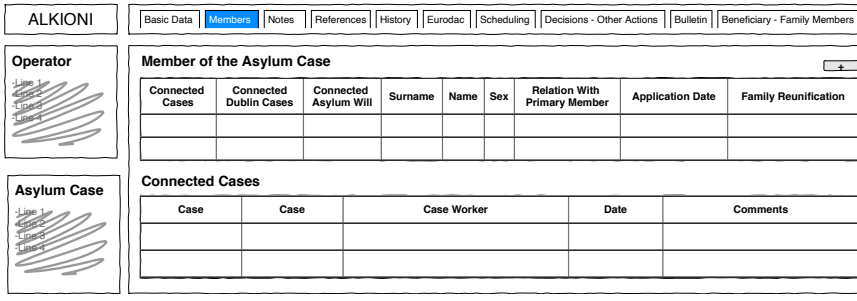

FIG. 12.1 Authors' elaboration of the original graphical user interface of the Hellenic Register of Foreigners, as accessible by the Hellenic Asylum Service.

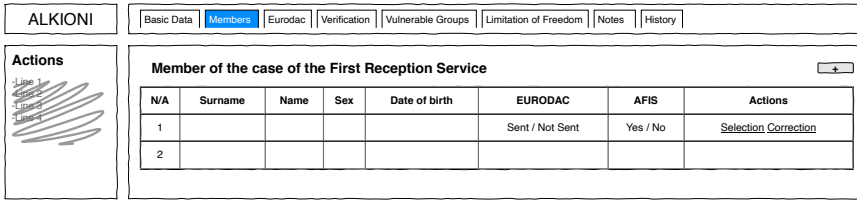

FIG. 12.2 Authors' elaboration of the original graphical user interface of the Hellenic Register of Foreigners, as accessible by the Registration and Identification Service (i.e., administrative civil personnel).

As a comparison between Figs 12.1 and 12.2 shows, some tabs and fields are accessible to asylum officers (i.e., 'References', 'Scheduling', 'Decisions', 'Bulletin', 'Beneficiary'), but not to administrative personnel, who have access to additional tabs (i.e., 'Verification', 'Vulnerable Groups', 'Limitation of Freedom'). Furthermore, different functionalities are accessible inside the same tab by different roles. For example, the tab 'Members' allows different tasks for each role. The information available for the asylum service relates to connections with other cases (i.e. family members). Differently, the registration and identification service can only access functions about the identification of individual applications through Eurodac.

Further evidence that supports the analogy with separation of concern is provided by back-end integration. While most tabs in Figs 12.1 and 12.2 link to data stored in and fields prompted by the Hellenic Register, the 'Eurodac' tab is loosely integrated with the European Eurodac information system.[6] The Eurodac component supports the fingerprinting process. When officers choose the Eurodac tab, the system opens up a separate software application that allows collecting and storing applicants' fingerprints on external databases, as well as checking whether asylum seekers have already lodged an asylum application. As it has emerged from technical document analysis and interviews with technical developers, the system then sends the fingerprints to the Hellenic Police Criminal Department. This Department in turn sends the fingerprints to the European Eurodac database and receives the hit or no-hit back. In this data flow it is important to note that Eurodac does not receive information about the contextual conditions of fingerprints collection. By doing so, modules have little direct knowledge of how each of them works and instead function in a self-contained and reusable manner.

In summary, both the interface design of the Register of Foreigners and its back-end integration with Eurodac show evidence of a separation of concerns between the Hotspots as sensors that collect data and the centres of calculation that use the data. Following the analogy with the design of software systems, the Hotspots data infrastructure uses a modular approach to separate and encapsulate different concerns, or functions.

This evidence triggers the question of how the separation and encapsulation of concerns in the Hotspot data infrastructure shapes the division of labour in European migration networks. Our on-field observations and interviews suggest that the separation of concerns in Hotspot data infrastructures entails a strengthening of epistemic divisions between different personnel roles. Such divisions are especially visible between national and European officers tasked with fingerprinting functions at Hotspots and expert officers at centres of calculation. Interviews with IT developers who work on the Register of Foreigners in Athens suggested that system design is explicitly expected to elicit boundary work. When asked about how the Hellenic Register of Foreigners integrates with the European systems, IT developers described the role of fingerprinting officers as having to be only concerned with doing the correct steps. They even specified that fingerprinting officers shouldn't know where data is transferred to.

Furthermore, the separation of concerns and ensuing encapsulation of functions can make work at the Hotspots invisible, as fingerprint data that are uploaded do not contain any metadata of how they were captured. Recalling Bowker and Star (1999), what information is recorded matters. In this case, separation of concern as a design criterion makes invisible the efforts needed to make bodies machine-readable and to produce data of acceptable quality. As Kloppenburg and Ploeg (2018: 15) explain: 'Accuracy, speed, and security are not inherent characteristics of biometric systems: a lot of work is continually required to achieve these outcomes in actual operational settings.'

All in all, the analogy between separation of concerns and the design of the Hellenic Register of Foreigners allows highlighting new forms of division of labour and production of knowledge, not only between input points and centres of calculation, but also between different personnel roles. From a software development perspective, the separation of concerns is a strategy to manage the complexity of systems: separate modules can be organized independently and become reusable. In the European security and migration network, encapsulating modules and functions can shape how knowledge is produced and circulated across different types of labour.

DATA REDUCTION AS DESIGN CRITERION

A distinctive requirement of sensor networks is the need to maximize energy efficiency. As in unattended and exposed sensor networks energy is the most precious resource, sensor networks need to reduce energy consumption as much as possible. Recent developments have marked new paradigms in this regard. In last generation sensor networks, energy efficiency is often achieved by converting raw data into high-level information as upstream as possible: 'A perfect system will reduce as much data as possible as early as possible, rather than incur the energy expense of transmitting raw sensor values further along the path to the user' (Elson and Estrin 2004: 10).

The design criteria of 'data reduction' establishes that in sensor networks it is not necessary to provide a complete record of every sensor measurement, but rather to provide high-level syntheses. To achieve reduction and synthesis, most recent sensors are thus designed to pre-process raw data at each node in the network: data are aggregated, and redundant information is filtered, before being transferred to the centre of calculation.

Hotspots pursuing data reduction

To what extent can data reduction be observed at Hotspots, and with which heuristic consequences? Our analysis of registration practices, technical documents and interfaces about migrant data exchange between Hotspots and European agencies has evidenced a design criterion similar to data reduction. Notably, during registration and identification at Hotspots a vast and heterogeneous amount of data is collected by officers in spreadsheets and national databases. However, only a minor part of those data is inputted in European systems. Most data are only inputted in national systems and never made available Europe-wide.

This is not due to some form of governmental data jealousy (Bekkers 2007), but to system design underpinned by legal principles of necessity and proportionality. Data reduction, or filtering, between national and European databases used at Hotspots becomes evident if only one takes into account data models

(i.e., classification systems) implemented nationally by the Hellenic Register of Foreigners (Fig. 12.3), and Europe-wide by Eurodac (Fig. 12.4).

As Fig. 12.3 shows, the Hellenic Register of Foreigners collects a range of standard basic data: name, nationality, gender, ID, photo and date of birth. On top of that, it also includes less standard categories, like name of father and mother, religion, ethnic group, educational level and languages spoken, profession, family situation and number of children, members of the family who already reside in Greece, socio-cultural ties with Greece. Furthermore, separate sections accessible only to specific profiles (e.g., physicians) collect health and vulnerability data.

BASIC DATA			**PERSONAL DOCUMENTS**		
Surname Name Father's name Nationality Estimated nationality Estimated date of birth Declared date of birth Sex/Gender	Mother's name Mother's surname Country of birth	Photo of the person	Type of document Passport Residence permit Other	Identification no of the doc	Accompanied files
Religion Profession	Ethnic group Communication language Mother tongue	Education level Languages (other)	Marital status Contact details	Additional info	
OTHER DATA					
Sent to Eurodac Yes/No Last place of staying (country)	Expression of interest for application of international protection Yes/No Expression of interest for voluntary return Yes/No	Bed of alien Defined/ not defined Date of departure	Member of family		
Valuables Kind (pieces) Withholding of objects		No of Asylum will			

FIG. 12.3 Basic data collected on the Hellenic Register of Foreigners, as accessible by the Registration and Identification Service (source: authors' elaboration from system interface).

DATA COLLECTED ON EURODAC

(a) fingerprint data

(b) Member State of origin, place and date of the application for international protection

(c) sex

(d) reference number used by the Member State of origin

(e) date on which the fingerprints were taken

(f) date on which the data were transmitted to the Central System

(g) operator user ID

(h) date of the arrival after a successful transfer

(i) date when the person left the territory of the Member States

(j) date when the person left or was removed from the territory of the Member States

(k) date when the decision to examine the application was taken.

FIG. 12.4 Data collected on Eurodac (source: European Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013). Some categories of data are only recorded when applicable.

Differently, Fig. 12.4 shows data collected on Eurodac. As it clearly emerges, Eurodac collects very few types of data. What is not in the system is relevant here, especially if compared to the Hellenic Register of Foreigners: religion, ethnic group, educational level and languages spoken, profession, family situation and links within Greece, socio-cultural ties with the Hellenic Republic. Furthermore, most data are system native: they did not exist before the person was recorded in the system (e.g., place and date of the application for international protection). In other words, Eurodac creates a self-referenced digital index, in which information acquires meaning in the context of the system itself, and is functional to pursue its main goal: compare fingerprints with asylum requests.

Comparison between data models implemented in the Hellenic Register of Foreigners and in the European Eurodac database suggests that a sort of 'data

reduction', or filtering, takes place in the exchange of migrants' data from frontline Member States to European agencies. Such exchange indeed concerns only a few basic and biometric data. It should also be noted that national and European databases are not interoperable, but integrated only through unique identifiers, what we called indexing data (e.g., Eurodac unique number). Furthermore, neither European agencies nor non-frontline Member States can access data on national systems. Consequently, most personal data about migrants are 'filtered' at the national level.

This evidence further grounds our analogy between sensor networks requiring upstream data reduction and European security and migration networks filtering most part of data collected at Hotspots. The analogy triggers new questions, as well. We have seen how in recent sensor networks the distinction between input devices and centres of calculation corresponds to a specific division of labour. Data reduction partially re-distributes tasks by pre-processing raw data before they are transferred to centres of calculation. Extending the analogy, we can ask how division of labour in European security networks is re-arranged.

Indeed, the practices of data filtering just described suggest a *de facto* division of labour between frontline countries and the rest of Europe. As any Member State and most European agencies involved, frontline countries are tasked with policing functions. To this end, basic and biometric data are paramount. However, through its Register of Foreigners the Hellenic Republic also collects data about family composition, education, religion, ethnic group, health, linguistic and professional skills, family links and socio-cultural ties with Greece. That is, data necessary to fulfil a broader set of functions, like accommodation, family reunification, health care, asylum, integration into the job market and in society at large.

We can conclude that a division of labour between frontline Member States and European agencies and non-frontline members is performed by filtering data collected at Hotspots. A division of labour in which all institutional actors are tasked with some sort of policing functions. On top of that, functions like accommodation, family reunification, health care, asylum and integration are mainly delegated to countries hosting Hotspots. It would indeed be difficult to design integration policies without data about family composition, professional and linguistic skills.[7]

As a last note, it should be noted that such division of labour does not take place because of geographical location, but because of epistemic differences in how the Other is made legible. Through its Register of Foreigners, Greece enacts people on the move as long-term foreigners, while European systems like Eurodac enact them as irregular foreigners. In other words, different ways of processing alterity correspond to different ways of institutionalizing security order.

HOTSPOTS AS GLOBAL NODES OF EQUIVALENCE

Up to now the tentative analogy between architectures of sensor networks and Hotspots as 'sensors' of European security and migration networks has seemed to hold. Like sensors, Hotspots work as input devices, retaining a peripheral position in the European security networks, and they enact information that wouldn't otherwise exist. Furthermore, as for sensing networks, design criteria like separation of concerns and data reduction can be seen at work. Following such analogy has also allowed us to pose new questions about division of labour between input points and centres of calculation.

However, analogy should not be mistaken for ontological sameness. As in any experimental laboratory, we have to be ready to acknowledge the limits of analogy. We have to be prone to 'listen to objections' moved by human actors and objects. In our case, the analogy between sensor networks and European security networks shows its limits when the global scale enters the picture.

Hotspots are not only involved in European migration networks. They also take part in global security networks. Yet their role in global networks is not the same as in European ones: they do not act as input *points* – black boxed units for mere data collection and risk detection, without processing power, but as *nodes* – unfolded sociotechnical assemblages at which technical standards and practices developed outside Europe are made equivalent to European ones.[8]

We have already seen in the previous Section that the most recent developments in sensor networks have endowed sensors with some processing power. On the other end of the analogy, when analysed in a broader transnational context, Hotspots acquire other roles than mere input points: as (re)users or

clients. This is revealed more clearly when registration and identification centres are considered in a context that includes technical and economic elements, besides strictly security ones.

Methodologically, one way to pursue this epistemic enlargement consists in analysing formal documents released for standardization goals in procurement practices. Such sources can reveal more heterogeneous relationships than those commonly assumed as part of security networks. A case in point is provided by a procurement call issued in 2011 by the Hellenic Agency for Information Society, a governmental body. The call concerned hardware and software provisions of electronic identification and authentication services – including fingerprinting – for citizens and foreigners. It mentioned the following specifications for the automated fingerprint identification system (AFIS):

> 1. The proposed AFIS solution must have implemented at least one (1) working AFIS system at a National, State or Federal Level worldwide over the past five years (5).
>
> 2. The proposed AFIS solution must have at least one implementation in a criminal AFIS that supports database with at least four (4) million ten-fingerprints, one (1) million palm prints, and has a minimum daily volume of a thousand (1,000) ten-fingerprints uploaded into the system. (Hellenic Republic Ministry of Citizens Protection 2011: 139)

This excerpt asks for three distinctive requirements: 1) that software is implemented worldwide and then reused in Greece; 2) that it is a reuse of criminal implementations; 3) that it can handle rather large-scale amounts of data. On top of that, fingerprint scanners must be FBI-certified (Hellenic Republic Ministry of Citizens Protection 2011: 144). Furthermore, the AFIS interface with INTERPOL should use the ANSI/NIST-ITL -1-2000 Data Format for the exchange of fingerprints, facial images and scars, marks, or tattoos (SMT) information (Hellenic Republic Ministry of Citizens Protection 2011: 40–41).

By posing such requirements, the procurement call positions any agency, registration centre or Hotspot using identification and authentication services

in Greece at the intersection of multiple global networks. First, according to the call the AFIS software must have been implemented worldwide, thus positioning Hellenic registration and identification centres as *(re)users of global travelling software* (Pollock and Williams 2009).[9] Second, the AFIS software must have been implemented in criminal contexts, thus positioning Hellenic centres as *(re)users of security software*. Third, the large scale of the required system positions the Hellenic Agency for Information Society as *client of incumbent software suppliers*. Fourth, by asking that fingerprint scanners are FBI-certified, Hellenic authorities *delegate certifying functions* to the US Federal Bureau of Investigation. Finally and similarly, choices about the interconnectivity format to be used between Hellenic authorities and INTERPOL are *delegated* to US government organizations developing the ANSI/NIST standard.[10]

In this division of labour, the utilization of software, equipment, practices and standards developed and implemented outside Europe carves for Hotspots a more complex role than mere European input points for data collections. Rather, registration and identification centres are conceived of by Hellenic authorities issuing the call as nodes in global security networks. In such position, centres are expected to create equivalences between European and non-European elements. Locally-acquired ink fingerprints must be made equivalent to AFIS-encoded high-resolution digital prints. Database entries for 'mother's name' on the Hellenic Register of Foreigners is expected to be made equivalent to 'اسم الأم' in the words of the Arabic interpreter. Spreadsheets generated for internal use among Hotspot officers must be made equivalent to travelling software produced by transnational corporations. While this work of making equivalences can be successful or not, what is important to stress here is that – when the global scale is taken into account – Hotspots act as nodes at which work of equivalence between standards and practices developed in and outside Europe is ceaselessly carried on.

Two further aspects are important. First, from these examples drawn from our fieldwork it results that equivalence can be established between diverse languages (the second case) as well as between diverse materialities (the first and third case). Second, it goes without saying that in this activity of creating equivalences, power relations are affected. Equivalence always entails betrayal

and pronouncing 'mother's name' in Arabic is not the same as pronouncing it in English or Greek. Reading ink fingerprints does not include the same actors as reading digital scans. In both cases, some actors are excluded because they do not speak English or do not have access to the digital system.

CONCLUSION: HOTSPOTS AS SENSING NODES OF EQUIVALENCE

As mentioned at the beginning of this chapter, the heuristic potential of any analogy lies in opening new spaces for questions and directions of research. This is the case even with the analogy between architectures of sensor networks and transnational security networks. The analogy has allowed us to ask novel questions on the division of labour in European security networks, and to focus on the new distribution of roles between frontline and non-frontline Member States.

However, such analogy intended to test the tension between data and institutional infrastructures has shown its limits in not being able to account for extra-European connections. As in any experimental laboratory, we had to leave our analogy when we realized that sticking to it would have brought us in a misleading direction. To account for the roles that Hotspots can undertake in global security networks, we conceived of them as 'nodes of equivalence'. Such switch has helped in acknowledging the major work of establishing equivalences that is conducted daily by national and European officers, as well as by migrants and interpreters, at centres for the identification and registration of people on the move to Europe.

Such new questions and research directions appeal both to Security Studies proposing an analytics of security devices, and an emergent strand in Science and Technology Studies concerned with sociotechnologies of insecurity. In the first case, they solicit Security Studies scholars to move their attention from devices to infrastructures. Hotspots are not only points, but nodes integrating European alterity processing infrastructures and transnational security infrastructures not only metaphorically, but also materially. In the second case, they

urge Science and Technology Studies concerned with identification practices and infrastructures to consider how their object of analysis can throw light on emergent transnational constructions of order.

Finally and related to the last point, conceiving of Hotspots as sensing nodes of equivalence suggests a further question, to be investigated in future work: what organizing logics of authority emerge from the peculiar positioning of Hotspots at the intersection of European alterity processing infrastructures *and* global security networks? Like early Modern city leagues (Tilly 1990), Hotspots articulate a trans-local topology, in which they are nodes in global security networks characterized by non-contiguity. However, differently from city leagues, they do not articulate an isotropic geography, in which they are supposed to be the centre of a local economy. Rather, they remain at the periphery of European security and migration networks, whose core are the centres of calculation at European and national level. For sure, such topological arrangement requires further investigation, both in relation to European, global and to national centres.

ACKNOWLEDGEMENTS

In writing this chapter, the authors acknowledge the 'Processing Citizenship' project (2017–2022), which has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 714463. Both authors would like to thank Ermioni Frezouli for her work as coordinator of the Project's fieldwork in the Hellenic Republic. If she is not included as co-author, it is because of her doctoral commitments, which have not allowed her to engage in this writing endeavour. The authors would also like to thank Aristotle Tympas. For the sake of scientific attribution, Wouter Van Rossem has written the section entitled 'Separation of concerns as design criterion', while Annalisa Pelizza has authored the main argument and the other sections. The work has nevertheless benefitted from joint discussions, supervision meetings and collaborative analyses.

NOTES

1 As it will become clearer in what follows, in the context of this chapter we distinguish between 'points' and 'nodes'. We conceive of the first as folded devices tasked with an inputting task; the latter as unfolded actors which translate different sources into each other.

2 Here, 'our' includes also Ermioni Frezouli, in her capacity as temporary collaborator of the *Processing Citizenship* Project. Ms. Frezouli however decided not to participate in this chapter as co-author.

3 As a matter of fact, Hotspots ought not to be deployed exclusively in frontline countries. While they eventually were only implemented in Greece and Italy, originally the European Agenda foresaw their potential deployment in any Member State that required them (European Commission 2015b).

4 The shift from geographical to topological remoteness has mostly gone unnoticed by literature on 'fortress Europe' and borders. However, it is crucial to study the relationship between data infrastructures and institutional orders.

5 In Greek, *Χαρτογράφηση Κυκλοφορίας Αλλοδαπών*.

6 The Eurodac (i.e., European Dactyloscopy) system was first introduced in 2003 to support the application of the Schengen Treaty and Dublin Convention. It stores the digital fingerprints of every person claiming asylum in one of the European Member States. By doing so, it intends to univocally identify asylum seekers, so they cannot apply in more than one Member State. Eurodac was developed by European authorities and is now run by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

7 It should be noted, however, that in some cases non-frontline Member States receive such data through international organizations. That non-governmental and non-European organizations act as intermediaries of European relations is indeed an important topic of analysis, and is addressed in forthcoming work by Pelizza, Loschi and Lausberg.

8 In the STS field, we are well aware of the topological meaning of equivalence as translation, that is, making to things that are different occupy the same position (see e.g. Latour 2005).

9 Following our observation on field and analysis of the procurement call, similar considerations could be made for hardware.

10 The ANSI/NIST standard can be considered the dominant standard worldwide for exchange of biometric and forensic information. The American National Standards Institute/National Institute of Standards and Technology – Information Technology Laboratory (ANSI/NIST-ITL) defines the content, format and units of measurement for the exchange of biometric and forensic information utilized to identify and authenticate individuals. The first version of the standard for the interchange of fingerprint, facial and biometric information was published in 1986 by the then called 'United States National Bureau of Standards'. Its goal was to support electronic fingerprint submissions from US state and local authorities to the FBI (Wing 2013). The standard is now used by law

enforcement, homeland security, military and other authorities in 71 countries in all continents.

REFERENCES

Agar, J. (2003). *The Government Machine: A Revolutionary History of the Computer*. Cambridge, MA: The MIT Press.

Amicelle, A., Aradau, C., and Jeandesboz, J. (2015). Questioning Security Devices: Performativity, Resistance, Politics. *Security Dialogue* 46(4): 293–306. <https://doi.org/10.1177/0967010615586964>.

Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue* 41(5): 491–514. <https://doi.org/10.1177/0967010610382687>.

Balch, A., and Geddes, A. (2011). The Development of the EU Migration and Asylum Regime. In H. Dijstelbloem and A. Meijer (Eds), *Migration and the New Technological Borders of Europe. Migration, Minorities and Citizenship.* London: Palgrave Macmillan UK, pp. 22–39. <https://doi.org/10.1057/9780230299382_2>.

Bekkers, V. (2007). The Governance of Back-Office Integration. *Public Management Review* 9(3): 377–400. <https://doi.org/10.1080/14719030701425761>.

Bowker, G. C., and Leigh Star, S. (1999). *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: The MIT Press.

Dargie, W., and Poellabauer, C. (2010). *Fundamentals of Wireless Sensor Networks: Theory and Practice*. John Wiley & Sons.

De Goede, M., Simon, S., and Hoijtink, M. (2014). Performing Preemption. *Security Dialogue* 45(5): 411–422. <https://doi.org/10.1177/0967010614543585>.

Dijstelbloem, H., and Pelizza, A. (2019). The State Is the Secret: For a Relational Approach to the Study of Border and Mobility Control in Europe. In de Goede, M., Bosma, E., and Pallister-Wilkins, P. (Eds), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. London: Routledge, pp. 48–62.

Elson, J., and Estrin, D. (2004). Sensor Networks: A Bridge to the Physical World. In C. S. Raghavendra, Krishna M. Sivalingam, and Taieb Znati (Eds), *Wireless Sensor Networks*. Boston, MA: Springer US, pp. 3–20. <https://doi.org/10.1007/978-1-4020-7884-2_1>.

Estrin, D., Govindan, R., Heidemann, J., and Kumar, S. (1999). Next Century Challenges: Scalable Coordination in Sensor Networks. In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking – MobiCom 1999*, pp. 263–70. Seattle, WA: ACM Press. <https://doi.org/10.1145/313451.313556>.

Estrin, D., Girod, L., Pottie, G. and Srivastava, M. (2001). Instrumenting the World with Wireless Sensor Networks. In *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No.01CH37221)*, pp. 2033–36. Salt Lake City, UT: IEEE. <https://doi.org/10.1109/ICASSP.2001.940390>.

European Commission (2015a). The Hotspot Approach to Managing Exceptional Migratory Flows. <https://ec.europa.eu/home-affairs/e-library/multimedia/publications/the-hotspot-approach-to-managing-exceptional-migratory-flows_en>.

—— (2015b). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Agenda on Migration. Brussels. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0240>.

—— (2015c). Refugee Crisis: European Commission Takes Decisive Action – Questions and Answers. <http://europa.eu/rapid/press-release_MEMO-15-5597_en.htm>.

Gabrys, J. (2016). *Program Earth: Environmental Sensing Technology and the Making of a Computational Planet*. University of Minnesota Press.

—— (2019). Sensors and Sensing Practices: Reworking Experience across Entities, Environments, and Technologies. *Science, Technology, & Human Values* 44(5): 723–36. <https://doi.org/10.1177/0162243919860211>.

Gibbons, P. B. (2018). Data Storage and Indexing in Sensor Networks. In Liu, L. and Tamer Özsu, M. (Eds), *Encyclopedia of Database Systems*. New York: Springer New York, pp. 850–53. <https://doi.org/10.1007/978-1-4614-8265-9_112>.

Hacking, I. (1983). *Representing and Intervening: Introductory Topics in the Philosophy of Natural Science*. Cambridge: Cambridge University Press.

Hellenic Republic Ministry of Citizens Protection. (2011). Διακήρυξη Ανοικτού Διαγωνισμού Για Το Έργο «Ηλεκτρονικες Υπηρεσιες Ταυτοποιησης Και Αναγνωρισης Πολιτων (Ε-Ταπ)» (Open Call for the Project 'Electronic Identification and Identification Services (E-Tap)').

Kloppenburg, S., and van der Ploeg, I. (2018). Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences. *Science as Culture* 0 (0): 1–20. <https://doi.org/10.1080/09505431.2018.1519534>.

Laplante, P. A. (2007). *What Every Engineer Should Know about Software Engineering*. CRC Press. <https://doi.org/10.1201/9781420006742>.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Society*. Harvard University Press.

—— (2005). *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford: Oxford University Press.

Leander, A. (2013). Technological Agency in the Co-Constitution of Legal Expertise and the US Drone Program. *Leiden Journal of International Law* 26(4): 811–31. <https://doi.org/10.1017/S0922156513000423>.

Manning, P. K. (1996). Information Technology in the Police Context: The 'Sailor' Phone. *Information Systems Research* 7(1): 52–62. <https://doi.org/10.1287/isre.7.1.52>.

Pelizza, A. (2016.) Developing the Vectorial Glance: Infrastructural Inversion for the New Agenda on Governmental Information Systems. *Science, Technology and Human Values* 41(2): 298–321. <https://doi.org/10.1177/0162243915597478>.

——(2019). Processing Alterity, Enacting Europe: Migrant Registration and Identification as Co-Construction of Individuals and Polities. *Science, Technology and Human Values* 45 (2): 262–288. <https://doi.org/10.1177/0162243919827927>.

Pollock, N., and Williams, R. (2009). *Software and Organisations: The Biography of the Enterprise-Wide System or How SAP Conquered the World*. Routledge Studies in Technology, Work and Organisations 5. London; New York: Routledge.

Salter, M. B. (2008). When the Exception Becomes the Rule: Borders, Sovereignty, and Citizenship. *Citizenship Studies* 12(4): 365–80. <https://doi.org/10.1080/13621020802184234>.

Suchman, L., Follis, K., and Weber, J. (2017). Tracking and Targeting: Sociotechnologies of (In)Security. *Science, Technology, & Human Values* 42(6): 983–1002. <https://doi.org/10.1177/0162243917731524>.

Taylor, R. N. (2019). Software Architecture and Design. In S. Cha, R. N. Taylor, and K. Kang (Eds), *Handbook of Software Engineering*. Cham: Springer International Publishing, pp. 93–122. <https://doi.org/10.1007/978-3-030-00262-6_3>.

Tilly, C. (1990). *Coercion, Capital, and European States, AD 990–1992*. Oxford: Basil Blackwell.

Vogel, K. M., Balmer, B., Weiss Evans, S., et al. (2017). Knowledge and Security. In U. Felt, R. Fouché, C. A. Miller, and L. Smith-Doerr (Eds), *The Handbook of Science and Technology Studies*. Cambridge, MA: The MIT Press, pp. 973–1001.

Wing, B. J. (2012). The ANSI/NIST-ITL Standard Update for 2011 (Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information). *International Journal of Biometrics* 5(1): 20–29. <https://doi.org/10.1504/IJBM.2013.050731>.

Witjes, N., and Olbrich, P. (2017). A Fragile Transparency: Satellite Imagery Analysis, Non-State Actors, and Visual Representations of Security. *Science and Public Policy* 44(4): 524–34. <https://doi.org/10.1093/scipol/scw079>.

Yick, J., Mukherjee, B., and Ghosal, D. (2008). Wireless Sensor Network Survey. *Computer Networks* 52(12): 2292–2330. <https://doi.org/10.1016/j.comnet.2008.04.002>.