Digital data and the transnational intelligence space

Laurent Bonelli, Didier Bigo

6

DIGITAL DATA AND THE TRANSNATIONAL INTELLIGENCE SPACE

Didier Bigo and Laurent Bonelli

Introduction

The Edward Snowden disclosures on the American National Security Agency's (NSA) large-scale digital capture practices have spawned the opening of a series of political, juridical, philosophical, and academic debates. Discussions have predominately counterpoised the relationship between mobility and communications control, on the one hand, and the exponential growth in the amount of traces left by the daily activities of individuals using digital technologies, on the other. But what exactly are traces, what do they record, and how are they being recorded? Are they "raw data" available to all or, instead, data that belong to the realm of the private?[1] To whom do the data belong? To what extent do they constitute new sources of enrichment, awareness, commercial profits, statistical knowledge on populations, knowledge on the intimate lives of individuals, and, of course, surveillance?

If the internet was at one time perceived as the place par excellence for knowledge exploration and the organization of remote encounters, it is now increasingly being seen as a world that exacerbates the expansion of neoliberal capitalist logics. Within the directives of the latter, digital data become a new raw material that is both free and can be used to monitor the activities and behaviours of individuals with the help of automated data collection technologies. Challenging the relevance of national borders, the internet has also been understood as a key vector of globalized communication, wherein anonymity has allowed for networks to be created according to the affinities and mutual interests of individuals. In destabilizing notions of internal and external geography and thereby blurring or superimposing borders, the internet has had an impact on uses of violence, security mechanisms, and intelligence logics.

In exchange for the "free" use of internet services and resources, commercial actors making the internet work and further developing digital technologies believe to have the inherent right to exploit data produced by individuals. As a consequence,

internet users have been subject to a "digital encomienda."[2] Organizations interested in intelligence, in the broad sense of the term—be it the police and the military, or immigration and customs officers—have come to see the internet as somewhat of a double-edged sword. On the one hand, it is a major risk as it devalues their pre-existing professional routines. On the other hand, it presents unique opportunities to gain in-depth knowledge on individual practices, which had previously only been held in the hands of the private sector. These actors, however, have by no means reacted uniformly—either through functional adaptation or through the coordination of an "intelligence community"—to these pitfalls and promises. What they have all done, though, is subsequently integrate the collection of personal data and the analysis of these digital traces into their repertoire of activities.

In some cases, the interception of large amounts of data, with the help of algorithms, allows for the detection of behavioural abnormalities. This information can subsequently be used to identify risk profiles. However, as we will argue in this chapter, the way that these practices are performed vary greatly depending on one's degree of seniority in their occupational field, their capacity in terms of personnel, their technical skills (hardware and software), as well as their subjective visions on what exactly counts as "intelligence." Depending on their practical goals and know-how, intelligence agents produce different interpretations of what these influxes of data and analytical treatments can do for their profession.

These various actors first discussed amongst themselves and with politicians the value that data constituted by traces left on the internet, potentially amassed, and linked together using database software in order to generate statistical information might have for intelligence activities. This then raised the question of the utility of dedicating significant financial and human resources to the acquisition of remote interception technologies (satellite, digital) and their relative advantage in comparison to human means that could be used to reach the same results, notably by employing undercover techniques and informants. As we shall see, individual and collective actors responded to this dilemma quite differently. If various actors situated in the "field of intelligence professionals" have come to realize how easy it is to accumulate, exchange, and store digital data, to what extent has this accumulation of data been counterproductive, leading these professionals to miss the specific forest for the millions of trees?[3] The most specialized services (intelligence-counterintelligence) are still not convinced by accumulation techniques (collect it all) and have instead preferred to keep their sensitive case files outside of shared collection and exchange circuits. The outbreak of a number of public controversies—notably following the disclosures on the human rights violations committed by the Central Intelligence Agency (CIA) and its accomplices, the large-scale data capture practices of the NSA and the "Five Eyes," (United States of America, United Kingdom, Canada, Australia, New Zealand) and the near-routine use of drones outside of active conflict zones—forced intelligence agencies to rethink the utility and value of these strategies and devices. Digital technologies were questioned not only in terms of their capacity to provide greater security, but also in terms of the legal questions their use raised, privacy

issues, and, more generally, their adequacy with the position-taking in terms of values of countries that claim to be democratic and contest the practices of authoritarian regimes (Bigo 2012, 2016).

In this chapter, we will examine only some of the agents situated in the intelligence field of sensitive information. On the one hand, these professionals belong to intelligence agencies that see themselves as working to defend the national interests of their country. On the other hand, these professionals also exchange data with their counterparts in the national security agencies of other countries. These intelligence service agents thus have the capacity and the authority to intercept data not only at home but also abroad. For the most part, represented countries include former colonial and neo-colonial powers of the Global North, who esteem that they have a role to play at the regional or global level. Together, these agents form a transnational space that is linked by virtue of historical alliances that were first established during World War II and, more recently, through the efforts of those who have come to play a major role in the geopolitics of Internet cables.[4] This space has been named after a group specializing in communications surveillance: the Five Eyes, or the Five Eyes Plus. However, as we shall see, this transnational intelligence space is not limited to the intelligence agencies that are members of that exclusive group. The story of the alliance that lead to the creation of the Five Eyes is quite well known but has often been summarized as a story about common sensibilities shared between intelligence agencies with Anglo-Saxon origins, that created the necessary conditions for a form of mutual trust to develop between political leaders and agency actors. However, we are not convinced of this historical-cultural narrative on trust established between similar countries. Such an argument implicitly assumes that each country has a clear national history as well as a homogenous intelligence policy, meaning that the only thing that the researcher would need to do, is to compare these national trajectories to understand how trust first emerged between the concerned countries. Instead, we propose a study of the means and practices of intelligence agencies in order to then chart their position within a transnational space, without assuming that national or cultural belonging creates positions of proximity between agencies. In determining our case selection based on power relations, our focus will be on intelligence agencies that are the most resource-endowed in quantitative terms, that demonstrate a degree of professionalism, and that have a long history of managing sensitive information. Inspired by the work of Pierre Bourdieu, our study seeks to systematize elements collected in interviews with intelligence professionals by employing a structural analysis of the space in which the selected intelligence agencies are situated. To do so, we perform a multiple correspondence analysis (MCA), which allows us to rigorously visualize the space of institutional positions based on a series of defining characteristics (type of missions conducted, supervisory authority, territory of action, staff numbers, technological capital, etc.). In making connection between these objective positions and the discourses of actors regarding their practices and the meaning of intelligence, we are able to identify homologies as well as divergences that structure cooperation and data exchanges between agencies.

As we shall see in this study, it is not the number of internet traces left behind that matter. The fact that traces are produced does not automatically turn them into a source of wealth or power. Instead, what matters is how such traces are constituted as data and used for intelligence policy purposes as well as the horizon of suspicion in which they are used. So why intercept data? Simply because they are available and can be "picked" as flowers growing in a free space? Should we do this for all data in order to have a comprehensive graph that represents relationships between individuals and large groups of the population? Or should we restrict our use of data and leave them where they are, thereby preventing their use in cross-checking?

The existence of an intelligence policy that involved the large-scale surveillance of masses of individuals, categorized as suspect or as undesirable, has for the most part been trivialized. It has been argued that linking intelligence techniques with automated technologies that record digital traces left by the activities of individuals and their transactions is justified when it's preventive and protective function can help to anticipate and avoid violence. Yet, in our opinion, the relationship between the existence of the digital and predictive intelligence is not in and of itself inescapable. As opposed to being due to the inherent nature of the technology, this association has been politically modelled in a specific international context and depends on power struggles between the actors who determine the use and exchange value of digital data. The value of data is determined by the degree to which they can generate suspicion—notably when it comes to future acts—even if correlations made are so weak that they do not hold when faced with the law. Thus, markedly in contrast with legal practices, the actors of this space of doubt, of suspicion, and of possibilities play the role of "prince counsellors" that provides advice before decisions are made by politicians. Moreover, the symbolic value of intelligence data depends less on its content—despite the ideology of secrecy that sanctifies this content—than it does on who produced it, in what context, and for what reason.

It is this last point that we will deal with more substantially as it was paradoxically concealed in general statements made on the surveillance "society" and on algorithmic reasoning, which incorrectly suggest that internet users from around the world have been complicit in their own voluntary servitude (Bauman and Lyon 2013, Lehr 2019). This requires us to think reflexively about what the term "intelligence services" (or "security services") really means and the relations between the practices of intelligence agencies on one side and the modalities of digital data surveillance on the other side. Though fairly common in international relations, this chapter will not provide a disembodied analysis of intelligence practices or a history without actors, where intelligence agencies are seen as obeying the orders of political leaders who determine overarching strategies. Instead, we will highlight the heterogeneous characteristics that define intelligence actors, pointing to their differences in terms of socialization, professional habitus, and of different types of missions and actions that are performed. In doing so, we will identify arcs of tension that exist between organizations whose logics of action and modes of reasoning are either antagonistic or, at the very least, advance opposed strategies.

Our analysis will thus shed light on power relations that, thus far, discussions on rivalries between services have failed to capture.

Data, information, intelligence: data as performances and products of competition between intelligence agencies

What do we call "data" when this terminology is used for and in relation to political intelligence purposes? How are data generated and integrated into information chains that allow for the production of analyses that respond to the demands of politicians? What place then does this kind of data occupy in what scholars have termed the "intelligence cycle"? (Gill and Phythian 2016, McElreath, Graves, and Jensen III 2017, Murphy 2016).

Can the data be described, as some believe, as constituting all the traces of a person's or group's activities that may have been collected automatically or intentionally and which are then grouped into files? Referred to as "raw" data, does the data contain generic information in terms of the location of a person associated with an event, at a given moment in the past or in the present? In a second step, can this information then be used to anticipate future behavior through the application of algorithmic software? Within the data, can a distinction be made between content data, which reveal personal opinions based on content and so-called "connection" data, that is "metadata" or tracking data that make associations between individuals based on the exchanging of messages or the sharing of websites as well as through the establishment of shared interests based on the frequentation of the same people and places? This distinction between content and connection data has been presented by many agencies as a technically-relevant difference, as there would be only limited constraints in the exploitation of the latter in comparison to the former.[5] This distinction appears in a number of reports and analytical documents, notably in the United States. However, in opposition to this impersonal interpretation of technical data, various European Courts have pointed out that all tracking and localization data, whether derived from content or connection data, interfere with the privacy of individuals, and as a result are protected by international laws and agreements on personal data.[6] As we can see in these debates and developments, the issue of data ownership is absolutely crucial, as are the ways in which data are created and used for different purposes. Based on this observation, it would then seem necessary to reverse the dominant thinking about data. In other words, data are not the sources of information and analysis, but they are instead the product of it.

Data ownership: an electronic encomienda

The issue of data and the definition of this term cannot be settled by way of a technical consensus. It is a political and legal controversy, which necessarily undermines any conception of raw data as simply technical property that keeps track of the flow of information and to some extent to origin of this information, but that is independent from the ends for which it is used.

As we will argue here and have done so elsewhere, it seems that, on the contrary, it is exactly the different purposes for which data are used that play a role in the construction of the meaning and the form that data take. These meanings and forms are not natural, nor are they raw. Rather, they are the product of specific performances done by a series of actors. This standpoint, however, is not always recognized or appreciated at its face value. In interviews with actors coming from various intelligence agencies as well as in the narratives of scholars working on the "cycle" of intelligence (i.e. intelligence studies), physiocratic and industrialist visions are often mobilized as metaphors when describing the nature of data. For example, in physiocratic analogies, data is represented as a flower or vegetable that awaits harvesting—it is sown by internet users themselves, randomly moved, and left idle or exchanged for services provided by private companies, thereby no longer belonging to the sowers. The data is collected like the celestial manna, granted not by a divine figure but instead by computer science. In industrialist depictions, data is compared to a precious mineral that can be extracted from veined ore rock. In such an analogy, it becomes important to have the right drilling tools that can detect what is important and consequently select and retain only what is of value. Given the mass amounts of heterogeneous and weakly correlated data that circulate, it would be necessary to capture, intercept, and trace data that correspond to a specific profile. Ideally, information would emerge from connections made by that profile, which could then be refined and cut, like diamonds. The desired output would be analysed and that would lead not only to quality information, but to useful information that can be mobilized in political decision-making processes. The transformation of data into politically-relevant information is performed through the analytical practices of intelligence professionals and defines their very métier, which involves much more than algorithmic statistical correlations or the idea of simply collecting information that is already "out there." The two metaphors therefore are not so much about the way these professionals work but are instead used to suggest that the "raw" data do not belong to anyone and are therefore there for the taking. In both visions, individuals are not seen as having ownership over their data. Instead, data are available to those who exploit them and don't have value in and of themselves but acquire added value for those that make data connections and articulations. Data only "make sense" when information is extracted. Taking stock of this overall process, we argue a digital encomienda is at work.[7] As during the Spanish colonization, the "natives" (here, the internet users) have been deprived of their ownership rights and of their status as citizens of the worldwide web. This creates the conditions of possibility for the "colonization" of the web to generate profits and intelligence data. In exchange, web users receive the benefits of more targeted marketing and consumption, remote contacts and friendships (i.e. Friendship 2.0), and allegedly protection against terrorism.[8]

However, while intelligence agencies may be in favor of this primitive political economy of data, these data have an origin. As European courts and data protection authorities have repeatedly pointed out, these data have initial owners. The drafting and recent implementation of the General Data Protection Regulation (GDPR) in Europe confirms this.[9]

Intelligence data: the work and competitions of intelligence actors

Justifying a series of interception and retention practices, "intelligence studies" theorizations of the "fabrication of information" and its transformation into intelligence as being part of a "cycle" of production essentially aim to naturalize the existence of data along with the right to exploit and aggregate them. This is done in relation to modes of reasoning that are often already constructed, meaning that data are used to confirm these modes of reasoning, not invalidate them. In opposition to this argument, we suggest that "intelligence" data are constructed in a performative manner by the very political decisions that initiate data searches, the social use of surveillance techniques that may or may not render something "visible," and, lastly, the languages used by recipients (multiple, single, unwanted) to encode and decode intercepted data.[10] The performances of intelligence actors are thus dependent and based on data belonging to individuals. Very often, however, these actors colonize individual data and transform them into "intelligence tools" by serializing, anonymizing, and grouping data into files. Data from the intelligence world only becomes data when a political interest in their production and preservation has been established, when decisions have been made on where to draw boundaries, which visible elements should be thrown out, and which traces should not be of interest. Data is produced with the aim of creating lists of threats, risks, and vulnerabilities and identifying suspects. They are creating Data Suspects.

In terms of "data politics," our vision is to insist that data is a special performance that reconfigures the relationship between the digital and the material, while influencing contemporary relations between intelligence, surveillance, violence and obedience. These relations and configurations depend on the internal games of intelligence actors and the way that they define security, insecurity, and fate (Bigo 2008).

From such a perspective, intelligence data is understood as the product of political manoeuvres that constitute these data from the very outset according to that which they are "supposed to see," as though this was a neutral and objective act allowing politicians to make decisions. Yet, the act of creating data by orienting them so that they may prove the (legitimate) suspicion of different connections is very political—not in the decisional but constitutive sense. Moreover, this creative process and its outputs rely on mechanisms of association, connection, filtering, and profiling, which end up categorizing some individuals as more suspect than others, more undesirable than others, and more threatening to the established order than others.

As a result, intelligence data are very rarely sources that permit for the establishment of causalities. Instead, they are the result of a process that seeks to legitimize or delegitimize suspicions held by intelligence actors, which rely solely on correlations and not on evidence, hence structural struggles and oppositions between judicial authorities and intelligence services. Intelligence agents make interpretations and draw portraits that create a form of spectacle, that these agents enact

with their lists of suspects and their operational analyses of possible futures. These interpretations represent the core of the files on which the various intelligence services are working.

One major difference, however, is that while these files were previously materially written and recorded on paper, they are now are digitally written and stored on computers. Does this material shift affect the way files are constituted and the modes of reasoning harbored by intelligence agents? Following the new materialism turn, some authors like Marieke de Goede argue that a profound transformation in the modes of reasoning that are at work in the construction of data, but this is not certain.[11] This new mode of reasoning only seems to touch at the fringes of the intelligence craft, observed amongst services that deal with the mobility of travelers or suspicious financial operations, but not so much amongst intelligence services themselves. As Laurent Bonelli and Francesco Ragazzi (2014) have pointed out, the conjectural reasoning described by Ginzburg (1980) remains fundamental to the practices of numerous agents that prefer the "low tech." So, it is not clear whether an "algorithmic" reasoning—which is based on large-scale correlations and a speculative reasoning specific to computer-based tools, instead of precise chains of causalities—could be opposed to and thought of to fully replace a conjectural reasoning. Drawing from our recent work, the dominant reflection and practice of intelligence agents continues to be organized around files or archives that are shared only by a small group of professionals. These documents are read by groups in connection to other information that is deemed secret and operational. The value of information derived from digital data is far from equal to that derived from "low tech" files. While some digital data may be useful for identification and localization, thereby getting past the quasi-structural anonymous character of the Internet, for many actors, the accumulation of heterogeneous data may contravene the understanding of actions. A reasoning based on algorithmic correlations is not able to capture individual targets, but instead creates culpability based on association. This is why a conjectural-based mode of reasoning may be complemented with speculative information and possibilities, but it will continue to remain the core of a profession that ultimately works to study, discipline, and eventually chastise individuals. Without this practice of indexing, the professional practice of intelligence would comprise of no more than the production of geopolitical generalizations of tendencies, the projection of futures yet with no operational capacity.

Though critical in many respects, a considerable amount of the surveillance studies literature has come to consider too quickly the production and traceability of data as an inevitable feature of modern society. This interpretation, however, tends to approach data as "flat," "rhizomatic," and constituted by the "exhaust data" diffused between all social and international worlds. While traceability may be automatized and facilitate rapid communication, some authors overgeneralize the characteristics of digital data, thereby overlooking the data constitution process, which can make them particular, fragment their meanings, or lead to their integration as political products. These studies thus homogenize the policies and practices

of different worlds of intelligence, ignoring vertical hierarchies, competitions, and differences in the technical methods of surveillance that they use (Amoore 2013, de Goede 2012).

Some monitoring methods are transversal and capable of making the use of such techniques more horizontal by facilitating the remote transmission of information. However, this does not necessarily result in the homogenization of the resources and logics of action driving what the agents are looking for in practical terms. Existing theories of electronic surveillance do not sufficiently distinguish between social worlds, which then leads to the assumption that the digital world has a uniform effect that is determined by the technology itself. For example, the production of digital data in the worlds of health, of international commerce, and of security do not generate the same effects in each respective social world, nor does it determine fixed relations between those worlds. The way that actors use new technologies depends on their past dispositions as well as on their capacity or willingness to transform paper data into computer data. With regard to the latter, this maneuver depends as much on one's technical capacities as it does their views on the importance of secrecy, confidentiality, and interest, which may dissuade some actors from stocking data or disseminating them. Data from the digital world thus affects forms of power and everyday politics, but the opposite is also equally true. Data are integrated into social worlds and into everyday practices only if they are seen by actors as helping them in their power struggles. This is best observed when new technologies are modelled or articulated in relation to existing customs and functions.

In sum, computer technology does not "revolutionize" technology so much as it moulds and adapts itself according to differentiated registers that are brought into the routine practices of different social worlds, which together constitute political intelligence. Moreover, computer technology can in fact reinforce divisions between actors and intensify existing points of tension by favouring certain actors over others. This privilege emanates from a general acceptance of the technical dimension of intelligence, whereby large-scale surveillance will be done remotely, with greater attention given to trend analysis that takes on a preventive and predictive dimension via use of "data derivative" operations.[12] These technological innovations thus favor actors who both use it to revitalize the contributions of agents and operations in the field and to value the accumulation of heterogenous data, which can nevertheless highlight correlations and the human mind would not have been capable of identifying by running algorithmic analyses of big data. This is at least what we have observed in narratives used by the agents who are most interested in defining intelligence as the anticipation of hostile acts, no matter where they come from. This mode of reasoning is probably seen as convincing for new entrants into the field of intelligence, as they can only act at a distance and don't have any field agents on the ground or "relays." However, this understanding of intelligence is far less convincing among an older generation of actors, who have operational capacities and who think in terms of adversaries, enemies, and possibly suspects. This second group of individuals is also quite suspicious of the deindividualization of crime, theologies on the possibility of knowing the

unknowable, and efforts to plan the future as if it were a future perfect. These symbolic struggles over the value and manner intelligence should be done then then determine what data "is."

In the next section, we will further study three professional intelligence groups by analyzing the structural modalities that define them as distinctive spaces, each defined by differentiated modes of socialization. Yet, each of these spaces is subject to the reformulation of their practices due to the socio-technical stakes of the digital, while simultaneously maintaining the ability the frame and structure the way that intelligence data is defined and practiced. So, when read in relational terms, some groups of actors are more or less distinct. When their work practices are transformed, actors are pushed to rethink their identities and power positions. In some cases, these reconfigurations may even challenge the strong felt sense of some that they live in a small world apart from the rest (i.e. the deep state), that has its own rules; a world wherein the use of violence in the name of state reason, secrecy, and impunity vis-à-vis the rule of law are the norm, and wherein these actors are committed to a sense of responsibility and loyalty to specific values that must be safeguarded and yet constantly adapted to practical challenges.

The transnational space of intelligence: the structural modalities and dispositions of actors regarding the digital

Intelligence studies has to a large extent suffered from a form of methodological nationalism that presupposes the existence of a national intelligence community, that collectively defends national interests, and implements national security strategies. From this standpoint, data interception is typically read according to two different modalities, one concerning citizen and the other regarding non-citizens. When it comes to the foreign services, the exchange of data is not considered to be routine practice. Many scholarly works give the impression that most intelligence services are reluctant to share data, notably due to their commitment to secrecy. When data exchanges do occur, authors argue that this is only happening between national intelligence services that have developed mutual trust in the fight against shared enemies, such as during the World War II and the Cold War. While not taking issue with some aspects of this reading that may be erroneous, it is at the very least far too monolithic.

To challenge this depiction, over the last couple of years, we have developed a Bourdieusian-inspired analysis of the contemporary international by pointing to transnational fields of power, their dynamics, and the dispositions that the actors enact when what is at stake is the management and extraction of data for purposes of constituting watch lists of suspects (Ben Jaffel 2018, Bigo 2016, Bonelli and Ragazzi 2014). Specifying the activities of intelligence services into the general management of unease by security professionals, the idea of a guild of extraction of sensitive information has been proposed to analyze the current composition and roles of the different intelligence services in countries claiming that they are democracies and that they accept the idea of limits to secret, intrusive practices

regarding the whole population, be it regarding their citizens or foreigners (Bigo 2018). As we shall see later in this chapter, our research shows that in this particular area of intelligence, we can observe specific social universes that relate to the objective properties of intelligence services and the manner that they construct intelligence data. It seems that in the case of intelligence practices linked to "global" counter-terrorism—and likely other missions—transnational logics and allegiances are stronger than purely national ones. As intelligence data are constituted by the types of questions that are raised and methods of reasoning that are used, data exchanges are actually more routine between services that belong to different countries but that share the same visions, know-how and practices concerning intelligence objectives than they are between services of the same country that deploy different or even complementary practical know-how. It is therefore necessary to understand the emergence of so-called trans-governmental networks between intelligence agencies, or more accurately transnational guilds that bring together agencies sharing the same specialized visions and whose agents have similar dispositions emanating from their socialization at work. It is therefore the professional habitus that can allow individuals and agencies to overcome national differences. In some cases, loyalties between agencies can be stronger than an institutional attachment to the political leaders of their country. To name just one example from a series of recent cases, in the context are nearly-routine exchanges, it seems that one department from the Bundesnachrichtendienst (BND) entrusted confidential information about the government of Angela Merkel and German politics to their National Security Agency (NSA) allies (Hegemann and Kahl 2016).

There is therefore a transnational intelligence space made up of different groups of national services that cooperate together in the management of digital data and of sensitive information, more generally. This transnational space is not structured and divided according to the national policies of governments—even if they do play a role by way of existing coordination structures. Instead, this space is defined by the types of information that actors seek out, the characteristics of these services, their composition, and their practices. So, what are the relationships between three different universes, which are each defined by different practices of intelligence as an occupation?

In order to clarify our working hypothesis, we have made a first attempt to map the transnational space of intelligence agencies in countries that agree to call themselves democracies and, at the same time, have regional or global foreign policy ambitions. Embracing a methodology that draws from the work of Pierre Bourdieu and international political sociology, we have used multiple correspondence analysis (MCA) to draw this space. As a methodological tool, MCA essentially allows us to mathematically distribute the services in a two-dimensional space, gathering them according to their most significant resemblances and differences. While allowing for a more systematic analysis of qualitative data collected in interviews, MCA is a heuristic tool for identifying groups, which are by no means randomly constituted (Le Roux and Rouanet 2010).

The sheer size of the American services, and their budget, explains their overwhelming engagement in cooperative initiatives and their role as the leaders of

networks that bring together countries from the so-called Global North that engage in activities beyond liberal democracies (Bigo, Bonelli, and Deltombe 2008). Since Edward Snowden's disclosures on the activities of the NSA, the Five Eyes has become the most well-known of such networks. It brings together agencies from the United States, Great Britain, Canada, Australia, and New Zealand that work with satellite, electronic, and internet communications data. This network is no longer limited to a group of five, as now it now includes more than a dozen intelligence agencies or sub-units from countries like France, Germany, Spain, and Sweden, which have all put in place infrastructures for the interception of data passing through submarine and terrestrial cables.[13] Based on the understanding that nowadays nine countries are involved in the Five Eyes Plus network, we have selected 25 agencies from the represented member countries, which all claim to be democracies and also have the ambition of playing a regional or global political role. Categories of intelligence service agencies include counter-terrorism and counter-intelligence services (police and non-police), external intelligence services, and, when they exist, the technical services dedicated to large-scale data interception. For the time being, military intelligence agencies working on military-specific issues have been excluded from this study, although they do sometimes play a role in diplomacy or even the fight against terrorism. Financial intelligence services also at times become involved in the fight against terrorism but have also been left out as their main activities relate to anti-money laundering. Border control agencies have also been excluded.

TEXTBOX 6.1 METHODOLOGICAL DETAILS

For the United States, we have selected the following agencies: National Security Agency (NSA), Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI)[14]; for Canada: Canadian Security Intelligence Service (CSIS) and Communications Security Establishment (CSE); for the United Kingdom: Counter Terrorism Command (CTC), Security Service (MI5), Secret Intelligence Service (SIS or MI6) and Government Communications Headquarters (GCHQ); for New Zealand: New Zealand Security Intelligence Service (NZSIS) and Government Communications Security Bureau (GCSB); for Australia: Australian Signals Directorate (ASD), Australian Security Intelligence Organisation (ASIO), and Australian Secret Intelligence Service (ASIS); for France: Direction générale de la Sécurité extérieure (DGSE), Direction générale de la Sécurité intérieure (DGSI) and Service central du renseignement territorial (SCRT); for Germany: Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV), and Bundeskriminalamt (BKA); for Spain: Centro Nacional de Inteligencia (CNI), Comisaría General de Información (CGI) and Servicio de Información de la Guardia Civil (SIGC); and for Sweden: Försvarets Radioanstalt (FRA) and Säkerhetspolisen (Säpo).

(continued)

(continued)

For each of these 25 services, we analysed the following 9 active variables:

1. The territory of competency, with three modalities (internal, external, internal/external);
2. The legal authority of agents, with two modalities (yes, no);
3. Operational capacities, that is whether the agency has agents on the ground, with two modalities (yes, no);
4. Objectives assigned to the services, with two modalities (the fight against internal threats; the defense of national interest—which includes espionage);
5. The number of personnel, with three modalities (0–1999, 2000–4999, 5000+);
6. Technologies used, with three modalities (human intelligence HUMINT, technological intelligence signals intelligence (SIGINT), and mixed capacities MIXED_TECH);
7. Hierarchical authority, with three modalities (Ministry of the Interior or Ministry of Justice; Ministry of Defense or Ministry of Foreign Affairs; Head of Government);
8. Engagement in counter-intelligence activities, with two modalities (yes, no); and lastly,
9. The ability to conduct clandestine or covert operations, with two modalities (yes, no).

As a result of our MCA analysis, we have produced two graphs. The first graph (Figure 6.1) shows the most significant modalities that structure this transnational intelligence space by exploring the types of capital different services possess as well as their organizational attributes and their institutional objectives. The second graph (Figure 6.2) is based on an analysis of the objective properties of agencies, which allows for the visualization of specific subgroups or universes based on the identification of proximities and distances between the various services.

Axes 1 and 2 explain roughly 64% of associations between our nine categorical variables (respectively 44.03% for Axis 1 and 19.98% for Axis 2). On Axis 1, the most contributing variables on the left side of the graph (negative values) include domestic threats (7.8%), internal territories of competency (7.8%), the absence of clandestine operations (6.1%), counter-espionage activity (4.5%), attachment to the Ministries of the Interior or of Justice (6.1%), judicial authority (4.4%), and human intelligence (4.6%). The contributing variables run in opposition to those that appear on the right side of the graph (positive values), which include national interest (8.5%), internal/external territories of competency (7%), clandestine operations (7.8%), attachment to the Ministries of Defense or of Foreign Affairs (6%), technological intelligence (7%), and mixed human/technological intelligence (1.5%).

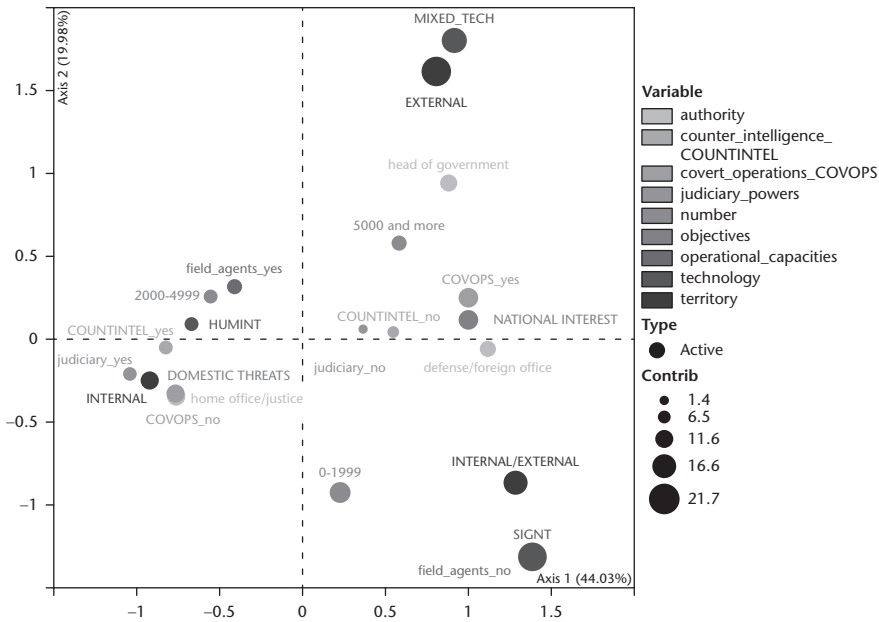

FIGURE 6.1 Most Contributing Variables on Axes 1 and 2 of the MCA

On Axis 2, the most contributing variables on the bottom part of the graph (negative values) include technological intelligence (12.7%), the absence of field agents (12.7%), and internal/external territories of competency (7.5%). In contrast, the most contributing variables on the top part of the graph (positive values) include mixed human/technological intelligence (14.6%), the presence of field agents (4%), and external territories of competency (19.7%).

This distribution of the properties and dispositions that define each of the intelligence service agencies than make it possible to observe the proximities and distances between those institutional actors in space. As shown in Figure 6.2, this exercise allows for the identification of three distinct sets or groups of actors.

The first pole (1), situated on the left in the middle of the table, represents a space of proximity between services that primarily recruit police and prioritize internal security issues. This set of actors is most concerned with internal threats. At times, however, they may develop forms of external actions and cooperation in order to prevent internal threats instigated by actors coming from abroad. They conduct two different categories of missions: (1) political subversion, which includes but is not limited to anti-terrorism; and (2) counter-intelligence. This first subgroup is also defined by their affiliation with Ministries of the Interior or of Justice.

Within this first group, we can identify two subsets: 1) agencies that have at least partial judicial authority (law enforcement agencies) and 2), which do not

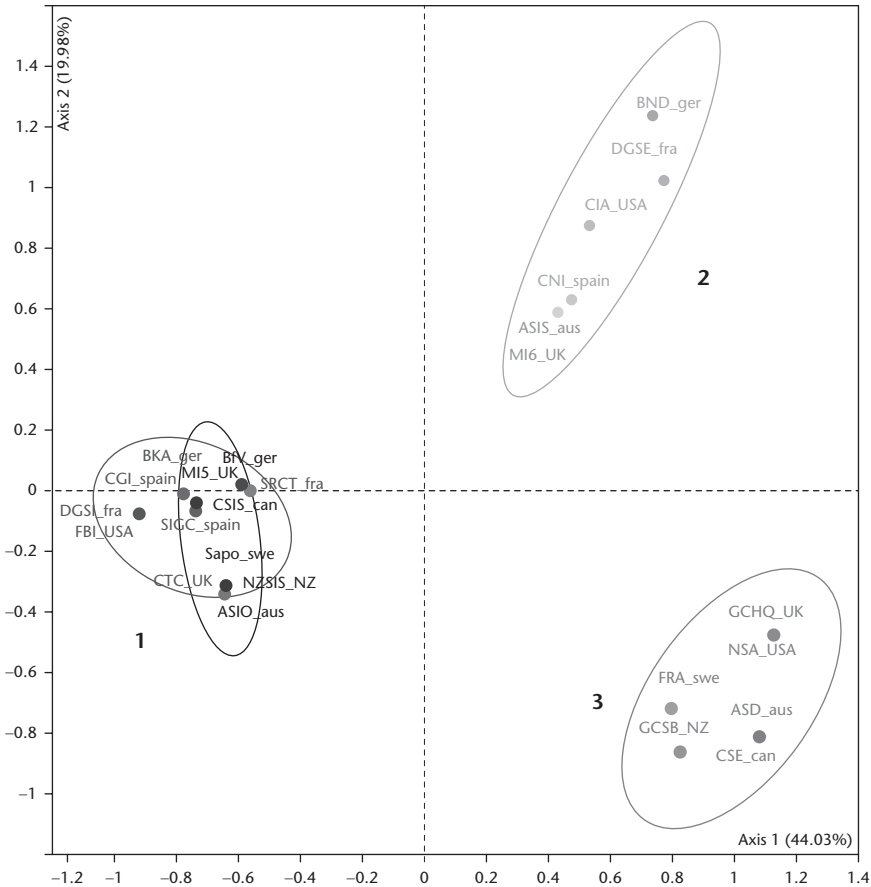

FIGURE 6.2 The Space of Institutional Positions

possess judicial authority. With respect to the first subset, we observe the presence of the German BKA, the Spanish CGI and SIGC, the American FBI, and the French DGSI. Situated in the second subset are the German BfV, the British MI5 and CLC, the Swedish Säpo, the Canadian CSIS, the Australian ASIO, the New Zealand NZSIS, and the French SCRT. Regarding the relationship of these agencies with digital and algorithmic reasonings, qualitative interviews with service agents suggest that they see the evolution of new information and communication technologies (NICTs) as both a constraint and a resource. On the one hand, NICTs are perceived as a constraint because of the flows of information that are now generated by individuals. Indeed, surveillance targets produce far more data today than they did in the past. The volume of available data means that qualitative analyses are a priori not possible. Yet, the amount of digital traces left by individuals is also a valuable resource for intelligence officers. For example,

in addition to telephone calls, SMS messages can be used to demonstrate the frequency of contact between individuals who previously sued other communication channels and who would not have otherwise been noticed. Additionally, digital communication makes it possible to geolocate individuals and to confirm the co-presence of two people in the same place at the same time. Similarly, the consultation and updating of information via Facebook also makes it possible to locate the internet user in question. While no one complains about the wealth of data that is available, these intelligence agencies often pinpoint the question of how to exploit this data as a major obstacle. One possibility is the use of computer software to filter the massive influx of digital data. Some software can also be used to draw graphs of relations based, for example, on correlations between called numbers and localizations in fixed time slots. These graphs can be cross-checked with elements collected using other investigation methods (i.e. witness hearings, interrogations, searches, etc.). It is only as of late, however, that digital data have begun to be used. Since their realization of the potential use they could make of digital data, internal intelligence services have of course adapted their practices to technological evolutions and corresponding societal transitions. However, new technologies have not destabilized the work logics of these agencies. This can be explained by the fact that while the studied agencies have increased staff numbers and strengthened units dedicated to Islamic political violence, they have only very marginally recruited new technological specialists. Therefore, they continue to principally recruit and integrate police offers, agents, and analysts whose skillsets correspond to more traditional intelligence occupational groups. Practical knowledge on how to deal with human sources of information (i.e. informants), shadow suspects, or carry out interrogations continues to be dominant. The most technical tasks can instead be subcontracted to outside parties. For example, in France, geolocalization analyses are entrusted to authorized private companies, which examine the data that has been collected following judicial requisitions and then submit reports to intelligence agents. In this case, digital data actually support and nourish long-term modes of reasoning and institutional practices.

This first subset of actors is clearly distinguished from the second pole (2), which predominately includes agencies that recruit military actors into their ranks, have the operational capacity to missions on external territories, and use espionage techniques. This second subset includes agencies like the CIA and other external service agencies, such as the Spanish CNI, the British MI6, and the Australian ASIS—all situated at the bottom of the eclipse—that rely more on human intelligence. Agencies like the French DGSE and the German BND share similar characteristics to the aforementioned agencies; however, in recent years, these two institutional actors have developed important data interception capabilities within specific departments that are dedicated to the interception of digital data so as to monitor social networks. Yet, they all remain under the general supervision of the Ministry of Defense or of Foreign Affairs. They also tend to see internal intelligence services as potential "clients," which can make specific service requests

to this second subset of actors. Amongst this subgroup, computer-based tools are predominately used to geolocate external targets, to keep in touch with overseas agents, and, occasionally, to drive armed drones in particular operational contexts. When carrying out politically costly operations, big data should thus not create confusion or inaccuracy in hitting targets, meaning that approximation is not really allowed. Digital data is not totally dismissed but is instead only used as a tool of exploration as it is responsibility on the ground, which comes before anything else.

The third pole (3) indicates the emergence of an autonomous subset of SIGINT-Internet agencies. The specificity of this group is that included agencies lack operational agents. Instead, these agencies provide other national intelligence services, both internal and external agencies, with the satellite, terrestrial, and digital data they need. This pole consists almost exclusively of Five Eyes agencies, with the exception of the Swedish FRA, which more or less joined the Five Eyes because of its role in the interception of terrestrial and submarine international cables going to and from Russia. This particular space is at the origins of a new mode of reasoning that delegitimized the effectiveness of traditional forms of intelligence when faced with small, unknown groups. Before the 2000s, Admiral Poindexeter alluded to the development of a global data system identifying targets not based on the pinpointing of individuals already known to intelligence services, but instead through the detection of behavior abnormalities that do not correspond to system logics. Initially called Total Information Awareness (TIA), this mode of reasoning was subsequently referred to as "collect it all" for detecting "weak signal" (i.e. a needle in a haystack), which consists of grouping individuals who did not necessarily know each other together into collectives based on their association with a specific risk profile (Ericson and Haggerty 2006, Harris 2010, Murray 2010). Recalled by its old friends inside the new administration, following 2001, Poindexeter had the means to realize this project of TIA, but the US Senate rejected it at the time for other reasons. Only a small part of it was enforced. Since, however, with its extraordinary capacity in terms of staff and budget, the NSA has once again embarked itself on this journey. But this time, the NSA has brought in the private sector, from data mining software companies and internet providers (i.e. the GAFAM) to telephone companies like Verizon.

Following the Snowden disclosures about the practices and ambitions that guided the NSA, we now know that several intelligence agencies, including the British GCHQ, argued that the potential surveillance of all would never work in operational terms. Instead, digital data collection needed to target small groups so that it could be complemented by human surveillance, judged as more effective. Other services followed the GCHQ in its strategy of recalibration. For example, it appears that services involved in the interception of sensitive information wanted to obtain the necessary legal facilities to be able to undertake large-scale surveillance of potentially-dangerous groups by throwing a "broad net," while simultaneously rejecting an algorithmic mode of reasoning. Interestingly, it is more financial surveillance services or, more recently, services controlling what type of people are authorized to cross borders—that is the newcomers in the intelligence

field—who make claims to being able to handle large amounts of data and persons by using weak signal approaches in order to predict their behaviour. According to them, the ethical-political costs of making false positives are not so important when dealing with suspected persons, they just have to "wait longer" on queuing.

This distribution in a two-dimensional space—which is not random—allows us to group together services from different countries according to the structural proximity of the type of institutional objectives they defend and the know-how they employ. In doing so, this method allows us to visualize cleavages between services from the same country, thereby contrasted to the dominant national-territorial representation of intelligence agencies. As this mapping exercise suggests, the usual discourses on mutual trust only operate between agencies with similar or identical structural positions. The structuration of two of the three poles around the divide between external security and internal security is a rather historically trivial one. However, the emergence of a third pole around SIGINT-Internet agencies may play a considerable role in the destabilization of the status quo if this specific universe begins to successfully impose its definition of intelligence data according to its own practices. Such a reconfiguration would also require the support of politicians, which to a large extent correlates with preventive and predictive political discourses. So, it is essentially in the 2000s that computerization and digital technologies introduced a new arc of tensions into the transnational intelligence space over who produces, exchanges, and analyzes data. Such tensions, however, already existed between intelligence professionals recruited from the military and those recruited from the police. Yet, it is the end of bipolarity that put into question and challenged existing rules and practices of espionage and counterintelligence.

To complement these findings, it would undoubtedly be interesting to know the extent to which politicians and top civil servants are able to impose imperatives of fusion, homogenization, or strict complementarity with regards to the practices of these three poles. Or whether, instead, these poles are autotomizing and create a transnational space of solidarity, complicity. Intelligence agencies, nevertheless, are to some extent subject to the will of political leaders who have control over budgetary and staff allocations. This effect of political control is more visible in countries that have put in place strong coordination structures. For example, the role of the Joint Intelligence Committee (JIC) in the United Kingdom has been to create and reproduce strong cohesions between national intelligence agencies exactly to avoid transnational struggles and alliances. Yet, as shown in the Feinstein report, other countries, and especially the US, have encouraged these transnational games in order to maintain a shroud of opacity around the actions of typically the least supervised external actions. As we have discussed elsewhere, this phenomenon of dynamics interaction means that in some cases the failures of some represent conditions of happiness for others. This is essentially what happened with the failure and controversy around the practices of torture at distance by the CIA and its accomplices[15]. This allowed for the delegitimization of the use of foreign military services in offensive counter-terrorism operations and allows

for less violent means with the NSA's remote action model, which relied on the identification of terrorists within social networks (numeric and non-numeric) and the algorithmic identification of behavior abnormalities. In this case, the failure of a specific subset of external services and the inefficiency of the strategies they used, led to international disproval, which essentially worked to reinforce the decisions to strengthen SIGINT-Internet intelligence services by giving them the resources they had long been asking for.

Concluding remarks

So, what are the results of our Bourdieusian international political sociology-inspired analysis? First, our analysis disproves the existence of a homogenous world (or community) of intelligence wherein all national agencies are complimentary to one another and wherein the boundaries of their missions are clearly defined by the law or by political authority. Our analysis of the constitutive practices of intelligence actors and their meaning-makings of data has destabilized the illusionary idea of the intelligence community as a single world united by common surveillance techniques that are changing the sense of security (and leading globally to speculation). Logics of action cut across and transgress distinctions between the internal and the external, the national and the foreigner. The apparent unity of a national intelligence community in each country must therefore be deconstructed to highlight the relationships that exist between different poles. These relationships are read in terms of how agencies construct intelligence data-suspect for different purposes, how they negotiate amongst themselves as well as with politicians about what approaches should be considered as the most appropriate. These agencies often compete with one another, not only within national fields but also within a transnational space where solidarities—which may still have a hierarchical nature[16]—are made between agencies deploying more or less identical forms of know-how. This reality undermines the dominant and almost exclusive discourse that national security is a source of legitimate suspicion, making it necessary to evoke a narrative on the prevention of attacks and to design global security policies against terrorism. Regarding the former, the more such narratives are questioned, the more it becomes tempting to present these transformations as the result of the emergence of the internet and digital evaluations, even though in fact this shift is the result of political transformations.

Distinctive logics defining cleavages between agencies are not pathologies. Rather, these differences are inherent to the very structure of the intelligence game. Efforts to merge services may not only reinforce inefficiency by reorganizing and destabilizing relations between different types of know-how but may also lead to the creation of hegemonic structures that will impose singular understandings of what data are and for what ends they should be used. This would undermine the plurality of interpretations as well as the richness of debates and discussions. To speak about these differentiated logics is not a return to the image of a tuff war. Instead, our aim is to provide a deeper understanding of the practices of

these agencies, which goes beyond official organizational charts given by political structures or communications agencies. These distinctive logics may also be reproduced within agencies, depending on which recruitment criteria and forms of socialization are privileged. Some intelligence agencies have opted for strong internal homogeneity, trusting only one type of profession or graduates of a single training school, in order to build solidarity. Others have inversely chosen to take on a diverse range of missions and thereby recruit people who have different characteristics in terms of training, gender, violence management practices, and use of numeric technologies. For example, a network engineer and a policeman obviously do not have the same relation to the digital, but they may nonetheless work for the same institution. While all dealing in some way with data, having know-how on how to use data technologies as a user should not be confused with skills required by software designer or by someone who creates profiles based on algorithms. The same goes for the latter, who build populations of target categories, and those who aspire to achieve the same mission, but do so by generating files on precise individuals and organizations, giving great importance to the individual psychologies and trajectories. These different types of intelligence agents all live and work more as analysts than as combatants, which makes them different from those that are deployed "on the ground" to use coercive means in foreign lands. Depending on one's training, the resources at the disposal of agencies and their legitimacy of their actions, resources, and capitals are unevenly distributed amongst actors situated in the intelligence space.

As we have seen in our interviews, it seems that digital techniques are put to use in two ways. Firstly, they can be used in support of the more traditional framework of conjectural reasoning in order to provide necessary evidence for the judiciary. Secondly, they can also be used to impose a preventive and predictive reasoning. The logics and mechanisms of reasoning that are specific to each universe and its actors—be it the police, military, or communications—are therefore to be considered more important than the technologies themselves. In other words, it is not computer technologies that play a role on their own, but rather it is the entry of computer scientists into intelligence circles and the manner in which they frame problems in relation to technology. It is for this reason that the entry of new technologies should not be overestimated (as some interpretations tend to do). Such assumptions tell us little about the effects of technology on practices. For example, actors may continue to use old paper filed while simultaneously mobilizing computer-based tools simply for their cross-referencing speed. Digital technologies may also be employed in the technological regulation of databases and their interoperability. This exercise imposes certain characteristics and criteria on the formatting of data, which is helpful if they are to be exchanged on a regular basis and in large quantities. Digital technologies may come to play a significant role within specialized departments of the military or police services that are dedicated to identification tasks and are supervised by new technical actors. Beyond recurring tensions and disputes precisely on the performativity of data, clashes may also arise between agents with different dispositions. More precisely, in worlds of

intelligence that previously worked primarily with non-digital information and data, the introduction of new techniques—including sophisticated ones—will not necessarily change existing modes of reasoning. It basically takes time for digital technologies professionals to successfully imposer their own interests and professional visions on more traditional actors situated in the intelligence field. However, private companies have played a substantial role in the recruitment of IT specialists, network engineers, data analysts, integration platform software designers, language and coding specialists, cryptologists, and mathematicians tasked with creating or combining algorithms that play on the recognition of weak signals in long series. While the individuals are employed by private actors with the overall ambition of selling products and services, as they increase in number, they begin to more significantly populate a world that previously consisted almost exclusively of police, gendarmes, military, internal intelligence specialists, and external border guards. As a result, these new actors change the rules of the game of these social universes, and in changing rules and habits, they end up changing certain dispositions. This is notably the case in the establishment of good working relations between the world of private contractors and that of public service agents.

Issues and tensions raised by the emergence of this new category of sensitive information professionals have therefore not had a uniform, even impact across different intelligence universes. However, in terms of their transversal impact, this group of professionals has nonetheless attracted the attention of those increasingly supporting preventive and predictive approaches. And together, they have defended the idea that it is only the potentialities and possibilities that digital data bring to the world of intelligence that can satisfy the desires of politicians, the fear of populations, and the interests of security apparatuses in the remote management of populations. Now an essential element in the world of intelligence and surveillance, the capacities of digital techniques nonetheless continue to be debated, all the while linking high politics with the everyday and redefining the way national security is understood.

Notes

1 The terminology used by the services is "raw data" for the data that are generated either by a research they launch or by what is called "captured data", usually by machines or terminals, as a secondary function. For example, cash registers, smartphones, and speedometers serve a main function but may collect data as a secondary task. In informatics, specialists called it "exhaust" data.
2 See note 7 for an explanation of this term.
3 Regarding the notion of field of professionals of sensitive information see Bigo 2018.
4 See in this book the chapter by Ronald J. Diebert and Lou W. Pauly.
5 Symbolically, the attempt to create a distinction between meta-data and data is a way to justify that data are not the property of the internet-user. It justifies exploitation of data and their circulation, compilation, disaggregation and reaggregation outside the knowledge of the individual at the source of the data.
6 On October 19, 2016, the Court of Justice of the European Union (CJEU) decided that the dynamic IP address of a website visitor is "personal data" under Directive 95/46EC (Data Protection Directive) in the hands of a website operator that has the means to compel an internet service provider to identify an individual based on the IP address.

7 The *encomienda* was a forced labor system prevalent in the Spanish Empire, whereby natives were stripped of their property rights. The Spanish Crown gave parcels of land to private individuals that worked in its name, and with that land additional natives who, in theory, worked in exchange for protection and their religious conversion. The relationship between intelligence agencies, the Big Four, and individuals is comparable to the *encomienda* system in so far as internet users are refused ownership to their own data and the work that they do to produce and diffuse them.
8 See Engin Isin and Evelyn Ruppert in this book.
9 The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas. See Elspeth Guild in this book.
10 The term performance has many different meanings in English, which converge with what we insist on. Performance means achievement simultaneously results, outcomes, findings, but also benefit, delivery, and show, spectacle. In some ways the three connotations are simultaneously true.
11 Most debates on intelligence data exchange are based on the *potential* offered by technology rather than the actual practices of intelligence service agents. This is also the case regarding the regulation of technology and road regulation. For example, it is not because a vehicle can travel at a constant speed of 200 kilometers per hour that it is allowed to do so and that the driver does so. The legal system is there to set limits and restrict technical potentialities. Authors like Louise Amoore and Marieke de Goede have sometimes framed practices and potentialities in equal terms, while equating present circumstances with emerging trends. This has led to an overly programmatic view of intelligence services and their intentions. This is demonstrated in the way that newcomers are treated as emblematic of paradigmatic changes, when in fact there are struggles against the transformations brought forth by new actors, as is the case regarding the validity of the accumulation and retention of data alongside the accuracy of predictive algorithms. See notably de Goede 2008 and Amoore 2011.
12 The data derivative comes into being from an amalgam of disaggregated data reaggregated via mobile algorithm-based association rules and visualized in 'real time' as risk map, score or color-coded flag. As explained by Louise Amoore: It is not that derivative forms supersede disciplinary data modes, and indeed among the reaggregated data elements are conventionally collected visa and passport data, but rather that the relation between the elements is itself changed.
13 Some journalists have spoken of the 9-Eyes, with the addition of Sweden, France, Spain and Germany; or even of the 14-Eyes with Belgium, the Netherlands, Italy, Norway and Denmark.
14 Given the range of missions conducted by the FBI—spanning from criminal police work to internal intelligence—we have only taken into account 3,600 agents situated in the Counterterrorism Division.
15 Guild, Elspeth, Didier Bigo, and Mark Gibney, eds. *Extraordinary Rendition: Addressing the Challenges of Accountability*. Routledge, 2018.
16 For example, such a hierarchy is established by the fact that the NSA has more staff at its disposition than all of the European services combined.

Bibliography

Amoore, L. 2011. Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28(6), 24–43.
Amoore, L. 2013. *The Politics of Possibility: Risk and Security beyond Probability*. Duke University Press.

Bauman, Z., and D. Lyon. 2013. *Liquid Surveillance: A Conversation*. John Wiley & Sons.
Ben Jaffel, H. 2018. Britain in Europe, Europe in Britain: The Field of Anti-Terrorism Intelligence Cooperation. PhD dissertation, King's College London.
Bigo, D. 2008. "Globalized (In)Security: The field and the Ban-Opticon", in Bigo, D. and Tsoukala, A. (eds.), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*. Routledge 10–48.
Bigo, D. 2012. "Security, surveillance and democracy" in Ball, K. and Lyon, D. (eds.), *Routledge Handbook of Surveillance Studies*. 277–285. Routledge.
Bigo, D. 2013. "Sécurité maximale et prévention? La matrice du futur antérieur et ses grilles" In Cassin B., Derrière les grilles: sortir du tout évaluation, 111–138. Fayard.
Bigo, D. 2016. Sociology of Transnational Guilds. *International Political Sociology* 10(4), 398–416.
Bigo, D. 2018. "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, M. C., and Vieth, K. (eds.), *Research Handbook on Human Rights and Digital Technology*. Edward Elgar.
Bigo, D., L. Bonelli, and T. Deltombe. 2008, Au nom du 11 septembre: Les démocratie à l'épreuve de l'anti-terrorisme, La Découverte.
Bonelli, L., and F. Ragazzi. 2014. Low-tech security: Files, notes, and memos as technologies of anticipation. *Security Dialogue* 45, 476–493.
De Goede, M. 2008. The politics of pre-emption and the war on terror in Europe. *European Journal of International Relations* 14(1), 161–185.
De Goede, M. 2012. *Speculative Security: The Politics of Pursuing Terrorist Monies*. University of Minnesota Press
Ericson, R. V., and K. D. Haggerty. 2006. *The New Politics of Surveillance and Visibility*. University of Toronto Press.
Gill, P., and M. Phythian. 2016. What is intelligence studies? *The International Journal of Intelligence, Security, and Public Affairs*, 18(1), 5–19.
Ginzburg, C. 1980. Morelli, Freud and Sherlock Holmes: Clues and scientific method. *History Workshop* 9, 5–36.
Guild, E., D. Bigo, and M. Gibney, eds. 2018. *Extraordinary Rendition: Addressing the Challenges of Accountability*. Routledge.
Harris, S. 2010. *The Watchers: The Rise of America's Surveillance State*. Penguin.
Hegemann, H. and M. Kahl. 2016. Re-Politisierung der Sicherheit? *ZIB Zeitschrift für Internationale Beziehungen* 23(2), 6–41.
Lehr, P. 2019. *Counter-Terrorism Technologies: A Critical Assessment*. Springer.
Le Roux, B. and H. Rouanet. 2010. *Multiple Correspondence Analysis*. Sage Publications.
McElreath, D. H., M. Graves and C. J. Jensen III. 2017. *Introduction to Intelligence Studies*. Routledge.
Murphy, C. 2016. *Competitive Intelligence: Gathering, Analysing and Putting it to Work*. Routledge.
Murray, N. 2010. Profiling in the age of total information awareness. *Race & Class* 52(2), 3–24.