Shared secrecy in a digital age and a transnational world

Didier Bigo

INTELLIGENCE AND NATIONAL SECURITY
2019, VOL. 34, NO. 3, 379–394
https://doi.org/10.1080/02684527.2019.1553703

Routledge
Taylor & Francis Group

ARTICLE

Shared secrecy in a digital age and a transnational world

Didier Bigo

ABSTRACT

This article examines the notion of shared secrets and the procedures by which secrecy is not the opposite of exchange of information, but the restriction of it to a certain 'circle' of people and the maintenance of others in ignorance. It creates corridors depending on the objectives of secret information, the persons having access, and the knowledge of this access by other people. Shared secrecy has been considered as an exception to common practice, but it has changed in scale with digitization and transnationalization of information, especially when suspicion is becoming used in statistical terms for prevention purposes.

Sharing secret information about suspects left in ignorance: mechanisms of transnational logics of intelligence in a digital world

I begin this article by investigating the relations between secret information, national security and the common understanding of secret intelligence as an exclusive product delivered by the intelligence community regarding the politicians who decide what policy to follow regarding threats, risks and vulnerabilities. I cross-examine the strong relation of exclusivity of secrecy between the national intelligence agencies and their reluctance to share information with foreign countries. From the Snowden disclosures of the National Security Agency (NSA) practices as the leader of an alliance composed of different SIGINT-internet intelligence services (the so-called Five Eyes), we have evidence of the fact that information which has been intercepted in the digital space concerning localization of individuals and things, identification of these individuals by interconnections of different data pertaining to various bureaucracies and private companies, as well as information on social networks, is shared between different foreign countries and sometimes for very different purposes. I propose the notion of *shared secret information*, even if it looks like a paradox, to understand what is at stake today in a world where the argument of a global insecurity pushes the different services to transfer some information to their 'counterparts' in allied countries, and the impact of this transnationalization of 'national' security when the digital world destabilize the state boundaries. I analyze here the notion of shared secrecy in the field of exchange of information through the procedures by which a specific product of a logic of doubt regarding marginal behaviours (as if they were a sign of guiltiness), produces a list of suspects, which have no right to know why and how they became suspects. In that case, secrecy is not the strict opposite of exchange of information, but the result of the collaboration of bureaucracies allowing the restriction to a certain 'circle' of people with authority to maintain the others in ignorance of the criteria of this suspicion and their modalities of evaluation as well as the techniques they use. This creates a problem regarding rule of Law and democratic principles, and supposes new discussions about the boundaries between secrecy, security, publicity and scrutiny.

As we will see, shared secrecy is therefore not a new phenomenon opposed to exclusive secrecy, but a long practice of communicating and exchanging information between different secret services organized into more or less informal alliances that simultaneously collaborate on

CONTACT Didier Bigo didier.bigo.conflits@gmail.com

certain topics while competing in others, or even on the same ones. This so-called *coopetition* was regulated when intelligence was centrally about spying and counter-spying around military state secrets. However, the scale of sharing secret information has been radically transformed when they have addressed individuals at the world scale and when the digitization of the world has simultaneously allowed them to follow the traces left by mobile or chatting individuals in the digital realm. In addition, nowadays the de-monopolization of intelligence practices correlated with the easiness to put others under surveillance has challenged the boundaries of the professionals of secrets. Private companies and individuals have used for their own purpose everyday forms of digital surveillance. Shared secrecy has therefore reconfigured the field of practices of secret services far beyond their official denominations and has included more and more traditional bureaucracies working at the borders, on finance, on insurance, as well as many private companies, including those who are not internet providers, but simply taken into the unbound securitization of everyday life. If many scholars accept this increase of the scale of exchange of secret information between an impressive range of actors, they still disagree on the reasons of such an increase. For some, this is the result of the rise of insecurities beginning with transnational terrorist activities, organized crime and infiltration of people on the move by these dangerous actors. Without denying that statistically it may exist, most researchers consider that it is ultra-marginal, and that the dynamics of institutions in their competitions and alliances are not reducible to a functionalist answer from external threats. They insist on the existence of a field of security professionals which exist as such, and not only as the addition of national fields. This field is organized around services who have the same kind of techniques, methods and ethos. They are indigenously called 'natural counterparts'. This is in our view one key element to understand the development of these different channels, 'corridors' of segmented information that nevertheless travel globally as secret information shared by many, even if it is in an asymmetric way.

So, if secret intelligence is not any longer an exclusive property of a national community of intelligence, who is now communicating with whom and on what type of secret intelligence information? How and for what purposes? We are clearly beyond small numbers in circulation, we have a mass production of 'shared secrets'. The argument of national security has obscured this phenomenon for a while. As long as this practice of exchanging secret information between different services pertaining to different countries was restricted to a world of spying and counter-spying, i.e. a small world of professionals that supposedly knew each other, it was possible to maintain the belief of a national exclusivity. But the targets of these exchanges of intercepted communication regarding individuals or behaviours of non-identified persons has become so intense, and so many observers have spoken of mass surveillance to characterize this large-scale intrusive practice of building intelligence data on list of suspects, that it cannot be sustained anymore.

In a second part, I detail the change of configuration of the field of the professionals of secretive information which is correlated with the change of scale of shared information and the transformation of the boundaries of this field under the effects coming from its digitization, its privatization and its transnationalization. I indicate that the current game of intelligence gathering is not led only by the games of spying but by its penetration to the intimacy of so many individuals that are objects of suspicion by correlations of profiles which are sometimes not associated with a reasonable cause and generate arbitrariness.[1] But, in my view, if the extension of the field of shared secrecy and intelligence is so advanced, it is not at the same moment a homogeneous phenomenon leading towards a trend of a global society of surveillance. The analysis of intelligence service actors, their social use of technologies, their own beliefs, show that old and new actors, heirs and pretenders, compete between themselves, and disagree on the limits, the boundaries of legitimate actions of an economy of doubt expanding to millions of people put under suspicion beyond fact finding, on the basis of correlations structured by algorithms based themselves on the flow of data considered as shared secret information. In democratic societies, it implies a public debate about these limits. Publicity, scrutiny and secrecy have to be held simultaneously, and strategies of communication are now crucial for secret services. They have to explain their policies, not in detail,

but on the principles by which they conduct them. Karen Lund Petersen suggests a change in the mode of communication by intelligence services with their audiences. They may be considered as earmarked only for the government and completed only for those who are elaborating national security decisions. In this vision sharing information is limited and needs to be constructed on an ad hoc base. The idea of public scrutiny is considered as antithetic with the role of secret services, and numerous publications of intelligence services insist on the fact that their purpose is to exist outside of the realm of the rule of Law, to do what is expressly forbidden by law but necessary for the country. Public scrutiny has therefore no place, control has to be done internally and by those who have given orders in case of malpractices. Nevertheless, at least two new paradigms emerge where the public plays a role. In the post-war on terror, it has been considered necessary to increase both the number of players and scrutiny. Information sharing within the sphere of the different agencies collecting information for the common struggle against terrorism, especially jihadism, has decompartmentalised the search for national interest and promoted more automated forms of data sharing with a large number of partners beyond traditional alliances, and encouraged a policy explaining to the public what secret services are doing for their protection and why they are cooperating between them. Beyond this more 'pedagogical' approach, a third model even suggests that the citizen collaborate and co-produce information in an encompassing view of protection against catastrophic events and organisation of resilience. This co-production may lead in that case to more scrutiny and oversight[2]

Secrecy today: reformulating the question

Against a certain common sense, secrets are not a way to mask information to everyone and a form of solipsism, they are always shared and almost always partially disclosed to create an attraction around their importance. A secret forgotten by everyone is not any more a secret. Procedures to restrict access are central as they mask part of the content but advertise the existence of a secret. Procedures therefore organise asymmetrical relations and provide for a group a certain amount of symbolic power by distributing the information along a continuum going from who is completely ignorant to who is less ignorant, instead of creating an impassable border between ignorance and knowledge. Everybody knows a bit of secrecy but not everything.

This creates an internal hierarchy and differentiates the insiders and the outsiders on the basis of the subtraction of a document or just a couple of relevant lines to the list of available documents. The social relation of secrecy is therefore functioning as a hierarchy inside those who share the knowledge that a secret exists, and this hierarchy is certainly more important for the everyday of the actors than the barrier opposing all of them to the people who ignore completely the existence of a relevant secret.

Secrecy is therefore like a pole in a magnetic field attracting people of different origins, and different services. It creates a form of 'complicity' between them and is a marker of objective relations into a field of practices. In the words of David Omand: 'If all knowledge is power, secret knowledge is turbo-charged power. It is in the nature of secret intelligence that it can be used to ensure access to policy-makers and build influence and prestige for the collecting agency. The risks in terms of over-promising to buy favour and then under-delivering, as seems to have been the case with Iraq WMD intelligence, become all the greater if secrecy is being used to reinforce personal relationships and ensure face-time with the leader'.[3] In his narrative the national committee (here the Joint Intelligence Committee) is a crucial mediator for the exchange, but while that may exist in the UK, our research shows that in other countries the mediation is almost inefficient or even non-existent despite the discourse of collaboration or the existence of formal fusion centres that replicate old data analysis instead of contributing to the production of timely intelligence. In other countries like the US, France, Germany, Spain, Italy, it seems that the different agencies exchange more with their foreign counterparts than with the national agencies doing data interception by other means, and who have limited trust in the other methods. The level of competition between national intelligence services seems higher and the collaboration weaker.

In addition, this type of sharing of secret information works only if the participants of all the continuum are eager to know, if they believe in the value of secrecy. If they do not, if they consider the secret superfluous, the information not valuable for their own purposes, the power based on the differential of (lack of) knowledge disappears.

So, if secrecy, as we proposed is not a technical element, but a politics, then secrecy is used and considered as a form of symbolic power having strong effects on the positions of the actors, vis a vis each other. The resource is not concentrated on a specific case or document giving access to certain knowledge, it is the authority emerging from the right to know which is important, and which is sometimes different from the bureaucratic structure itself. To say that differently, it is not because the absence of knowledge reveals an unknown which, once known, will give an additional reality, a key to understand the world, that secrecy is powerful. The discovery of a secret is rarely changing a situation in itself. What count in fact, are the transformations by which the procedures of secrecy are operating or not by selecting who is entitled to claim that he knows 'things' that the others don't know, and that he cannot reveal these elements for their own good, as it may endanger them. Trust in him, in his role of protector by those who know less is therefore necessary (and even more inside the services).

Secrecy is therefore not the object of the different intelligence services but the architecture, the exoskeleton which built internal hierarchies as a result of the performative claims and rituals around the right of access and the proclamation that a specific element has to be classified. This is what constructs the chains of dependence between the actors of the field and these hierarchies are also what destroy the so-called sense of a 'community of intelligence' where equality inter pares (experts) would be the rule. Part of the life of secret services is organised along this discrimination which also directs the sense of allegiance, which may differ from the official flow-chart.

Shared secrets in transnational alliance: yes to exchange of information but not everything is for your eyes

It would be an illusion to think that national security acquired by national means only has been the rule until recently. National security has almost always been acquired through transnational types of collaboration. But a nationalist take on this topic which overvalues the coherence of the government and the national state as 'one' actor has led to this illusion (in the Bourdieusian sense) of a national sovereignty on the data regime of intelligence, which in fact does not exist in practice, but is repeated again and again as a form of justification of the intrusive practices, especially regarding the fact that they are and were addressed centrally towards foreigners. This justification by the national means only of capture of data exists as a categorical imperative for a narrative valorising the legitimation of national security over the rule of law as it existentializes some events and masks others. In practice, sharing information between different national services of different countries has been a very common practice. Different governments had to exchange different bits of information to make sense of the overall picture. The first books on the raison d'Etat in the 16th century explain immediately the advantages of sharing information, but the IR narrative of the mid 1960s has invisibilized these sources and insisted that 'intelligence services' don't share information abroad, that they capitalise them and enter into collaboration only at the national level and rarely, selectively, with foreign allies. But it is obvious that the two phenomena are not opposed. Secrecy works very well with exchange, and not only with a monopoly of one person or group. National exclusivity on the means and construction of intelligence data is a doxa from the World War II and the cold war, but has never been a practice. Sharing began as soon as technologies of communication and surveillance at distance existed. Galileo's spyglass, for example, provided one of the first ways to anticipate fights to come, and the advent of the telegraph changed the scale of combat, integrating transnational activities for local fights.[4] The US army during the World War I was certainly among the first to develop a strategy of intelligence sharing with certain protocols organising levels of differential access.[5] It became even more important

during the Second World War and from that time, transnational alliances have existed with high level of exchanges while keeping levels of secrets into a small group of 'specialists' of management of sensitive information.[6] Nevertheless, the process of extension of meaning of intelligence information, the globalisation of the risk narrative and digitization, have extended the phenomenon beyond the capacity of controls, and with internet developments it was almost impossible not to have disclosures of the practices of interception.

As Warner develops; 'finally intelligence took on a multiplicity of meanings, some of them only barely overlapping. It remained a synonym for espionage, of course, but it also came to mean any sort of information that decision makers might need to select a course of action. It also came to mean the overall system that manages the state's espionage (and counterespionage) function, its collection of secrets and non-secrets for ministers and commanders, its interaction with friendly intelligence services, and the work product of these functions. In short, those secret activities had become systematized as intelligence'.[7]

This implies a reversal of causality. Intelligence has been the end results of many different practices, heterogeneous and on the move in terms of purposes and technologies. It has not been an organisational principle regulating nationally state survival and interests. The government of one country has never been in practice in a monopolistic position. The state is a field of action, not an actor. And some transnational fields have intersected strongly with the national state field, even gaining supremacy where sending secret information to a foreign agency was considered as a more important loyalty to respect than the one with the national politicians. The BND affair in Germany and its link with the NSA are one among many examples of these practices. This does not mean that in other cases the national imperative is not working against foreign collaboration if sensitive matters (industrial secrets for example) are at stake. In the Five Eyes messages, the NSA has flagged messages with the label NOFORN to restrict access to the knowledge of another country selectively. Typically, the CIA has posted advice for US government operatives infiltrating Shengen explaining how to avoid controls to conduct action on allied territories without their knowledge. It was under NOFORN (WikiLeaks release 21 December 2014). But, beyond the anecdotes of commercial influences and the fact that some countries are not under a no-spy agreement, even those with such an agreement have been subjected to spying through collaboration between the agencies working on the same domain but simultaneously with the ignorance of the other national agencies, and even of the government. Allegations have been made that if the suspicion of terrorism regarding a foreigner may compromise US interests, they may not inform the targeted country, even if it is an ally. In addition to these complex situations, where important information is not delivered, we may add also cases where the allied agencies are aware but do not communicate with their own political authorities. Paradoxically, it could be said these cases are rare, but are often among the most important to know for the national security of the country at the governmental level. When they are kept inside a specific channel, the game is therefore more highly complex than the image on national-foreign exchange may suggest. It pluralises the 'corridors' of information, depending on the bilateral relations between the agencies, independently of national government's disagreement.[8]

The consequences of this de-monopolisation are sometimes not fully considered. The national state game is only one of the many games for intelligence data. Despite the break through, Michael Warner for example continues to believe in the supremacy of states and in a Westphalian world where Max Weber's definition of the state continues to be pre-eminent, where private is obeying public through delegation, where internet companies are subordinate to government, where digital is just an expression of the 'real' (off line). We suggest the need to de-essentialize the state even more. It is important to take into consideration the changes to the fields of power at the transnational level and how they affect politics. Reasoning in terms of national security is no longer a coherent way to understand how shared secrecy is connected and circulates, how public and private actors are now so intertwined that we have to speak of hybrid security and not of a public-private partnership, and in addition to explain the multiplication of the effective practices of secret

services which pass through the publication of nominal lists of suspects (individual and organisations) and call for the collaboration of the public in the identification and localisation of these suspects. This shift is what I have called the emergence of a digital reason of state on a transnational scale

Towards the emergence of a field of digital reason of state populated by transnational guilds of extraction of secret information

If it is crucial to do a sociogenesis of the secret intelligence field to avoid the illusion that it is completely new, it is also important to observe the transformations connected with the eruption of the digital age and the ease of surveillance which facilitate both the sharing of information and the explosion of secrets and uncovering of them via internet technologies and the role of private companies. I insist here that the scale and scope of surveillance and the transnationalization of intelligence services we have witnessed over the last few years require a renewed investigation of contemporary world security practices on the one hand, but also a careful mapping of our very own categories of analysis on the other.

Sovereignty, secrecy, security communities, territory, border control, technology, intelligence and rule of law have inevitably ended up meaning different things for different people. What is under question is not one of these categories over another, but how all these categories have simultaneously changed. I am arguing here that this boils down to an argument over the digitisation and heterogenization of *Raison d'Etat* (Reason of State) destabilising public and private, internal and foreign, shared and (national) secret distinctions.

Key to my argument about the transnational fields of shared secret information channels (or corridors), is to understand and analyse how the classic *Raison d'Etat* and its contemporary iterations, such as national security, have undergone profound mutation with the process of digitisation, the emerging 'datafication' of our societies and the extension of police and intelligence services. I do not develop here the long genealogy of these relations and causations, but I consider that the field of shared secret information is dependent in its extension and reconfiguration towards less HUMINT and more SIGINT activities on 'the emergence of a digital reason of state' based on the possibility for intelligence services of different countries extending their goals of prevention and prediction of crime to a global reach, convincing their own politicians that the future of intelligence is clear: it is to include and expand technologies collecting traces of human activities.[9] This increase in and need to gather digital communication and data, once accepted politically, has nurtured in return a wider transnational collaboration amongst national intelligence and security professionals and resulted in an extension of the category of foreign intelligence to share data that could be of national concern more specifically. This has created a spiral effect. By projecting *national security 'inside out'*, via a transnational alliance of the professionals of national security and sensitive data, *an 'outside in' effect of suspicion* for all Internet subjects has been created, destabilising the protection for national citizens if they are communicating with foreigners. It changes the categories of 'foreign' and 'domestic' by dispersing them and transforming the line that separated them into a *Möbius strip*.[10]

The division between internal and external practices of intelligence and secrecy, while maintained to ease the possibility without warrant on foreign intelligence is de facto obsolete. It does not mean that we are encountering a merging of internal and external into a global without boundaries, but we observe a logic where, intersubjectively, everything is analysed either as external or internal depending on the interests of the surveillant-actors, even if, more recently, the Courts have tried to reverse the reasoning of the services and to show that they cannot choose the legislation of foreign or domestic the way they want, but have to regulate the interception with more general principles: necessity, proportionality.[11]

This is what we will examine now. What have been the consequences for the targets of intelligence of the change of regime of intelligence data privileging transnational exchanges and

digitization? Certainly, digitization at the world scale has been contemporary to the phenomenon of hybridization of the public and private logic. This has created many questions about the level of participation of many private entities into the circulation of information on one side and of their participation in channels of secret intelligence, either indirectly, as provider of information they retain but do not analyse themselves, or more directly when they are asked to contribute to develop them.

These two phenomena of hybridization and digitization have transformed the relation between intelligence, surveillance and obedience (or compliance) in everyday democracy. This has been done in western countries without much protest, and even after the disclosures of practices in such a detailed manner and with the participation of major newspapers, the general public has considered that it was a question for professionals, not for them, to decide on the boundaries between secret procedures and democratic rulings.[12] Some commentators have therefore considered that 'the people' have accepted the fate of an evolution that they like (or not) but cannot change.[13]

This is the belief of a technological determinism within surveillance that I want nevertheless to challenge because in the end this is the main argument in favour of the prolongation of secrecy procedures without proper oversight and scrutiny by public mechanisms. People do not accept surveillance, they are just unaware of the high level of circulation of shared secrets and if they knew, they would be less keen to participate to it. But, before discussing the consequences of this circulation of shared secrets, we need to emphasize how they are exchanged today in such increasing numbers.

Channelling secret information? How and for what purposes?

As explained by Sir David Omand: 'For intelligence and law enforcement to be able to identify communications of interest and, where authorized, to access the content of relevant communications themselves is in fact a harder technical challenge than the many internal NSA PowerPoint presentations stolen by Snowden might suggest'.[14] And this is certainly true. PowerPoints are oriented towards presentations and so simplify techniques, they are not 'truth' about practices. Nevertheless, they give indications about the ways the services enter into contact, what software helps them to automatize some type of exchanges, and the correlations between the technical systems and the judicial obligations.

Obviously secret services share much data between them, but in very asymmetrical ways and through very different levels of right of access.[15] Exchange has never meant equality of situation. Here exchange is the result of the structural positions of the different services regarding each other and not just a relation of 'trust' between them. Sharing information is highly differentiated: what is on offer for a 'foreign' partner may be the data on some individuals if the foreign partner asks and already knows who they are, or key elements of the identification. It may be access to far more general and numerous data that can facilitate a search for identification criteria (for example a bank account transaction, or vaguer criteria where the period is a full month with the criteria only that money is coming from an unknown bank account but whose country deposit is known – Mali to Norway transiting via…). It may also be a series of tools interconnecting databases via interoperability platforms or search tools but limited access to data. And it may be general results of data analytics but without any names. All these modalities are different. Some like the first and the last are old practices. The second and third are more recent, connected with digital capacities to deliver large scale of data for imprecise criteria quickly. The human capacities to treat the data once filtered are therefore of crucial importance. Technical skills are insufficient if they are automatized, they need to be held by specialists.

Only the powerful services get a chance to use to their profit the sharing of data. Their number of personnel, budgets and position regarding the internet traffic are key elements that we have analysed elsewhere.[16] In addition, to add a layer of complexity, they are not, by far, the only actors involved. The access in bulk to substantial quantities of the Internet supposes the interception and

storage of metadata and sometimes the data related to these metadata. To access internet cables they often work with their own private companies who have built or collaborate in the construction of cables and the latter are key actors in the interception practices of data and the secrecy about this interception.

Once the services have the saved metadata which can provide information concerning when and to whom phone calls are made or emails and texts are sent, they still have to identify the suspects, and they are often obliged, beyond their own national resources, to look at international databases through different requests, either directly in a bilateral manner if they know in what country they may be, or via what is called 'Advanced "front end" tools allowing analysts to efficiently access and run advanced queries on intercepted data, in particular, in order to discover new leads in their investigations'.[17]

Among different tools, one can quote ICREACH for exchange between US agencies and their closed counterparts, and one which has been highly popularized, Xkeyscore. Xkeyscore is a program that has been shared with other intelligence agencies including the Australian Signals Directorate (ASD), Canada's Communications Security Establishment, New Zealand's Government Communications Security Bureau, Britain's Government Communications Headquarters, but also Japan's Defense Intelligence Headquarters and the German Bundesnachrichtendienst. Xkeyscore allows searching and analysis of global Internet data, with specific selectors and a high speed answer. According to an NSA slide presentation about XKeyscore from 2013, it is a 'Digital Network Intelligence Exploitation System/Analytic Framework'. According to a good Wikipedia article, 'XKeyscore holds raw and unselected communications traffic, so analysts can perform queries using "strong selectors" like e-mail addresses, but also using "soft selectors", like keywords, against the body texts of e-mail and chat messages and digital documents and spreadsheets in English, Arabic and Chinese.'[18]

A second program, less well known, is ICREACH.[19] In a nutshell, the National Security Agency is secretly providing data to nearly two dozen U.S. government agencies with a 'Google-like' search engine built to share more than 850 billion records about phone calls, emails, cellphone locations and internet chats. ICREACH contains information on the private communications of foreigners and, it appears, millions of records on American citizens who have not been accused of any wrongdoing but have entered into some previous profiles of suspicion and have been kept there, just in case. As Ryan Gallagher explains 'ICREACH has been accessible to more than 1,000 analysts at 23 U.S. government agencies that perform intelligence work, according to a 2010 memo. A planning document from 2007 lists the DEA, FBI, Central Intelligence Agency and the Defense Intelligence Agency as core members. Information shared through ICREACH can be used to track people's movements, map out their networks of associates, help predict future actions, and potentially reveal religious affiliations or political beliefs.'[20] The search tool was designed to be the largest system for internally sharing secret surveillance records in the United States, capable of handling two to five billion new records every day, including more than 30 different kinds of metadata on emails, phone calls, faxes, internet chats, and text messages, as well as location information collected from cellphones. ICREACH does not appear to have a direct relationship to the large NSA database, previously reported by The Guardian that stores information on millions of ordinary Americans' phone calls under Section 215 of the Patriot Act. Unlike the Section 215 database, which is accessible to a small number of NSA employees and can be searched only in terrorism-related investigations, ICREACH grants access to a vast pool of data that can be mined by analysts from across the intelligence community for 'foreign intelligence'. Data available through ICREACH appears to be primarily derived from surveillance of foreigners' communications, and planning documents show that it draws on a variety of different sources of data maintained by the NSA.[21]

It seems that on specific occurrences, ICREACH was also opened to other partners of the Five Eyes plus, including Canada and Australia, but this has been denied. We cannot know if it was a two-way circulation between agencies or if it was only one-way, with Australian and Canadian data

being stored into ICREACH. In that case the ASD may have fed information into the NSA's vast ICREACH search engine but not had access to it.[22]

We have certainly to learn more on the right of access and to avoid the sensationalism of some media, but we are clearly beyond small numbers. Shared secrecy is about the millions of pieces of individual information and metadata circulating between transnational data bases. They are the virtual 'haystack' mobilized when profiles of suspicion are constructed for a specific purpose. But, and it is one of the specifics of the data analytics program, they are oriented towards prevention and conceived to build predictive profiling around a specific hypothesis of doubt concerning 'abnormal behaviours' and-or trajectories and-or multiple identities. This future perfect orientation of a future already known is in itself a problem as machine learning works to confirm hypotheses, not to invalidate their basic assumptions, and the correlations uncovered by the analytics cannot be considered as proof of causality, a lesson Emile Durkheim set out in his famous book on suicide with reference to the correlation of suicide and sunspots.[23]

The arguments of prevention and prediction: an ideology or a reasonable justification for exceptional means?

A story is constructed based on the potentiality of the system. It is said that it is now possible to trace almost all of the online activities that an Internet user undertakes during the day: what they read on the web or purchase on Amazon, what they send to colleagues and family members via email, what sort of holidays they take and whether they travel abroad, and what kind of online payment system they use. The capacity to act at distance has increased the traceability of data; the possibility of data retention; the capacity to build software that enables complex relations between databases, and to deduct from these data emerging trends, statistical categories of behaviours or individuals; and the belief that these emergent and minority trends give intelligence services an advantage in conducting their various activities such as espionage, economic intelligence, and the struggle against terrorism and crime.

The overall argument of a permanent war on terror and its claimed necessity to connect always more of the lacking dots to the large network of people under electronic surveillance, succeeds, it seems, to move the people living in liberal states to consider that they need Total Information Awareness against erratic violence led by revenge and widespread diffusion. Authorities need to have a grip to anticipate the future, to suspect rightly the people who act abnormally, because they are preparing the worst. The argument of a pre-crime society has replaced that of a society liberated from communist collectivism.

This is the new utopia of a society conducted by anticipative knowledge built through data analytics where profiling is more and more subtle and self-correcting, while data collected are bigger and bigger and, once retained, filtered, and selected on specific requests. They allow for better detection of the white noises, the black swans, the abnormal behaviours, everything that does not fit with the 'normal' order. A different political imagination has radicalized the fear of global terrorism and the necessity of a maximum and global security regime to counter terrorism on the one side, and on the other has also produced a fear of an Orwellian world in the making, in which citizens are systematically spied upon in their everyday practices.[24] But most secret intelligence professionals fight against this ideological stance and resist the argument of a scientific prediction. They accept the idea of forecasting on precise consequences, but do not see themselves as astrologers. Nevertheless, some are tempted to play that role to please politicians in charge and the industry building these systems.

This 'knowledge' of predictive analytics is said to be the answer to the dissemination of violence into inter-individual relations, a technological fix that reconstructs the political in liberal democracies far from the eruption of political violence. Politics will no longer be a question of ideological judgments, but a question of anticipation of the hidden enemy, of its stealth moves. Politics will be the art of war supplied by the technology of traceability and the use of a Maxwell's Demon

activated in some computers to know the positions and trajectories of all human beings suspected of distorting the norms and of being at the margins. Joining the dream of expertise with astrology, connecting hard science and religious sacrificial rituals, destroying the political as a relation to focus on the margins, mixing the image of the future with an old past of superstition, this reasoning is in addition the one that favours protection of society over the rights of the individual and destroys the very idea of privacy and freedom of thought. But, to the despair of many activists, people on the web do not react in mass against these practices.

De-monopolization of the field of secrecy: spying and counter spying, secret defence, national security, industrial secrets, everyday surveillance

If answers about the activities and group of people in charge of the extraction of secret, sensitive and personal information was easy during the period of the Second World War and then the Cold War, with its rituals around spying and counter spying, monopolised by the most powerful states to monitor the activities of the other system of alliance in terms of armaments and technological progress, this is not the case anymore. We have developed in detail the conditions under which the specialised group or more exactly the guilds of secret, sensitive and personal information have evolved with the digitization of the reason of state.[25] Consider the example of the specific politics of hostility against lawyers by the Bush administration to create the idea that technological progress needs to be used at its full scale and without restriction because of the context of secret war. In that context without even the need to know, any opportunity to know cannot be neglected to anticipate the future. Every data that can help to build profiles of suspects is therefore considered as a legitimate source by the intelligence services. This vision is one that is at war with the rule of Law and public-judicial scrutiny but the neo-conservatives nevertheless succeeded in modifying the economy of the field of secret intelligence by justifying large-scale collection of data captured almost directly from internet cables and without proper warrants.[26] Polls have not shown strong resistance. As a result, it has allowed a course to harvest data, a form of digital encomienda authorizing the people involved into the interception of data, and the enrolment (by coercion or strong suggestion) of the biggest US companies in the field of Internet data and social networks to consider individual data as their 'property'.[27] More structurally, if this has been possible to pursue beyond the official end of the war on terror, it is also because intercepting data which are confidential can be done very cheaply and with considerably less effort than before, the ratio of surveillant-surveillees moving from 4/1 to 1/hundreds.[28] Even more generally, as very well explained by Warner in *The Rise and Fall of Intelligence*: 'Today, many states (beyond the cold war alliances) can do so once again; and what is more, private entities and even individuals (some with criminal motivations) can gather secrets and manipulate events around the globe. The skills needed to "do" intelligence have diffused around the world and across societies; they can literally be purchased online. The problems caused by this spread of intelligence, moreover, now reach beyond the security services to corporate offices and private homes. In short, intelligence has traded uniqueness for ubiquity'.[29]

Secrecy of little secrets coming from intimate life has invaded the world of intelligence while secrets, even of some importance, are shared by more and more people who have not been trained by their education and profession to respect the rituals around them. To sum up, for decades, the field was delimitated along crystallized lines. The actors were public bodies called secret services and they were arguing that secrecy was a necessity for protecting the national security of each state, but now with the digitization of information and the globalization of the exchange of information as well as the riskification of the world where distant catastrophes may have an impact in every local place, the boundaries are no longer 'waterproof' between the 'secret' services and other public or private bodies.

The legitimacy of the 'public secret services' claiming to be the sole experts in providing analysis for national security is now destabilized. Private organizations collecting data, managing them with

more efficient tools, challenge their monopoly and invade their territory of secrecy obliging them to have collusive transactions enlarging the sphere of shared secrets.[30] International exchange of information and the belief that 'big' data analytics are based more on big numbers than on small and smart data, are also challenging the national character of the collection-interception of data and privilege large groupings of services who have the same know-how but different nationalities and interests. The fact that specialists are sceptical about these capacities of artificial 'unintelligence' has not yet changed popular and journalistic beliefs.

The notion of shared secrets in a transnational world: the five eyes plus practices revealed

The disclosures in 2013 by Edward Snowden of the secret US-NSA programme, PRISM, and of more than a thousand types of intrusive software with genuinely hush-hush codenames have raised serious concerns about the scope and scale, the qualitative and quantitative dimensions, of surveillance of everyday internet users for intelligence purposes. What has been done by the NSA and the Five Eyes network during the previous 10 years, in secret? Is it possible in democracies to act in such a way, which is certainly less directly violent than the CIA's physical networks, but nevertheless problematic for democratic forms of states?

Quite clearly, Snowden's disclosures of NSA practices have sparked significant public and political concerns. Some concerns about security to start with – security for whom? – were identical to the critique of the war on terror, but they were followed by questions about technological progress and a sense of the ineluctability of the deprivation of confidentiality and privacy in our modes of communication, wrapped around an overall argument about the inherently violent, unsecured and dangerous state of the world.

The extension via the digitization of information of the number of people inside a procedure of restriction of access, as well as the generalization of large transatlantic channels of exchange of information exacerbates the tensions between the actors participating to the production of secrecy. And this is what we will analyze now. Are the secret services losing the control of secrecy for (national) security? Are they obliged to compose with other actors who manage more secret procedures of secrecy than themselves inside the general management of information? Who has the authority to control sensitive information and to frame it under secrecy? It seems that the destabilization of the initial conditions of secret services regarding spying and counter spying where the rules for national security secrets (including exchanging individuals) were set up is so strong that the barriers distinguishing who the secret services are have exploded, with the de-monopolisation of the practices of spying and counter spying, with the privatization of surveillance, with the commercialization of the Internet and its willingness to make money from personal data, with the desire to anticipate the future of human beings. The de-assembling and re-assembling of the secret services beyond the public services of a state including private contributors, and beyond the national territory with the integration of heterogeneous information beyond internal collection of data, is interrogating the very nature of the group of persons who are the professionals of extraction of (secret, sensitive and personal) information.

There certainly lies a change in the regime of justification of national security within this argument. First a justification has been expressed and presented openly, because the scandal open by the disclosure of large-scale surveillance was too strong to enable a return to opacity, to the traditional: 'no comment, no denial' policy. But, the national security argument has been connected centrally with the large-scale intrusive data interceptions the press has called mass surveillance and bulk collection, while the services and the internet providers have considered that their methods were necessary, appropriate and proportionate.

The controversy has implied on the technological side a branching out of existing rhizomatic commercial surveillance for profit and intrusive methods of interception and collection of personal information by specialized intelligence services and their contractors. It has also opened a legal

conflict with the judiciary on many fronts, and the national security terminology, which was in many countries a doctrine coming from the US and the UK, has nevertheless entered legislation after the Snowden disclosures of 2013, even if for most of them – France, Germany, Spain, Italy – the notion of 'secret defense' is still more relevant in a legal context than that of national security.

A counter move: rule of law, human rights countering technological arguments and necessity of intrusive intelligence?

National Courts and European Courts have been more and more clear in their judgements post-2010 that if it is to the government to decide the content of national security, this cannot be completely discretionary. This has been and is still the main challenge theoretically for the term national security and the encapsulated practices of human and technological intelligence. National security (and the secrecy around it) cannot be transformed into a blanket for executive arbitrariness that other powers and citizens cannot check. Even when citizens believe that, in general, agents of secret services are also good citizens, they want nevertheless to have the capacity to differentiate inside the group, to punish those who have acted against inviolable rights, like the prohibition against torture, and to know who has given these orders. From the 2010s, in a not yet stabilised doctrine, a framing, which has been developed in Europe via the role of Courts (ECJ and ECHR), but also in national courts in the UK or Germany, has contradicted the US NSA approach of the post-war on terror era based on a more military and strategic vision justifying the president's power and its own practices. It seems that in Europe, legally, national security cannot trump the Rule of Law and democracy for political opportunist interest, the derogations have to be necessary and proportional to the threat. The threat itself cannot be the product of a flourishing imagination, it needs some evidence of an actual project of realisation. Prevention is not fiction, anticipation has to have grounds.

Nevertheless, the reactions of the highest courts, acclaimed by activists and lawyers challenging the government have not transformed the everyday practices of internet users, and push them to defend by themselves their rights of data protection, privacy and forms of freedom which are endangered by intrusive intelligence. The argument of the necessity of struggle against terrorism has been quite powerful, as well as the argument that the traces left by the use of internet and the limitations of privacy are the normal counterpart of more communication at distance, as Zuckerberg bluntly said. Nevertheless, after the Cambridge Analytica scandal involving researchers, strategic communication firms and google research for profit via the brokerage of personal data for other commercial (or political) means, and the development in Europe of General Data Protection Regulation (GDPR), the argument of the necessity of collecting data to have access to digital tools simplifying everyday life begins to be challenged, as well as the politics of the SIGINT-Internet secret services, and the logics of the capitalism of platforms which are intertwinned with the escalation of the numbers of little secrets in circulation.

Conclusion: Is it possible to be innocent in a world of suspects? Conformity regarding the diagonal of intelligence, surveillance and compliance

The consequences of this taming of the future are affecting democratic dimensions. Do we have 'scientific' oracles to listen or is this noise about the new form of reasoning a way for an industry of surveillance to sell products and to convince us that anyone in the public is innocent, but he is the only one, all the others being for good reason, suspects? Is it in that case a way to advance compliance of consumers towards a more invisible surveillance? The conjunction of capacities to collect data easily and massively at a cheap price, reversing the relation between intelligence work and surveillance by collection of large-scale data, and facilitating the accumulation over the quality of information contained into these data, has reinforced this dream of anticipation of the future and the discourse of a pre-emptive or preventive action. It has dressed this myth with some clothes of informatics sciences that do not fit together. It has destroyed guilt and innocence for a policy of

permanent suspicion. More importantly even, it has transformed the image of potential suspect into the one of an enemy criminal, of an intimate public enemy, and has rendered banal this figure of the suspect with no right, no chance to defend himself, no chance to change his mind. As soon as the suspect emerges from a list of names, he is not anymore a potential suspect, a potential terrorist, he becomes a terrorist, a murderer. Digitization operates magically with a politics of number that concretise, operationalise the figure of the invisible, of the unknown. This is why analysing the conditions of the emergence of digitization and the link with the transformation of intelligence is so important. It is not just a correlation, a chance for the Sigint Service that their field has exploded in size and importance, it goes further. The Internet is not just an accumulator of data, it is a translator of logic. We are now all virtually living as the only innocent in a world of suspects.

To sum up, to understand the effects of the connection between intelligence practices and the rise of technologies connected to the digitization of the world is complex. So too is the possibility of tracing actions with the ambition of knowing and anticipating the future. Methodologically, it is difficult to distinguish between the pretenses to know, and the effective capacities to discover trends oriented towards future human actions. This depends on the belief about preventive actions and scientific prediction coming as an outcome of large-scale collection of information (in bulk). But, I contend here against other analysts, who argue that this transformation is the inevitable product of an evolution of technologies related to the internet and the more general digitization of the world and its impact on the 'off-line' world. The path transforming the Internet into a tool of surveillance and the social networks into forms of co-watching reinforcing in-group rules as well as reframing subjectivities by reinforcing compliance, is not an historical necessity, and is not with us forever. It is the product of discretionary acts of politics at a certain moment.

The so-called inevitability of escape from a society of surveillance today is therefore not a description of the world as it is, but a form of doxa inherited from the extension of the field of extraction of information to a new set of actors, which is the product of certain dynamics of struggle between the actors managing digital information and especially data based on individual traces, be they from private actors and commercial logics or from governments and their services of interception of communication and security logics. Surveillance is therefore not inherent from communication and information gathering. It depends on a specific configuration of actors that succeed in differentiating themselves from other actors as the legitimate owners of secrecy, and the ones distinguishing suspects from innocents.

Notes

1. The distinction between correlation and causality is here a central element. See Emile Durkheim who insists that sociology is about causality and not simply correlations. Correlations may help find causality, but they may be the product of hazards or embedded stereotypes creating false causalities.See more recently Colburn 2008: p 10. For a more optimistic view Dhar 2013: pp 64–73.
2. Petersen, Karen Lund in this issue.
3. Omand, *Securing the State*, 191.
4. Weaver and Pallitto, *Extraordinary Rendition*.
5. Information processing drove an imperative to share information across national lines with allies.
6. The UK-USA agreement to share signals intelligence was a key moment. It covered • collection of traffic • acquisition of communication documents and equipment • traffic analysis • cryptanalysis • decryption and translation • acquisition of information regarding communications organizations, practices, procedures and equipment. In short, the British and American codebreakers would share almost everything, from the raw take to their finished analytical products, nevertheless UKUSA agreement excluded sharing with 'third parties'.
7. Warner, *The Rise and Fall of Intelligence*, 1.
8. See Greenwald Glenn Foreign Officials In the Dark About Their Own Spy Agencies' Cooperation with NSA Intercept 13 March 2014. Greenwald develops different cases including cases where the ally partner of the NSA is asked to spy, for the profit of a foreign partner, on its own citizen ot its own government (as in the case of Angela Merkel phone). The French DGSE has also exchanged a lot of information with the CIA during the War

on Terror despite the official split between Jacques Chirac and George Bush on Iraq. It is still difficult to know if it was with his agreement or not.

9. Bigo et al., "Mass Surveillance of Personal Data"; and Bauman et al., "After Snowden."
10. Bigo, "Internal and External Security(les)"; Bigo, "Political Sociology"; and Bigo, "Sécurité intérieure, sécurité extérieure," 316.
11. Cole et al., *Surveillance, Privacy*.
12. Mueller, *Public Opinion*.
13. Harcourt, *Exposed*.
14. Omand, *Securing the State*, 11.
15. Cf the notices: for US eyes only, or not for UK eyes on some messages. For details see the excellent website: https://search.edwardsnowden.com/docs/OperationalLegalities2015-06-22_nsadocs_snowden_doc .
16. Bigo et al., "Digital Data and the Transnational Space."
17. Omand, "Understanding Digital Intelligence," 7.
18. Xkeyscore- See Wikipedia, and for more details: The Unofficial XKEYSCORE User Guide; https://search.edwardsnowden.com/docs/TheUnofficialXKEYSCOREUserGuide2015-07-01_nsadocs_snowden_doc .
19. https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/ .
20. See annex 1.
21. Excerpts of Gallagher 2014. See also https://theintercept.com/document/2014/08/25/sharing-communications-metadata-across-u-s-intelligence-community/. ICREACH is 'not a repository [and] does not store events or records in one place.' Instead, it appears to provide analysts with the ability to perform a one-stop search of information from a wide variety of separate databases. The mastermind behind ICREACH was recently retired NSA director Gen. Keith Alexander, who outlined his vision for the system in a classified 2006 letter to the then-Director of National Intelligence John Negroponte. The search tool, Alexander wrote, would "allow unprecedented volumes of communications metadata to be shared and analysed, opening up a 'vast, rich source of information' for other agencies to exploit.
22. https://www.theguardian.com/world/2014/oct/13/australias-defence-intelligence-agency-conducted-secret-programs-to-help-nsa.
23. Durkheim, *A Study in Sociology*.
24. Against this idea that intelligence services spy on their own citizens, the answer is to distinguish the different users of the Internet by the origins of the communication and the supposition of their nationality. Western intelligence services would respect their citizens and would have safeguards. This is certainly true, but it is also a justification for almost no limits on the surveillance of foreign internet users, and it comes at a huge cost for privacy and democracy that cannot be reserved to one nationality against the others. Members of transnational agreements like the 5 eyes plus, have also sometimes switched their national who are foreigners for the other services, and exchanged targets of surveillance to bypass their legislation in the two distinct ways to intercept data differently depending if the process is purely external and therefore a foreign interception of intelligence or if it is an internal one subjected to more judicial control and often specific warrants both in the US and in Europe. This has created one of the most central controversies between judicial review and justifications of intelligence services which is not yet settled, and discussion continues about retention of data, definition of meta data, circuit of foreign intelligence in regard to internal security intelligence, third party disclosure exceptions, and the validity of the UK Investigatory Powers Act.
25. Bigo, "Beyond National Security."
26. Weber et al., *The Routledge International Handbook*.
27. See note 16 above
28. Reith lectures by MI5 former head Eliza Manningham-Buller: https://www.bbc.co.uk/programmes/b0145x77 To have a list of suspects is not having them under effective surveillance- Cf also the problem in France with the number of terrorist attacks in 2015 done by individuals put on the S (surveillance) list and the later debates about the capacity of the services.
29. See note 7 above.
30. Dobry, "Le renseignement politique dans."

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This article is an original piece doing the synthesis on the questions of use of secrets of the research on the professionals of societal security SOURCE (FP7 Security 313288) and of the research on intelligence services UTIC (ANR-14-CE28-0024)

Notes on contributor

Didier Bigo Professeur Department of war Studies King's College London Research professor (MCU) Sciences Po Paris Directeur of the Centre d' etudes sur les Conflits, la Liberté, la Sécurité (CCLS) www.ccls.eu personal website http://didierbigo.com/ latest publications: Guild, Elspeth, Didier Bigo, and Mark Gibney, eds. Extraordinary Rendition: Addressing the Challenges of Accountability. Routledge, 2018.

ORCID

Didier Bigo http://orcid.org/0000-0002-1908-6532

Bibliography

Bauman, Z., D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. B. J. Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (2014): 121–144. doi:10.1111/ips.12048.

Bigo, D. "Internal and External Security(les): The Möbius Ribbon." In *Identities, Borders, Orders*, edited by M. Albert, D. Jacobson, and Y. Lapid, 91–116. Minneapolis: University of Minnesota Press, 2001.

Bigo, D. "Sécurité intérieure, sécurité extérieure: Séparation ou continuum ?." In *Transformations et réformes de la sécurité et du renseignement en Europe*, edited by É.-Y. Laurent and B. Warusfel, 121–144. Bordeaux: Presses Universitaires de Bordeaux, 2016.

Bigo, D. "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 *Kettemann and Kilian Vieth: Research Handbook on Human Rights and Digital Technology*, edited by B. Wagner and C. Matthias, 61–82. Global Politics, Law and International Relations, 2018.

Bigo, D., and L. Bonelli. "Digital Data and the Transnational Space of Intelligence." In *Data Politics, Routledge International Political Sociology*, edited by D. Bigo, E. Isin, and E. Ruppert. 2019. Forthcoming.

Bigo, D., S. Carrera, N. Hernanz, J. Jeandesboz, J. Parkin, F. Ragazzi, and A. Scherrer. "Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law." CEPS Liberty and Security in Europe No. 61. 2013.

Bigo, D., and R. B. J. Walker. "Political Sociology and the Problem of the International." *Millenium. Journal of International Studies* 35, no. 3 (2007): 725–739. doi:10.1177/03058298070350030401.

Colburn, A. "Correlation and Causality." *The Science Teacher* 75, no. 2 (2008). https://www.questia.com/read/1G1-182530694/correlation-and-causality.

Cole, D., F. Fabbrini, and S. Schulhofer. *Surveillance, Privacy and Trans-Atlantic Relations*. London: Bloomsbury Publishing, 2017.

Dhar, V. "Data Science and Prediction." *Communications of the ACM* 56, no. 12 (2013).

Dobry, M. "Le renseignement politique dans les démocraties occidentales. Quelques pistes pour l'identification d'un objet flou." Cahiers de la sécurité intérieure (I.H.E.S.I.), 1997. n°30, 1997.

Durkheim, E. *Suicide: A Study in Sociology*. Abingdon: Routledge, 2005.

Gallagher, R. "The Surveillance Engine: How the NSA Built Its Own Secret Google." The Intercept. 2014. https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton.

Harcourt, B. E. *Exposed: Desire and Disobedience in the Digital Age*. Cambridge: Harvard University Press, 2015.

Mueller, J., and M. G. Stewart. *Public Opinion and Counterterrorism Policy*. Cato Institute, 2018. https://www.cato.org/publications/white-paper/public-opinion-counterterrorism-policy.

Omand, D. *Securing the State*. Oxford: Oxford University Press USA – OSO, 2014.

Omand, D. "Understanding Digital Intelligence and the Norms that Might Govern It." CIGI, Global Commission on Internet Governance, No. 8. 2015.

Petersen, K. Lund in this issue.

Warner, M. *The Rise and Fall of Intelligence: An International Security History*. Washington, DC: Georgetown University Press, 2014.

Weaver, W., and R. Pallitto. *Extraordinary Rendition*. The Oxford Handbook of National Security Intelligence, Oxford University Press, 2010. doi:10.1093/oxfordhb/9780195375886.003.0020

Weber, L., E. Fishwick, and M. Marmo, eds. *The Routledge International Handbook of Criminology and Human Rights (Hardback)*. Routledge, 2018. https://www.routledge.com/The-Routledge-International-Handbook-of-Criminology-and-Human-Rights/Weber-Fishwick-Marmo/p/book/9781138931176.

Annex 1. Disclosure of NSA documents by Edward Snowden- Gallagher Ryan 2014