International
Political
Sociology

International Political Sociology (2014) **8**, 121–144

After Snowden: Rethinking the Impact of Surveillance

Zygmunt Bauman

University of Leeds

Didier Bigo

King's College London and Sciences-Po Paris

Paulo Esteves

Pontifical Catholic University of Rio de Janeiro

Elspeth Guild

Queen Mary and Radboud University Nijmegen

Vivienne Jabri

King's College London

David Lyon

Queen's University

and

R. B. J. Walker

University of Victoria and Pontifical Catholic University of Rio de Janeiro

Current revelations about the secret US-NSA program, PRISM, have confirmed the large-scale mass surveillance of the telecommunication and electronic messages of governments, companies, and citizens, including the United States' closest allies in Europe and Latin America. The transnational ramifications of surveillance call for a re-evaluation of contemporary world politics' practices. The debate cannot be limited to the United States versus the rest of the world or to surveillance versus privacy; much more is at stake. This collective article briefly describes the specificities of cyber mass surveillance, including its mix of the practices of intelligence services and those of private companies providing services around the world. It then investigates the impact of these practices on national security, diplomacy, human rights, democracy, subjectivity, and obedience.

Large-Scale Techniques of Surveillance and the Global Reach of the Internet: A Permanent Gap

Edward Snowden has famously disclosed extensive information about the practices of the US National Security Agency (NSA) with regard to PRISM and other

Bauman, Zygmunt et al. (2014) After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, doi: 10.1111/ips.12048

US surveillance programs—including Xkeyscore, Upstream, Quantuminsert, Bullrun and Dishfire—as well as the involvement of services in other states, such as the UK-GCHQ and its Tempora (as well as its Optic Nerve) programs. Much of this information, especially about the scale, reach, and technical sophistication of these practices, came as a surprise even to seasoned observers, and its significance remains unclear. This is partly because the extensive details about the complex systems that have been exposed are difficult to track, although many of them seem to have serious and immediate consequences. It is also because these details seem to imply significant transgressions of established understandings of the character and legitimacy of those institutions concerned with security and intelligence operations, thus stimulating intense political controversy. And it is partly, and even more disconcertingly, because some revelations seem to confirm long-term transformations in the politics of states; in relations between states; and in the institutions and norms established in relation to democratic procedures, the rule of law, relations between state and civil society, relations between public policy and corporate or private economic interests, the acceptability of cultural norms and even concepts of subjectivity.

There is thus an urgent need for a systematic assessment of the scale, reach, and character of contemporary surveillance practices, as well as the justifications they attract and the controversies they provoke. We need to know whether these practices mark a significant reconfiguration of, say, relations between intelligence gathering and surveillance of the Internet and other systems of telecommunications, or whether they mark sustained challenges to fundamental rights in the digital sphere. And we need to pay very close attention to the longer-term implications of practices that have already raised very serious questions about widespread transgressions of legal principles and democratic norms in ways that speak to historical shifts in the locus and character of sovereign authority and political legitimacy.

The NSA programs are, first and foremost, intended to harvest data from (submarine) Internet cables (Upstream, Quantuminsert) and/or to intercept data during their travel (Tempora). They involve the placement of interceptors on the large fiber-optic cables connecting the different hubs of the Internet. In the UK, the GCHQ's Tempora program is reported to have placed 200 interceptors on cables running from the British Isles to Western Europe and the United States. The French DGSE has allegedly placed similar interceptors on underwater cables out of its military base in Djibouti. Among other activities, the German BND has been said to tap directly into the largest Internet Hub in Europe, the Frankfurt-based DE-CIX. Sweden's FRA taps the underwater cables that connect to the Baltic countries and Russia. The different intelligence services work more or less together in networks to gather information and extend a global reach, covering the Internet. Their relations tend to be asymmetrical—sometimes they are competitive and collaboration diminishes on sensitive issues—but they nevertheless find that collaboration is necessary to produce a reliable picture of the global Internet. They invariably claim that they have insufficient resources, that they need more data, and that they should have more exchange—with less control and oversight—in order to speed up the process. Unsurprisingly, such claims stimulate counterclaims about Stasi-like forms of mass surveillance, as well as complaints about the reversal of the presumption of innocence through an a priori suspicion that the individual then has to dismiss by his transparent behavior.[1]

[1] For regular updates on the revelations about different surveillance programs, see the Web sites of the Guardian and the Christian Science Monitor. Among the many available reports, see the US Review Group on Intelligence and Communications Technologies: *Liberty And Security in a Changing World*, chaired by Richard A. Clarke, December 12, 2013. See also the US Independent Privacy Oversight Board report, chaired by David Medine, January 23, 2014; the EU Report of the Libe Committee of the EU Parliament, chaired by Claudio Moraes, March 12, 2014; and the Research Study on National Programmes for Mass Surveillance of Personal Data in EU member states and their Compatibility with EU law, CCLS-CEPS, November 2013 (see References).

Suspicions are also aroused by a second and more targeted practice of interception, Xkeyscore, which is linked to the platform of integration of the NSA PRISM program and works along similar lines to that which was initiated by the Total Information Awareness program of Admiral Poindexter. This involves the acquisition of consumers' personal data by forcing those private companies (such as Google, Microsoft, Apple, or Skype) regularly collecting vast amounts of data for commercial purposes to hand it over to the intelligence services without the knowledge of users. The NSA and several European services are believed to have obtained large amounts of precise data through this channel. It is not gathered through raw data transiting cables but is mostly connected with the willingness of users to use the services of cloud computing—provided, for example, by Microsoft platforms or Dropbox—and their ignorance of the secret collection of their data. This is also the case with information coming from social networks, such as the ones managed by Facebook. Such data and metadata permit a mapping of relations between people, their IP addresses, and the sharing of content, location, and interests. Therefore, the networks of these different services are not only transnational but also hybrids between public and private actors. This extension in terms of actors and reach is not a smooth process; it also exacerbates struggles. Some intelligence services, especially NSA and GCHQ, work on a very large scale and use voluntary or forced collaborations with private providers (Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL, Apple) and telecommunication companies (BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel and Interroute) in order to collect the dots and to try to connect them using profiling and visualization software. Other services disagree with this strategy and do not request data from providers, preferring instead to concentrate on specific targets, working on a small scale but with more certainty.

A third type of practice involves the collection of phone calls, text messages, Skype communications and the diverse audio and video signals that pass through computers, smart phones, satellite communications, and traditional landlines (as with Dishfire for text messages). These effectively update and enlarge the kind of surveillance of telecommunications that produced earlier scandals involving the Echelon system for the interception of personal and commercial communication (Schmid 2001).

These various practices for intercepting communication are both complex and interconnected and are designed to secretly process personal data. Such data consist of both content (recordings of phone calls, text messages, images of webcams, substance of email messages, entries on Facebook, the history of an Internet user's access to Web sites, and so on), and metacontent (data recording the means of creation of transmitted data, the time and date of its creation, its creator, and the location where created). Once gathered, both data and metadata are retained for a certain period of time (as in Tempora) and then organized through platforms of integration (such as PRISM) to become intelligible by means of the visualization of networks, beginning with persons or Internet addresses that are already under suspicion.

Access to greater information about these practices has rightly generated considerable controversy, but there is a danger that both popular and scholarly debate will be reduced to familiar narratives about technological developments reshaping the relations between watchers and watched, or the fulfillment of predictions by George Orwell or Philip K. Dick, or the transformation of representative democracies into totalitarian regimes in the name of protection. Both the information that has become available and the many attempts to assess its significance suggest that much more profound questions must be posed. One question concerns the conceptual disconnect between, on the one hand, dispositions and aspirations shaped by the idea of an interstate world in which each state has a clear vision of its own national security and, on the other, the surveillance practices undertaken by a network of different intelligence services, sharing some information while also acting against their fellow partners and thereby destabilizing traditional understandings of alliances and state behavior. A second question concerns the use of these technologies and the materiality of Internet cables as sources of information whose specific geography gives political advantages to some countries and may reconfigure power politics at the world scale. A third question concerns the strategies of multiple actors to resist these policies by diplomatic and legal strategies, as well as the adjustment of the behavior of Internet users in their everyday practices: whether, for example, they will continue to participate in their own surveillance through self-exposure or develop new forms of subjectivity that is more reflexive about the consequences of their own actions. A fourth question concerns the source and legitimacy of the authorities claiming to act in the name of political necessity and security.

Such questions oblige us to rethink the canons of "surveillance studies" and "critical security studies" that have already criticized views of surveillance as a tool in the service of the most powerful actors and interests. Scholars have promoted promising ways of thinking about the complex and rhizomatic character of interconnected networks of surveillance tools, in which self-exposure has become commonplace, but now also have to make sense of the extension of intelligence gathering together with powerful integrative platforms such as PRISM.

Part of the difficulty of any such rethinking arises from the pervasive sense that whatever is happening in relation to the NSA is shaped by many dynamics (other than the relation between technological innovation and political possibility) which few scholars, and even fewer policymakers, understand. These include social and cultural shifts reshaping the acceptability of, say, new practices of communication, new modes of knowledge, and rapid shifts in the expression of personal identity. More significantly, they include the general shift to the market rather than state law as the ultimate measure of political and ethical value. Most perplexingly, perhaps, we seem to be engaging with phenomena that are organized neither horizontally, in the manner of an internationalized array of more or less self-determining and territorialized states, nor vertically in the manner of a hierarchy of higher and lower authorities. Relations, lines of flight, networks, integrations and disintegrations, spatiotemporal contractions and accelerations, simultaneities, reversals of internality and externality, increasingly elusive boundaries between inclusion and exclusion, or legitimacy and illegitimacy: the increasing familiarity of these, and other similar notions, suggests a powerful need for new conceptual and analytical resources. Perhaps we should be re-reading Leibnitz.

A Mobius Strip of National Security and Transnational Surveillance

Bulk Data Access, National Security, Foreign Intelligence: The Unequal Distribution of Suspicion

The work of intelligence is said to begin from suspicion of dangerous acts committed by a group under surveillance. It then proceeds to the identification of unknown persons related to the initial group, within three degrees of separation (or hops). That is to say, for a suspected person with 100 friends at the first hop, the person in charge of surveillance at the NSA or one of its private subcontractors can, without warrant, put under surveillance all 2,669,556 potential connections at the third hop.[2]

Given the magnitude of the data thereby accumulated, analysts do not read all the content, but rather visualize the graph of the relations that are identified and focus on what seem to be the most significant sections showing specific nodes of connections between data. This is far from a full reading of the contents of such data. It is also far from a scientific procedure which might warrant claims to certainty and precision about the results obtained. It is, rather, part of a process of intuition and interpretation that may vary considerably from one analyst to another. Fears about Big Brother are thus largely irrelevant. The pretense to truth accompanying these visualizations is unfounded, working only to transform suspicion into more impressive forms of expertise through predictions about the actions of individuals when even general forecasting about future trends is quite complicated. What is at stake in this respect is less a marriage between technology and a science of society, more one between technology and a speculative faith in systems designed to "read" big data.

The potential field of suspicion is massive in the sense that it has no end and spreads through networks. But it is not massive in terms of global reach or the surveillance of everyone. This is indeed the main argument made by the different intelligence services. They say that they have objective criteria to restrict their searches and that they cover only foreign intelligence (cf. US-FISA and FISC, GCHQ requirements, French internal directives)—thus, communications involving a "foreigner" at one end will be examined, in priority, in a special circuit. However, it also seems that the system may identify suspicious behaviors of nationals (and will in those cases have to ask for a warrant in the UK and US jurisdictions). The bulk collection of data and the visualization through networks makes it impossible to be certain about the difference between nationals and foreigners. Legality requirements threaten the functioning of the system and so they presume that the law must adjust, not the system. To avoid this "complication," transnational networking between different services has enabled a blurring of the boundaries of domestic and foreign jurisdiction. It seems that the different services in charge of their own national security, working through the gathering and exchange of information, ask other security services to perform some of their tasks, bypassing limitations on foreign intelligence by using "a citizen privacy shopping" to exchange surveillance of their own citizen with another service. In this way, what is national and what is foreign becomes mostly irrelevant for transnationally organized operations.

National Security and Digitization of the Reason of State

These ways of gathering and sharing information have paradoxical effects on national security requirements. National security is no longer national in its acquisition, or even analysis, of data and allies' different national security imperatives may clash, causing trust to disappear. Digitization creates big data gathered at a transnational scale, blurring the lines of what is national as well as the boundaries between law enforcement and intelligence. These trends encourage the move from the judicial framework of criminal policing to preventive, preemptive and predictive approaches and from a high degree of certainty about a

[2] Barak Obama, following one of the 45 recommendations of the review group on intelligence and communication technology, delivered December 12, 2013, seems ready to limit the search without warrant to two hops (in this case 16,340), reducing the scale of the search while keeping the principle alive. Speech January 17, 2014, available online at the Guardian, http://www.my-rss.co.uk/feeditem.php?feed=0&word=&search=laws&item=263734. (Accessed March 19, 2014.) For an interactive search on hops, see http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. (Accessed March 19, 2014.)

small amount of data to a high degree of uncertainty about a large amount of data. The hybridization of private and public actors destabilizes socialization through national state interests and secrecy, opening possibilities for major leaks by persons with different values.

To put this more theoretically, the change and uncertainty surrounding the categories of "foreign" and "domestic" is dispersing them through the webs of connections and transforming the sovereign line that separated them clearly into a Möbius strip (Bigo 2001). By projecting national security "inside out"—through a transnational alliance of the professionals of national security and sensitive data, both public and private—an unexpected "outside in" effect of suspicion is created for all Internet subjects. Many of these "data subjects" react and reject the situation in which all Internet users are treated as potential suspects, rather than as innocent in principle.

The practices of large-scale surveillance by the NSA and its counterparts must thus be understood, not as media-driven scandal which will soon pass, but as indicators of a much larger transformation affecting the way the boundaries of national security function. This is due to the conjunction of three processes that have become interwoven: transnationalization, digitization, and privatization.

This conjunction creates an overarching effect of dispersion that challenges the very idea of a reason of state conducted by a "state" in which the government determines national interests and national security and asks its own services to operate accordingly. Even if it has always rested on exaggerated claims about autonomy and self-determination, the concept of reason of state is now less and less encapsulated in the formula of a national security performed by intelligence services socialized into secrecy and public responsibility, patriotism, and suspicion of services in other nations. Rather, we see the transformation of a reason of state through the emergence of a digitized reason of state performed by a heterogeneous complex of professionals, of sensitive information hybridizing private and public actors. The transnational nature of gathering information that crosses the boundaries of states dissociates the discursive, homogeneous nature of national security interests while reconstructing an aggregate of professionals. These professionals exchange information through digital technologies, produce intelligence according to their own interests, and despise the idea that the rights of all Internet users can create limitations to their projects.

Consequently these transnational guilds of professionals are directly challenging the authority of the professionals of politics which, in principle at least, and within the limits of an international order, had the capacity and authority to define the content of national interests and security (Bigo 2013). They also challenge the authority of national citizens by reconfiguring the ideas of privacy, secrecy of communication, presumption of innocence, and even democracy. It may not be going too far to suggest that what we still call national security has been colonized by a new nobility of intelligence agencies operating in an increasingly autonomous transnational arena.

A Field of Computerized Exchange of Information Between Professionals of Sensitive Information and a Guild Trying to Organize It

If one looks at the number of agencies, the size of their work forces, and the technological capacities of the different intelligence services, it is clear that we cannot use the notion of networks to imply a system of reciprocity and equality. These networks of relations are asymmetrical and hierarchical, as were the guilds in the middle ages with their rituals, codes, and rules of obedience and solidarity.

The NSA has eight times more employees than the DGSE and BND, and seven times more than the GCHQ. In addition, the NSA employs private contractors to do part of their job, so the number of employees could be 12–16 times greater than those of any other agency. Likewise, the NSA has a budget of US$10.8 bn (7.8 bn Euros) a year, whereas within Europe GCHQ's budget of 1.2 bn Euros is well below the NSA, but nevertheless over twice the yearly budget of other agencies such as BND, FRA, or DGSE. This is why it may be more accurate to speak of an Anglo-American guild of professionals extended to other Western intelligence services than to analyze the network as a US-European collaboration on an equal footing, or even a transatlantic collaboration correlated with NATO.

The strength of this guild may reflect the fact that a considerable degree of solidarity had already been created at the end of the World War II, with countries accepting the hegemony of the United States. The so-called "five eyes" (United States–UK–Canada–Australia-New Zealand) is a network of intelligence services, extended recently to Sweden and now possibly France and Germany, and seems to have been the main vehicle through which the NSA has extended its surveillance beyond its own technical abilities in order to have a global reach (especially through the submarine cables already mentioned). This network of security professionals and sensitive information has functioned as a node for the gathering and sharing of data, giving the impression of a strong reciprocal collaboration and a common goal: antiterrorism. Nevertheless, the revelations of Snowden have shown the structural asymmetry of this relation in terms of the exploitation of data and intelligence. Far from a seamless flow of information, power relations structure the game.

Multiple Sites of Resistance

Some partners of the NSA (Germany, Poland, Sweden, Netherlands, even France) have been shocked by the way they have been duped, transformed into instruments when they thought they were collaborators. Trust between the services—which was limited, but nevertheless existed in the name of the struggle against terrorism—largely disappeared when it became clear that spying on politicians, industrial espionage, data mining of the personal information of large populations in order to profile the evolution of consumer choices, and even political opinions about future elections, have been used by NSA analysts. This included spying on the populations of the countries with which they were allied and with whom they collaborated in the "five eyes plus" network. There has thus been a realization on the part of some partners of the NSA that collaboration in support of the national security of the United States has compromised their own national security and interests, and with their own "involuntary" complicity.

The question of loyalty has thus been raised in that the very services in charge of national security have put nations in danger by giving away information to the NSA. The UK has been in an especially delicate position given that GCHQ has participated in aggressive behavior against other partners and EU institutions[3] while being part of the European Union and having signed the EU treaty which requires member states' loyalty. Conversely, the revelations that the NSA has set up files which were "not for British eyes"—because they were important and played against UK interests—have created unease in some UK police services and a certain sense of betrayal, reflecting the loss of the privileged position the UK had with the United States.

In this respect, Snowden's revelations have created a snowball effect of distrust about the positive effects of exchanging data with the NSA and have pushed private providers such as the French company, Orange, to verify its technical infrastructures. They discovered that most of the technologies the NSA has used to gather the information it wanted (almost everything) were dual: first by requesting

[3] GCHQ has been accused of a Belgacom intrusion in order to spy inside the EU Commission and Parliament—an operation codenamed Socialist and undertaken via Quantuminsert.

collaboration in relation to reasonably legitimate matters (mainly connected to antiterrorism and organized crime) and second by fraudulently introducing tools into their collaborators' systems, especially those recently aggregated to the main node (France, Germany, Sweden, Netherlands, and possibly Brazil).

Politicians of these countries have been caught between their official support for the need to gather information against terrorism, their Americanophilia, arguments for a common alliance, and the aggressive behavior of the NSA. If they have largely succeeded in silencing the reservations expressed by some operators within the network (investigative magistrates for example), they have not succeeded with all the private providers, and even less with civil society and the various NGOs. Hundreds of judicial claims, coming from very different actors with very different motives, have been launched and it will be impossible to block them without profound reform.

Games That States Play Along the Möbius Strip

The transformation of territorial lines into a Möbius strip rearticulates the sovereign games that states usually play. While big data collection blurs categorizations of what is "domestic" and what is "foreign," the consequent reconfiguration of the boundaries of the sovereign state into a Möbius strip has in turn become a site, in and of itself, of political struggles, resistance and dissent. Along the Möbius strip, states, social movements, and individuals can play a variety of games, reenacting the meanings of sovereignty and citizenship, security, and liberty. In the case of states, reactions against mass surveillance have varied from assertions of universal rights to reconstitutions of sovereign territorial boundaries, from the digitization of security to the digitization of geopolitics. Several dimensions of the Brazilian government's recent reaction against techniques of mass surveillance are exemplary of the different games that states play along the Möbius strip. This section will address these games and how they shape political struggles around the digitized reason of state.

How to Turn the Möbius Strip Back into Sovereign Lines

Edward Snowden's exposure of NSA surveillance operations in Brazil—including the monitoring of President Rousseff's mobile phone and the collection of data from the country's oil company and, indiscriminately, from Brazilian citizens—triggered a series of actions in several arenas. In addition to the postponement of a state visit to the United States, originally scheduled for October 2013, President Rousseff dedicated her statement at the opening of the United Nations General Assembly to the issue of mass surveillance or, as she called it, "a global network of electronic espionage." The statement condemned the NSA's practices on two grounds: violation of human rights and "disrespect to national sovereignty." Consistent with Rousseff's speech, the most noticeable outcome was the inclusion of privacy rights in the agenda of the UN Human Rights Committee and the introduction of a Resolution at the UN General Assembly, with the support of the German government. Even though the resolution did not mention the United States, its proposal was a way to censure the practices of mass surveillance conducted by American agencies. Nevertheless, contrary to the many accusations of violations of national sovereignty (vocalized by many governments, Brazil and Germany included), what distinguished this reaction was the stage on which it took place and the vocabulary through which it was articulated. At the UN, states are supposed to employ a universal vocabulary, enabling therefore claims for the recognition of privacy as a human right.

The enactment of a universal vocabulary destabilizes the core of mass surveillance practices, bringing to the fore the ways in which they constitute their main object of concern: the "data subject." The "data subject" is a conditional form of existence whose rights are dependent upon its behavior within digital networks. The observation and analysis of specific behaviors make it possible to draw generic profiles and to identify threats and targets. Hence, the degree of separation between the subject and an identified target triggers specific surveillance techniques and defines the rights to which the "data subject" is entitled. Under the digitized reason of state regime, individual rights are conditioned by a specific series of relationships and by the particular positions that the subject occupies within these boundless networks. "Data subjects" are constituted and accessed with regards to their particular position. Their rights depend upon how distant—or not—they are from given targets. This positional articulation is at odds with the cosmopolitan assumptions that underpin the universal rights campaign by the Brazilian and German governments. Their attempts to reconstitute individual rights, and ultimately the regulative idea of an autonomous subject, against the digitized reason of state, might appear outdated and, perhaps, conservative. In this sense, political debates regarding the techniques of mass surveillance at the General Assembly were primarily a struggle between two modes of existence: the data subject and the cosmopolitan subject of universal rights. Nevertheless, the cosmopolitan leaning of the General Assembly resolution was a way to reconstitute the promises of the modern international, not only through the safeguarding of individual autonomy, but also through the assertion of the responsibility of states in protecting it. Against the practices of mass surveillance, states such as Brazil and Germany have tried to turn the Möbius strip back into sovereign territorial lines.

Nevertheless, the cosmopolitan move was not made at the expense of state sovereignty, at least not in the case of the Brazilian government. Within this particular game, the enactment of a cosmopolitan vocabulary authorizes the state to act in order to protect its citizens' rights, including the right of privacy and, as will be discussed below, to protect data. Hence, at the UN, the game that Brazilian authorities are playing is actually an attempt to reconcile individual autonomy, state sovereignty, and universal rights. Although strategically this game challenges the foundations of the digitized reason of state, the techniques mobilized and eventually deployed to protect citizens' rights may, in effect, reinforce it. Claiming that privacy is a human right, Brazilian authorities support the creation of a multilateral and multi-stakeholder arrangement "capable of ensuring freedom of expression, privacy of individuals and respect for human rights" (Rousseff). Yet, the same claim authorizes the Brazilian government to declare its resolve to "do everything within its reach to defend the human rights of all Brazilians and to protect the fruits born from the ingenuity of [its] workers and [its] companies" (Rousseff). That is, what President Rousseff has in mind is a set of domestic measures intended to build up national capabilities to protect the privacy of Brazilian citizens against the threat of US mass surveillance.[4] Even though the multilateral regulation of cyberspace and the national capacity for the protection of citizens' privacy might complement each other, the prospects for the development of techniques of national protection may trigger another game: a digitized geopolitics.

The Digitized Reason of State and Its Digitized Geopolitics

The policies announced by the Brazilian government to contain the threats presented by US mass surveillance techniques include the increase of international Internet connectivity and domestic content production. According to Brazilian

[4] Al Jazeera, Brazil is Beating United States at its own Game. Available at http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html. (Accessed March 19, 2014.)

authorities, the production of domestic content, such as a national email service or a national social media, would allow Brazilian citizens to keep their data within national borders. The debate regarding the creation of a "European data cloud" raises similar issues. Indeed, Brazilian authorities are not alone. In a similar vein, Dutch authorities have tried to keep the government's data out of the reach of American companies, while the European Union is discussing the possibility of isolating data storage from US mining techniques, and the German government is trying to keep traffic local by warning Internet users when they pull out of European cyberspace. Not to mention the well-known cases of the Chinese "Great Firewall" or the Iranian "Halal Internet." In every case, states are thickening their digital borders. Although one should not overlook the differences between what Brazilian or German authorities are doing to protect data and privacy, and what the Chinese government is doing with its firewall, in each of these cases a massive infrastructure has to be built. Hence, a vast array of technologies, legislations, and expertise has to be developed and deployed either to protect data, to control traffic or even for surveillance. On top of all of these investments in state capacities for protection or surveillance, security professionals and intelligence experts have to be mobilized to manage the national systems.

By building their fortresses in the clouds, states shift from the cosmopolitan move to strategic play. While the first move is based on claims to universal rights, the strategic game is based on claims to state sovereignty, or in this case cyber-sovereignty. Within these strategic games, very often, the reference to universal rights fades and ends up being replaced by a strategic reasoning embedded in uncertainty and fear. Concepts such as national interest, national or state security, espionage, and war come to the fore when state representatives go public to support policies and techniques that protect a given society. Cyberspace is, then, described as a US-centered space, and so US cyber power should be balanced through the development of national cyber capabilities or international coalitions.

In the Brazilian case, attempts to expand international Internet connectivity (within the regional space but also on a global scale) are consistent with the idea of protecting national data as well as of balancing or competing with the US position in cyberspace. The program comprises three articulated initiatives: the construction of intercontinental undersea fiber cables, many of them connecting Southern countries; a satellite program, planning to launch a "Geostationary Defense and Strategic Communications satellite" in 2016; and, finally, an overland fiber cable connecting countries in South America. One of the core moves in this game has been the announcement of a BRICS cable, connecting all of the BRICS countries independently from the United States.[5] Every single initiative articulates different branches of the Brazilian government with Brazilian or transnational corporations, and every project is transnational by its own nature.[6]

This new game results in an expansion of the digitized reason of state. Instead of evading the Möbius strip, states play geopolitics within it. The digitized geopolitics assumes that cyberspace is a battlefield and that states must build up their own cyber capabilities in order to defend themselves and/or must engage in international coalitions in order to face the challenges posed by mass

[5] Washington Post (2013). *Experts see Potential Perils in Brazil Push to Break with US-centric Internet over NSA Spying.* Available at http://www.washingtonpost.com/world/europe/experts-see-potential-perils-in-brazil-push-to-break-with-us-centric-internet-over-nsa-spying/2013/09/17/c9093f32-1f4e-11e3-9ad0-96244100e647_print.html. (Accessed March 19, 2014.)

[6] Brazilian telecom companies are constructing the undersea cables with public or international funding. For example, the South Atlantic Express cable connecting Brazil and South Africa is funded by the Bank of China; the satellite is a joint venture of the state owned Telebras and the private Embraer with technology provided by the French-Italian Thales Alenia. Al Jazeera, Brazil is Beating United States at its own Game. Available at http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html.

surveillance and digital espionage. The paradoxical effect of this particular game seems to be that states' resistance against mass surveillance ultimately reinforces the digitized reason of state regime. Reproducing the opposition between security and freedom, while playing the digitized geopolitics game, states might end up subsuming citizenship and rights to the positional logic of a data subject. While fighting against mass surveillance, states may create the appropriate conditions to conduct mass surveillance themselves.

Human Rights and Privacy in the Age of Surveillance: The Power of International Law?

The Snowden revelations regarding mass surveillance have not only had very substantial political repercussions through 2013 and into 2014, but have also raised profound legal questions. In this section, we examine some of these questions from the perspective of the political moves around them. We will limit the legal detail to a minimum, instead focusing on what it means for the international relations storm which the revelations have unleashed.

Two interconnected but separate human rights issues arise with regard to mass surveillance. The first, which is the most fundamental but the most frequently ignored, is the right of every person to respect for his or her private and family life. The second, which is generally the subject of more substantial political and media noise, is the duty of states to protect personal data. Those political actors who have an interest in promoting the legality of mass surveillance usually put forward two arguments. The first is that national and international security is always an exception to both the duty of every state to respect people's privacy and the duty to protect personal data. This is the most trenchantly defended of arguments as when this one falls away, those actors seeking to justify mass surveillance find themselves on very weak legal ground. The second is that states' obligations to protect personal data are subject to very different rules and requirements according to the political preferences of different states. Thus, as there is no harmonization of the specific rules as to what is acceptable data protection internationally, states which are exercising their national and international security prerogatives only need to fulfill their own national data protection rules.

Right to Respect Privacy and Right of Data Protection

Before engaging directly with the arguments and examining how political actors dissatisfied with them have responded, we would like very briefly to clarify the relationship of the right to respect for privacy with that of data protection. The right to respect for a person's privacy is the overarching international human right. It is found in the UN Universal Declaration of Human Rights, 1948,[7] and its legal form is found in the UN International Covenant on Civil and Political Rights, 1966.[8] Any interference with the privacy of a person must first and foremost be subject to the consent of that person. The right to consent or refuse use of personal data belongs to the individual, not the state. Further consent is only valid if the individual knows exactly what he or she is consenting to. This aspect of the right requires there to be purpose limitation regarding the collection and use of personal data and prohibits function creep. Where the state seeks to interfere with the right to collect and use personal data which constitutes an intrusion

[7] Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[8] Article 17(1): No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.

into the privacy of the person concerned, such interference must be justified by the state authorities. First it must be permitted by law, and that law must be sufficiently clear and public that everyone can know what it is and how to adjust their behavior accordingly. Any exception permitted by law to a human right must be interpreted narrowly. It must have a legitimate objective and be necessary to achieve that objective only. There must be no alternative which would be less intrusive into the life of the person. There must be judicial oversight of any state interference and a person affected by interference must have access to justice to challenge it. Mass surveillance by its very nature is not targeted at any person specifically; thus the possibility to justify the interference with the privacy of any person individually is an exceedingly difficult task. Where such mass, weakly targeted surveillance techniques have been used in Europe, the Human Rights Court has found them inconsistent with the right to respect for privacy. Mass surveillance is, by definition, arbitrary.

States' duty to protect data arises from the person's right to respect for his or her privacy. Where states interfere with people's privacy, they must fulfill strict rules to justify that interference. Further, states are under a duty to ensure that private sector actors do not breach a person's privacy. Thus, states are under an obligation to regulate the collection and use of personal data by the private sector. This gives rise to the obligation of data protection. The duty to protect personal data arises when personal data are being used by state or private actors and are designed to ensure that the use is consistent with the individual's right to respect for his or her privacy. It is for this reason that there are many different types of regimes of data protection depending on the country under consideration. How states go about protecting data is for them to determine; the key is that personal data must be protected because the individual has a right to respect for his or her privacy. The content of the human right to respect for privacy of the person is not variable.

The US Position Regarding International Human Rights Law and the Brazilian German Initiative

Moving, then, from the state of human rights to the political struggle regarding mass surveillance, clearly the US authorities are faced with a dilemma in international human rights law, an area where they have always been rather wary. The 1950s approach to international human rights law was to claim that the instruments do no more than set out principles, they are not "real" law in any significant way and are certainly not available for people to rely upon. This political position has been undermined by the development of very precise international obligations, the establishment of Treaty Bodies with jurisdiction to receive and adjudicate on complaints by individuals regarding alleged breaches of their international human rights and the embrace of international human rights law by national courts. The principle approach to international human rights law is no longer tenable, it is a fig leaf deployed occasionally by states seeking to act arbitrarily.

As the Snowden revelations rose up the scale of international issues, a number of states, primarily led by the Brazilian and German authorities, began to address the issue of how to deal with US mass surveillance and interception of communications. There was much discussion about bilateral negotiations and unilateral action (for instance, building new cables which avoid US territory) and so on. However, it was rapidly evident that bilateral and unilateral approaches were not going to be satisfactory. In Europe, the fact that the UK authorities were carrying out mass surveillance for their US counterparts and others (the so-called Five Eyes), yet were not only members of the Council of Europe but also of the European Union, was only one example of the problem of unilateral or bilateral approaches. Clearly, for most actors, only multilateral efforts were likely to bring results where the weight of the United States and some of its collaborators could be counterbalanced by a loose alliance of other states. As soon as the issue is defined in this way, the obvious venue to commence a response is the UN General Assembly, and the territory on which to prepare the response is that of international human rights obligations—the prohibition of arbitrary interference with people's privacy.

This is the road which the Brazilian and German authorities have followed. By August 2013, moves were afoot for a resolution of the General Assembly. Five non-governmental organizations—Access, Amnesty International, Electronic Frontier Foundation, Human Rights Watch and Privacy International—were closely linked with the efforts, applying pressure for a strongly worded resolution. The Brazilian and German authorities were by no means alone in their efforts to achieve agreement on a UN General Assembly Resolution. Many smaller states, most notably Austria, Hungary, Liechtenstein, Norway and Switzerland, but also others, very strongly supported the work from the beginning, even seconding staff to assist with the workload. The matter was assigned to the General Assembly's Third Committee and it is there that the tense negotiations on the wording of the Resolution took place. A text was adopted on November 26 in the Third Committee, and on December 18, 2013 it was adopted without a vote in the General Assembly of the UN.

The Resolution is based on the right to respect for privacy in the Universal Declaration and the International Covenant on Civil and Political Rights 1966 (ICCPR) with specific reference to the prohibition on arbitrary interference. It ties the right to privacy to the right to freedom of expression—if people are subject to mass surveillance they are no longer able to express themselves freely. The so-called chilling effect, the preamble to the Resolution, insists on the negative impact that surveillance and interception of communications, including extraterritorial surveillance and interception on a mass scale, has on the exercise and enjoyment of human rights. The Resolution calls upon states to respect the right to privacy and prevent violations, to review their procedures, practices, and legislation regarding surveillance of communications and the interception and collection of personal data, including mass surveillance, interception, and collection, with a view to upholding the right to privacy. It also calls upon states to ensure the full and effective implementation of all their obligations under international human rights law and to establish or maintain independent, effective, domestic oversight mechanisms capable of ensuring transparency and accountability of states' actions.

Most importantly, the Resolution directs the UN High Commissioner for Human Rights to present a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale, and to report to the Human Rights Council it its 27th Session (September 2014). The current High Commissioner, Navi Pillay, a South African jurist with a very impressive human rights career, was appointed to the post in 2008. She is no stranger to the problem of the right to privacy and mass surveillance, having already spoken on the subject at the Council in September.

The UN Human Rights Council (composed of 47 states elected by the General Assembly) has also already engaged with the issue. The matter was on the agenda of the 24th Session of the Council held in September 2013. The High Commissioner noted, at that meeting, that the threat which mass surveillance poses to human rights is among the most pressing global human rights situations today. Many state representatives present at that session referred to the report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue on freedom of expression in the Internet age May 16, 2011) which had already outlined many dangers of state surveillance and its impact on free speech. What is perhaps surprising is that the September and December 2013 meetings of the Human Rights Council received so little press coverage. The meeting was well attended by state representatives, and the discussions were incendiary in their condemnation of mass surveillance and interception of communications. Many state representatives attended the meetings with statements of condemnation of mass surveillance and interception of communications already prepared and agreed with neighboring states on whose behalf they were mandated to speak. While one might well expect the German representative to present a text on behalf of Austria, Hungary, Liechtenstein, Norway, and Switzerland, it is perhaps less obvious that Pakistan, speaking on behalf of Cuba, Venezuela, Zimbabwe, Uganda, Ecuador, Russia, Indonesia, Bolivia, Iran, and China would also present an agreed text condemning the practices. While the counter move, particularly in respect of this second set of countries, is usually to attack them on the basis of their internal practices of surveillance and suggest, if not accuse, them of hypocrisy, the fact of the intervention nonetheless must be noted, likewise the possibility that a group of states with serious disagreements among themselves would choose common ground on this subject.

The next step will be for the High Commissioner for Human Rights to prepare and present her report to the Human Rights Council in September 2014. Undoubtedly, her team will be presented with substantial amounts of information, evidence and legal argument to assist in the writing of the report.

Intelligence, Democracy, Sovereignty: Which Demos for What Security?

Thanks to the documentation distributed by Snowden and others, we now know more than we did about the character and extent of the intelligence gathering practices of various agencies charged with enhancing our security. Precisely what we know, what we don't know, and what our limited knowledge adds up to remains uncertain, in ways that challenge both scholarly analysis and our sense of how we should respond through policies, procedures, institutions and collective actions. One may or may not be disturbed by what has become known, but what has become known certainly disturbs conventional understandings of what it means to think about practices of security—and not only security. On the other hand, the old suspicion that agencies claiming to secure our life and well-being often turn out to be extremely dangerous retains considerable wisdom.

It is in this context we can appreciate many of the initial responses to the immediate consequences of the patterns being identified. Privacy, human rights, and the rule of law have become deeply entrenched, even if imperfectly achieved, principles of modern societies, especially those affirming some kind of liberalism. Snowden has brought considerable evidence that such achievements are being treated with contempt, whether willfully, and even conspiratorially, through ignorance and naivety, or through structural processes no one quite understands. Moreover, contempt has been redistributed toward friends as well as enemies, to citizens and foreigners, in ways that generalize the taint of suspicion and throw into question everything we thought we knew about the role of individual conscience, freedom of expression, innocence and guilt, liberty and responsibility, public and private. Apologists for more intrusive and secretive forms of security often invoke extremist narratives about the threats we may face, but it is not difficult to imagine equally extreme narratives about the evisceration of the forms of modern subjectivity and self-determination that give security agencies much of their legitimacy. What, after all, are they supposed to be securing?

"Democracy" is unlikely to be the immediate answer given by security professionals, despite the rhetoric of many politicians. The state or the nation would be preferred: the condition of the possibility of a collectivity of citizens grounded in a specific geographical location that may or may not achieve democratic forms of polity; or perhaps the international system that is the possibility condition of this condition of possibility; or, more accurately, the delicate or clumsy interplay of states within a system of states that gives us some possibility of reconciling our claims to particular citizenships and nationalities with our universal status as human beings. Traditional understandings of security may be torn between nationalist and internationalist camps, between national security and collective security as the UN Charter puts it, but the obvious weaknesses of both camps only serves to underline their mutual dependency as expressions of the competing principles of self-determination and universality shaping modern political life. One major complication here is that some states, and currently one state, act as if they are both particular and universal, merely a sovereign state with a national security problem but also a global hegemon responsible for something more encompassing. Other complications include the fact that economic processes are not always subsidiary to the political order of internationalized states.

What is especially interesting about the patterns that might be read into the information released by Snowden is the potential confirmation of claims that we now live in a world that is organized neither within states acting within a system of states, nor an embryonic hierarchy of the kind envisaged by theorists of globalization, global governance, and so on, nor a new kind of empire or concert of great powers. Moreover, it seems unwise to assume that these patterns can be understood without some grasp on contemporary shifts toward globalizing markets and corporate wealth as the primary measure of economic and even political value. Some of the responses to Snowden's revelations suggest that there is still life in the old national/international model. But many also suggest that something less predictable is occurring. Some indications of this unpredictability are suggested by the many ways in which the practices of intelligence agencies, like the NSA, challenge our assumptions about democracy.

In this context, it is important to remember that democracy, along with other forms of political pluralism, is conventionally something that might be limited, or even sacrificed, to secure the primary order of nation-states in a system of such states. Yet what is especially at issue in recent revelations is not just the traditional question of when it might be possible to suspend democratic norms in order to mobilize more effective security operations or to draw a sharp line between a civil arena in which democratic norms are appropriate and a security arena in which democracy must give way, although many apologetic narratives certainly reproduce this tradition. It is, rather, the apparent rearticulation of boundaries both between states, and between the state as the seat of political necessity and civil society as an arena of political and personal liberty; and thus, in both cases, between the demands of security and the possibilities of liberty or self-determination. If this is indeed part of the pattern that is emerging, the meaning both of security and of democracy, as well as the relation between them, will become radically destabilized, and not obviously for the better.

In addition to the previous discussions of privacy, the rule of law, and various attempts to resist imperial pretensions, four other lines of analysis are worth emphasizing in this respect. They all concern the limits of the dichotomies between national and international, state and civil society, liberty and security, and democracy and knowledge that are invariably reproduced in conventional analysis and public debate. The uncertain status of sovereignty is apparent in all four cases (for reasons broadly outlined in Walker 2010).

First, our political world is neither national nor international, though the presumption that it is still sustains widely pervasive political ideals. Snowden's documentation confirms that uncertainties about how we should understand democracy given the dynamics that are reshaping relations among states, and between states and civil societies, are rapidly merging with uncertainties about how we ought to be locating the political orders being structured in relation to new networks of intelligence and security agencies. We are clearly not talking about the classical image of national security states here. These networks are variously international and transnational, with cartographies that look more like electrical circuits than territorial properties. Boundaries have become elusive phenomena, in ways that demand unfamiliar ways of understanding forms of subordination among various subsystems, conflicted loyalties and divided citizenships, and dislocations of the spatiotemporal frame within which we know where we are, when we are, and thus who we are. Yet while they may be elusive, boundaries are not being erased. It may be that the NSA and other intelligence agencies work through networks that evade many boundaries, but their very reason for existence is precisely to affirm boundaries of inclusion and exclusion, both familiar and unfamiliar. Given all the evidence of new patterns of inequality around the world, we should clearly be very wary of the prospect of novel forms of inclusion and exclusion enacted through new technologies of population control.

Second, a key feature of the most influential accounts of democracy throughout the twentieth century has been a distinction between state and civil society and related distinctions between public and private. These distinctions have often been fuzzy. Nevertheless, recent evidence suggests an even more sustained erosion of such distinctions and the presumed right of state agencies to penetrate deeply into the everyday worlds of civil society and private life. This does not take the form of the totalizing police states of recent memory. It is nevertheless clear that new procedures for intelligence operations, data-gathering, mobilizing suspicions, and identifying potential threats, especially in ways that rely more on computer manipulations of evidence that may or may not have empirical credibility, and which rely on statistical probabilities within abstracted populations to identify particular individuals, pose dangers to established liberties and rights that are analogous to regimes we prefer to imagine as swept away in revolutions, democratizations, modernizations. Part of the analytical difficulty here arises from a double dynamic: On the one hand, we see a complex interaction between public and private agencies, not least agencies of corporate and market capital rather than of liberal citizenship; and on the other, we see evidence of complex networks of intelligence and security agencies that seem to have achieved considerable autonomy from both state and civil society or, in a related language, from both state sovereignty and popular sovereignty.

Third, far too much political analysis and debate now begins with security, as if security is a problem and principle that stand on its own, or is even the primary principle that trumps everything else; the tendency is commonplace even among supposedly "critical" literatures. Although some people have insisted on this primacy as a simple (socio-Darwinian) fact of life, no discussion of modern democracy, or any other principle of modern politics, can afford to make such an elementary mistake. As so many of the canonical authors appropriated by the security analysts of our time have recognized (Machiavelli to Hobbes to Kant to Clausewitz to Schmitt and even on to some versions of the concept of national security), claims about security imply that there is something to be secured. That something has generally referred to a specific political community attached to principles of liberty and equality internally, and with a capacity for self-determination in relation to other such communities. Most obviously in the present context, this has generated the longstanding tension between claims to liberty and claims to security. This is a tension that has been effaced by the division of intellectual labor that has turned security into an autonomous specialization to be pursued with little regard or considerable contempt for the liberties of "the people" in whose name security is used as a trump card. The precise character of this tension has also been depoliticized by repeated claims that a "balance" must be struck between two different values.

Yet the relationship between liberty and security cannot be understood as a balance in the usual senses of this term. Security names the conditions under which the primary value of liberty must reach its limits, under which normal assumptions, ethical injunctions and laws must be suspended. Any such suspension is classically the responsibility of the sovereign state and is thus at odds with the responsibilities of a sovereign people. Consequently, the relationship between these two antagonistic understandings of sovereignty has to be negotiated. In some influential (authoritarian, totalitarian, fascist) readings, negotiation simply means a sovereign decision to suspend the norm in the name of a people or nation: that state sovereignty must trump popular sovereignty. Democratic traditions have been forced to work out various accommodations with the demands of security as a limit condition, usually by insisting on close scrutiny of decisions, divisions of institutional powers, and an insistence on the legal conditions under which laws might be suspended. This is not a choice between commodities in a market. Rhetorical invocations of a balance simply obscure and threaten what goes on at what may be the most important, intense, but neglected site of modern democratic practice. The way is then open for *de facto* claims that the responsibilities of sovereignty rest with those charged with our security and that the space for negotiation open to those supposedly being secured must be reduced. Given both the range of plausible threats confronting contemporary societies, and especially the capacity of a broad range of security agencies to highlight some threats rather than others and to push the need for security as the primary principle governing our lives, what used to be understood as authoritarian options are made to seem desirable, even natural.

Finally, but absolutely not least, the unchecked demand for secrecy on the part of intelligence and security agencies is devastating. Democracy has always been tied to the quality of knowledge within a demos: From the Greek *polis* to the European Enlightenment to the value more recently placed on education, investigative journalism and public opinion, most conceptions of democracy rest on some sense that people are able to think and make judgments for themselves. The cult of secrecy takes us back to far too many historical cases in which claims were made that "the people" cannot afford to know what's good for them while their sovereign needs to know as much as they can about the people whose sovereignty they claim to express. So, whose authority are we talking about here? Or as Thomas Hobbes might have put it, how is authority now authorized?

Subjectivity and the Surveillance of Cyberspace

The transformation of the citizen into suspect is not a new phenomenon, as Hobbes confirms in his discourse on subversion and sovereign power. Where Hobbes' world is territorially confined, the world of late modern security agencies is global and transnational. The differentiation of citizen and non-citizen can be witnessed at every border crossing where the non-citizen is subjected to biometric identification, full bodily exposure, and other modes of scrutiny; the traveler, meanwhile, is simply resigned to the panoply of humiliating subjectivizations. There is, in this regime of security practices, this terrain of the border crossing, a learning process that governs behavior, our threshold of tolerance of such interventions, and in many ways our now established indifference or even complicity in the discomforts of the other.

It is this indifference that is put into question with the Snowden revelations—that all citizens of any state, leaders and led alike, any communicating being, any user of late modern communications technologies, is rendered a suspect.

However, the concept of suspect is now thoroughly transformed, for we are no longer able to confine it to its juridical sense, which refers to criminality, nor are we able to confine its meaning to its socio-political iteration relating to enmity or potential subversion.

What is clear is that the subject of surveillance is now a subject whose communicative practices are seen by the surveillance agencies as of potential informational value or utility, where this value might be related to security or the economy. It is hence not that we are all suspects now, but rather that our data inputs and networks might be deemed of value, understood in terms of utility, at some point in the future. As the subject communicates in cyberspace, there might be some awareness that the communication network is variously being monitored, registered, stored; however, there is a lack of knowledge as to the informational utility accrued to that communication by the surveillance agencies. How the mass surveillance of communications might impact on behavior is clearly a pertinent question; however, just as the subject who travels adapts and conforms to the requisites of travel, so too in this instance there will be adaptability and creativity in the modes of self-government that prevail in the face of our late modern intensification of surveillance practices.

The complex intersection of the public and the private is nowhere more sharply apparent than in cyberspace. There is here both intimacy *and* a public presence. However, it is the intimate that prevails, irrespective of the fact that the subject of cyber-communicative practices is fully aware that cyberspace, as such, is open to the world, vulnerable to the gaze of the stranger, variously the hacker, the marketeer, or even the state. "Digital being" (see Negroponte 1995) is connected and networked being, present in this distinctive terrain of social interaction, a space drawn and enabled by networked codes that recognize no boundary as such except the technical. The cyber subject is figured and configured as a being that emerges and is produced by forms of disembodied performativities that come to constitute cyberspace (see, for example, Luke 1999). Luke suggests that cyberspace might be understood as a "social structure," where "new subjectivities" and forms of agency are produced. More usefully, however, we might understand this terrain as the manifestation of a space, the cartography of which is a multitudinal array of overlapping and intersecting lines and nodes reflective of the billions of communications worldwide. Yet, in among this networked complexity, the "practical consciousness" of the digital being assumes intimacy despite the odds.

What is often represented as a significant generational shift reflects the individual self-revealing all, not just to friends and family, but potentially to all "customers" using social network vehicles. The overriding assumption of those who communicate in this manner, especially those in liberal democratic societies, but certainly not confined to these, is one of sovereign control, a sovereignty of selfhood understood in terms of the freedom to express, communicate, and mobilize on deterritorialized terrain that can potentially defy structures of power and domination. The defiance of distance is here somehow equated with the defiance of territorially bound authority, so that even where such authority seeks to assert presence, the imaginary is one of possibility, and even of transgression. This was the narrative that fed interpretations of the so-called Arab Spring, the London riots, the anti-globalization movement, and other expressions of protest and resistance across the world (see, for example, Gerbaudo 2012). Here was, and we might say is, the instantiation of a global public sphere (Castells 2008), the communicative practices within which could variously hold authority to account, mobilize within and across territorial boundaries, and in so doing come to constitute an altogether other space, a cosmopolitan interconnected world, where the cosmopolitan is at once of difference and homogeneity.

However, it is this precise blurring of boundaries, this limitless terrain of the possible—where difference can inhabit the familiar, the homogeneous—that calls forth, that challenges, a security apparatus which, as Foucault (2007) tells us, does not function along the model of repression, but rather one of production, of allowance and license. This is the triumph that is liberalism, for here any repressive practice is a regressive practice. It is a letting down of the side in all its sophisticated achievement, all its distinguishing hallmarks—that this is neither Mugabe's Zimbabwe nor Communist China. The liberal example is one of security through liberty, not security at the expense of liberty. Cyberspace had come to represent the technological manifestation of a transformative liberty where communicative practices—of the political, sociocultural, pedagogical, and economic kind—could take place. The question for political authority, and we are focusing here on liberal political authority, was how to regulate this terrain of unbridled communication, what technologies of control could be mobilized that in themselves were not subject to the limits of state boundaries and state-defined sovereign authority. If such technologies could be created, they too had to be of the network kind, digitally defined, of software and not hardware, hidden from view and yet transnational and global in their reach.

Informatics is now the discipline of choice for liberal power. Yet despite the focus on software, on codification expertise rendered in digital form, the hardware too is important in the materiality of technologies designed to control this space of the limitless. From computer storage disks to undersea cables, these are the technological, engineering elements of a machinery that services the freedom to communicate *and* the capacity to monitor and control. Within these frameworks of disciplinary knowledge, as with all knowledge systems and the discursive formations that ensure their reproduction, the epistemic subject steers an uneasy terrain, between politics and government, resistance (we might think of groups such as Anonymous or Hacked-Off; see Coleman 2011) and employment, to service the digital market or the state. The difficulty is that there is no dualism or opposition between these, for each draws on the other. Thus, the world of the resisting hacker, an expertise developed in the intimacy of the study, is drawn upon and perhaps perfected by the resources available to the service providers or the state. Rarely is the move made from the world of the state to the individual resister. Power comes to permeate knowledge, and the subject produced in this complex matrix is always already complicit, involved somehow, in its reproduction. To trace these connections, to map out not just the networks and their nodes, but these intricate imbrications of power, knowledge and subjectivities is the task of any critical intervention on cyberspace, its everyday constitution through practices and frameworks of knowledge, and its constitutive power in subjectivization.

Many might claim that virtual communications mean the "end of privacy" (as predicted in Whitaker 1998). This is the context into which the Snowden revelations enter. For irrespective of the background knowledge we, as inhabitants of cyberspace, have of the possibility and even actuality of the profile as the advertiser's dream in a global digital market place, the game shifts to an altogether different gear when the profiler is the state and, more significantly still, when the profiled can be anywhere in the world. A space wherein the defiance of technical obstacles to communication was translated in many instances as the defiance of power was, thanks to Ed Snowden, suddenly revealed to be subject to the most interventionist penetration of the communicating subject by a sovereign power that views the world within its remit of operations. In this deterritorialized articulation of power, limits seem inconsequential; distinctions between friend and enemy, domestic and international, public and private seem to dissolve. In this "dragnet" world of surveillance, every instance of communication is recorded digitally, variously stored, and triumph—often portrayed in the leaked

NSA papers in the form of the smile symbol (see the Guardian's NSA Files for the recently revealed papers under the operation labeled "Dishfire")—is defined as the capacity to capture hundreds of millions of SMS communications per day.

Politically, language comes to be the terrain upon which, and through which, modes of legitimization and delegitimization take place. The preferred terminology for defenders of the NSA and GCHQ is "bulk access" as opposed to "mass surveillance."[9] The latter is reminiscent of the Stasi in East Germany, and any likeness to Stasi activities is disputed. The term "bulk access" is suggestive of operations that seek the discovery of the "needle in the haystack," the individual terrorist, or cell of terrorists determined to enact an atrocity somewhere and at some unpredictable time. Indeed, the British Foreign Secretary, William Hague, suggested as much when he stated "if you have nothing to hide you have nothing to worry about." The surveillance operation is here deemed a sieving operation, one where the "mass" runs through the sieve unobserved and unobstructed, while the one singular aberrant communication is caught, and through this the potential perpetrator of an act of terrorist violence. Where the communications of world leaders and oil companies are also caught in the dragnet, these are the unfortunate, collateral instances that a bulk access operation might unintentionally capture.

However, if we insist on the term "mass surveillance," the focus is on the "surveillance" of the "mass," where mass can be understood to mean not the biopolitical terrain of population, but much more radically the "multitude" of singular and networked communications subject to surveillance, even though the "data" as such might appear digitally in a networked profile revealed by "metadata" or even "content." The subject of surveillance is hence not simply population, though the "profile" can be said to be carrier of particular populations, but above all the individual subject of communication. It is in this sense that the space of intimacy is, we now know, absolutely penetrated by these agencies, so that a profile is constructed from the digital trace left by the communicating, interactive subject.

The trace will be left in all its intimacy and with the full knowledge that it is no longer private and that the agencies involved in surveillance have access. The formula, liberty through security, when understood normatively, provides no limits to such access. However, the positive conception of rights does, for this is the break, the limit recognized in law, as indicated elsewhere in this article, where privacy is conferred not just cultural, but also juridical value.

Living with Surveillance: Resignation, Perplexity and Resistance

Whatever the specific responses to Edward Snowden's revelations about mass surveillance and the NSA, it is clear that public opinion has been piqued and many around the world are discussing what we are progressively discovering about security agencies and national intelligence. It is equally clear that members of the establishment have moved quickly to underscore the need for such surveillance in the interests of "national security" or "public order." The official response of President Obama to the Snowden leaks, stated in January 2014, is to reinforce claims that government mass surveillance is necessary and to focus attention on private sector corporate surveillance as requiring more oversight (Podesta 2014).

But what of ordinary citizens and consumers, going about their everyday lives with an increasing sense that maybe their activities and communications are

[9] The term "bulk access" was used by Sir David Omand, former Head of the UK's GCHQ as the more appropriate descriptor of NSA and GCHQ activities. See "Mass Electronic Surveillance and Liberal Democracy," Research Centre in International Relations, Department of War Studies, King's College London, January 21, 2014.

tracked and monitored more than they realized? There's nothing as direct or as in-your-face as Big Brother on a glaring telescreen, of course, but rather a more Kafkaesque unease that the ostensibly innocent metadata (the location, duration and recipients of calls, for instance) do in fact have consequences. But it all seems so fluid, slippery, and hard to grasp. Indeed, it seems to match the very quality of relationships characterizing a consumer-oriented culture—fissiparous, mutating, and flowing in ever-changing channels and conduits. This has been called "liquid surveillance" (Bauman and Lyon 2013).

Understanding public opinion is notoriously difficult but by approaching the question from several angles it may be possible to take a reading, to sense what may be happening as people respond to the revelations. There are direct measures—such as polling or using more in-depth interviews and ethnographies—and indirect approaches, placing the matter in cultural and historical context and attempting to discern the signs of the times. Each has a place, and we can at least make a start, albeit recognizing the difficulties stemming both from the fact that only a few months have elapsed since Snowden initiated his program in June 2013, and the fact that experiences vary extensively across the regions and countries affected by US-based surveillance.

An Angus Reid Global poll toward the end of last year (Reid 2013) showed that what you think of Snowden depends partly on where you are. Thus, 51% of Americans regard Snowden as a hero for "letting the public know that our governments are running electronic surveillance programs that threaten people's privacy," while 49% consider him a traitor who "threatens western intelligence operations." Yet 60% say widespread government mass surveillance is unacceptable. However, in other countries, support for Snowden is higher: 67% of Canadians and 60% of Britons view his whistle-blowing as positive. Only 5% of respondents in Canada trust government to guard their data, and this only rises to 7% in the United States. Whether in the United States, Canada, or the UK, it is clear from these results that a substantial proportion of the population are concerned about government surveillance and that there is a high degree of cynicism about what governments do with those data.

As the Snowden news is so recent, there is little in-depth analysis of people's views on government-led mass surveillance, let alone post-Snowden ethnographies of how people now organize their daily lives in relation to online data. Given this, we have to fall back on broader and longer-term probes into attitudes. Snowden's work has disclosed evidence of the extent to which the NSA and related agencies rely on Internet companies and social media platforms such as Facebook for access to transactional and interactional data. But for most social media users, surveillance as hierarchical power seems to have little salience unless they live in conflict zones or in countries with overt political repression. Much more likely, they engage in social surveillance (Marwick 2012) where, in Foucault's "capillaries of power," the power differentials of everyday interactions are more immediately significant than whatever the NSA and its cognate agencies are doing. This is not to say that awareness won't rise, particularly in relation to global events such as the-day-we-fight-back coordinated online resistance on February 11, 2014.

The broader context of the Snowden revelations is not merely the decline of political participation within liberal democratic states but also, as Agamben has suggested, the breakdown of politics itself. Agamben insists that under the sign of security today's states have shifted from politics to policing and from governing to managing—using electronically enabled surveillance systems—thus undermining the very possibility of politics (Agamben 2013). That this occurs simultaneously alongside the growth of all kinds of surveillance, not just those associated with communications and transactions, augurs badly for the chances of a revived politics, especially when, at a mundane level, cultures of surveillance seem so innocuous.

Three sorts of factors probably help to indicate why surveillance of all kinds still appears to be publicly acceptable to many, although it must also be noted that these factors may overlap to reinforce or weaken each other in specific contexts.

The first is familiarity. Surveillance today is so pervasive, and has so many dimensions, that it has simply become part of everyday life. Surveillance is around us in so many contexts, not just the obvious (or, today, not so obvious because they are miniaturized) video cameras in the street, shopping mall or school, or the security procedures at the airport, but also in the very buildings, vehicles, and devices in use from day to day. Surveillance is embedded in cars (GPS, Internet, data recorders and hi-definition cameras) and buildings (access card systems, sensors). So many of these are simply taken for granted; they're domesticated, normal, unremarkable. Many people no longer notice them and certainly do not think about their surveillance capacities (New Transparency 2014).

The second is fear which, many argue, has become more significant since 9/11 (Lyon 2003; Bauman 2005). Government, security companies, and the media play cynically on the fear factor, which has chilling as well as direct effects. Fear works for corporations trying to sell new equipment; for governments which see their task as allowing market forces freer rein and maintaining security; and for the media which depends on polarizing "good guys versus bad guys," especially if the "bad" can be thought of in "Muslim" terms (Kurzman 2011). The chilling effects occur, for instance, when politicians or journalists do not clearly distinguish between those who really *are* terrorists and others who may be legal protesters (against environmental degradation, human rights abuses, or aboriginal exploitation) or undocumented migrants. The levels of fear vastly outstrip the actual statistics of terrorist activity and, arguably, encourage an acceptance of intensified surveillance.

The phenomenon of "fun" is the third critical factor fostering intensified surveillance. This may sound somewhat trivial in the context of post-9/11 fears, but it is not insignificant that social media also expanded exponentially during the past decade, in ways that are mutually supportive. The key to understanding social media is its basic premise, "user-generated content." In the so-called Web 2.0, information is not just provided by large organizations—rather, everyone participates. Wikipedia was perhaps the earliest popular model. Social media, however, works not only through user-input but, crucially, through relationships between different users—Facebook's "friends" being the most obvious and, still, pervasive. Moreover, people engage with Facebook and other social media using their real identities, connecting with others of similar outlook. This "social surveillance" (Marwick 2013; also called "peer" or "lateral" surveillance) is decidedly enjoyable for participants. The clustering of groups who like the same music or movies or sports is achieved by the users themselves, before the work (of Internet marketing companies) of splitting them up using algorithms begins. Social media continue to be hugely popular, and while they can be a potent means of shaping political opinion and protest, they also provide the raw materials of data for both corporations and, as Snowden has shown us, police and intelligence agencies.

"It all seems so fluid, slippery and hard to grasp" for the "ordinary citizens and consumers." One feels, one knows one is being watched, but doesn't know (and doesn't much care) by whom and for what purpose. TV cameras are nowadays perhaps the most common sight on every stroll—on busy and depopulated city streets alike. They are so common so as to be no longer noticed —"hiding in the light," or rather in their familiarity. As a matter of fact, they don't hide—they advertise their presence, blatantly and with pride. And there is something more setting them apart from the camera hidden in the TV screen in Winston Smith's bachelor's room: They don't watch to keep you in line and force you to stick to the scheduled routine; they don't give you commands; they don't strip you of your free will, choice, and ability to set your own preferences. They are where they are (that is, everywhere) in order to keep you, and the freedoms you cherish, safe.

Though being fully aware of the ubiquity of spying (renamed, in politically correct parlance, "data collection") and the enormity of the "databases" it produced (having left far behind whatever the CIAs, KGBs, and STASIs of the past ever managed to amass, with all their uncountable legions of paid informers), the depth and width of equanimity with which Snowden's revelations were received by the "ordinary citizens and consumers" was very surprising. Media people sorely miscalculated if they had hoped for rocketing TV News ratings and newspaper sales. However earnestly they tried, leaking Snowden's exposures caused slight, hardly felt tremors, where earthquakes were expected.

One suspects that a significant role in this reaction (or rather absence of reaction) was played by the conscious or subconscious satisfaction felt by billions of Internet users engaged, with abandon, in 24/7 self-spying. After all, one of the main attractions of the Internet is the freedom of constant, on-demand access to the (online version of) the "public sphere," previously open solely to the chosen few, with big radio, TV, or press companies sternly guarding the entry. For uncountable millions, scared by the specter of loneliness and abandonment, the Internet offers an unprecedented chance of exit/salvation from anonymity, neglect and oblivion. A collateral effect of Snowden's revelations was making Internet users aware just how big, and stuffed with important people, "people who truly matter," that public sphere is. It rendered their half-conscious hope look suddenly much more realistic, and supplied the resounding proof, if proof they needed, of just how sound is their investment of time and energy into virtual friends and the virtual public arena. If anything, the most profound and lasting effects of the whole affair will be another leap upwards in the dedication and enthusiasm of Do It Yourself (DIY)—voluntary and unpaid—spying, to the gleeful joy and comfort of consumer and security markets.

Assuming the factors mentioned here are correct, the danger for any seeking accountability from large agencies and democratic participation in new information protocols is that from the point of view of everyday Internet and social media users it will be business as usual. This is helpfully countered by the drip-feed effect of the Snowden revelations. It seems that each is calculated to touch on different dimensions of surveillance, orchestrated by government agencies but enabled through the cooperation of Internet corporations. To keep the issues in the public eye over a longer term than the usual brief media Interest normally permits is an achievement of some very canny whistle-blowing. What will actually produce some more serious public engagement remains to be seen.

References

Agamben, Giorgio. (2013) From the State of Control to the Praxis of Destituent Power. Public Lecture in Athens, November 16. Available at http://roarmag.org/2014/02/agamben-destituent-power-democracy/. (Accessed March 12, 2014.)

Bauman, Zygmunt. (2005) *Liquid Fear.* Cambridge: Polity.

Bauman, Zygmunt, and David Lyon. (2013) *Liquid Surveillance: A Conversation.* Cambridge: Polity.

Bigo, Didier. (2001) The Möbius Ribbon of Internal and External Security(ies). In *Identities, Borders, Orders. Rethinking International Relations Theory*, Vol. 18, edited by Albert Mathias, David Jacobson and Yosef Lapid. Minneapolis: University of Minnesota Press.

Bigo, Didier. (2013) The Transnational Field of Computerised Exchange of Information in Police Matters and Its European Guilds. In *Transnational Power Elites: The New Professionals of Governance, Law and Security*, edited by Niilo Kauppi and Mikael Rask Madsen. London: Routledge.

Castells, Manuel. (2008) The New Public Sphere: Global Civil Society. Communication Networks, and Global Governance. *The Annals of the American Academy of Political and Social Science* 616 (1): 78–93.

Christian Science Monitor. Available at http://www.csmonitor.com/USA/2013/1016/NSA-revelations-A-timeline-of-what-s-come-out-since-Snowden-leaks-began/June-5-8-2013. (Accessed March 12, 2014.)

Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. (2013) Final Report of the Review Group on Intelligence and Communications Technologies: Liberty and Security in a Changing World, December 12.

Coleman, Georges. (2011) Hacker Politics and Publics. *Public Culture* 23 (3): 511–516.

European Parliament. (2014) Report of the Libe Committee of the EU Parliament Chaired by Claudio Moraes of 12 March 2014, on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs. A7-0139/2014. Available at http://www.europarl.europa.eu/committees/en/studies.html#studies. (Accessed March 12, 2014.)

European Parliament. Research Study by CCLS-CEPS, Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer on National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU law. 2013-PE 493.032. Available at http://www.ccls.eu, and also at http://www.ceps.eu/book/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law. (Accessed March 12, 2014.)

Foucault, Michel. (2007) *Security, Territory, Population.* London: Palgrave.

Gerbaudo, Paolo. (2012) *Tweets and Streets: Social Media and Contemporary Activism.* London: Pluto Press.

Guardian.com. Available at http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded. (Accessed March 12, 2014.)

Kurzman, Charles. (2011) Where Are All the Islamic Terrorists? *Chronicle of Higher Education.* Available at https://chronicle.com/article/Where-Are-All-the-Islamic/128443/. (Accessed March 12, 2014.)

Luke, Timothy W. (1999) Simulated Sovereignty, Telematic Territoriality: The Political Economy of Cyberspace. In *Spaces of Culture: City-Nation-World*, edited by Scott Lash and Mike Featherstone. London: Sage.

Lyon, David. (2003) *Surveillance After September 11.* Cambridge: Polity.

Marwick, Alice. (2012) The Public Domain: Surveillance in Everyday Life. *Surveillance and Society* 9 (4). Available at http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/pub_dom/pub_dom/. (Accessed March 12, 2014.)

Marwick, Alice. (2013) *Status Update: Celebrity, Publicity and Branding in the Social Media Age.* New Haven, CT: Yale University Press.

Medine, David, Rachel Brand, Elisabeth Collins Cook, James Dempsey, and Patricia Wald. (2014) Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court. Privacy and Civil Liberties Oversight Board, January 23. Available at http://www.fas.org/irp/offdocs/pclob-215.pdf/. (Accessed March 12, 2014.)

Negroponte, Nicholas. (1995) *Being Digital.* New York: Vintage.

New Transparency. (2014) *Transparent Lives: Surveillance in Canada/Vivre à nu: La surveillance au Canada.* Edmonton, Alberta: Athabasca University Press.

Podesta, John. (2014) Big Data and the Future of Privacy. Available at http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy/. (Accessed March 12, 2014.)

Reid, Angus. (2013) Angus Reid Global Poll. *The Huffington Post*, October 30. Available at http://www.huffingtonpost.com/2013/10/30/edward-snowden-poll_n_4175089.html/. (Accessed March 12, 2014.)

Schmid, Gerhard. (2001) Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI)).

Walker, R. B. J. (2010) *After the Globe, Before the World.* London: Routledge.

Whitaker, Reg. (1998) *The End of Privacy: How Total Surveillance Is Becoming a Reality.* New York: New Press.