Surveillance & Society

Article

Contesting a Biopolitics of Information and Communications: The Importance of Truth and Sousveillance After Snowden

Miguelángel Verde Garrido

Freie Universität Berlin | Berlin Forum on Global Politics (BFoGP), Germany.
verde.m@gmail.com

Abstract

This article aims to provide a novel conceptual understanding of the nature of the global mass surveillance policies and practices revealed by whistleblower Edward Snowden in collaboration with the *Guardian* and *Washington Post* newspapers. The critical analysis and conceptual reinterpretation of state and corporate surveillance and its impact on the political agency of civil society is multidisciplinary. An intersection of Surveillance Studies, political philosophy, and global politics/international relations provides an overview of the policies and practices that states and corporations develop and implement in relation to information and communications technologies (ICT). Clarifying how contemporary society is global and digital, it analyzes the way in which political economies inform contemporary policies and practices of surveillance. A critical analysis of the relation of political economy to neoliberal governmentality, biopolitical technologies of power, and contemporary regimes of truth leads to posit that global mass surveillance is a technology of power deployed by a contemporary biopolitics of information and communication. A conceptual reinterpretation of Foucault's notion of parrhesia and Mann's notion of sousveillance leads to posit that parrhesiastic sousveillance is a sociopolitical and technologically-enabled modality of resistance that can resemantize contemporary politics of truth and lead towards a newborn digital agency for global(ized) civil society.

To those who speak the truth

1. Why a *global* surveillance society?

It should be no surprise that the Pulitzer Prize for Public Service was awarded in 2014 to the two newspapers, the *Washington Post* and *The Guardian*, which first published stories about the global surveillance scandal after the careful analysis and validation of the information and materials leaked to them by Edward J. Snowden, a former National Security Agency (NSA) contractor turned whistleblower. The Pulitzer Prize awarded the newspapers for their role in helping, by means of aggressive reporting, "to spark a debate on the relationship between government and the public over issues of security and privacy" after their revelation of "widespread secret surveillance by the National Security Agency" (The Pulitzer Prizes 2014). Snowden described this accolade, the highest awarded in United States journalism, as a vindication for those who believe the public has a role in government. He added that the efforts of brave reporters and their colleagues, despite extraordinary intimidation—which includes forced destruction of journalistic materials, inappropriate use of terrorism laws, and other mean of pressure—has led to what the world now recognizes as a work of vital public importance (The Guardian 14th April 2014).

Verde Garrido, M. 2015. Contesting a Biopolitics of Information and Communications: The Importance of Truth and Sousveillance After Snowden. *Surveillance & Society* 13(2): 153-167.
http://www.surveillance-and-society.org | ISSN: 1477-7487

What is surprising, in general terms, is the fact that there is nothing new about revelations of the global scale of surveillance of information and communications. During the fear of the threat that 'the year 2000 problem' (Y2K) could represent to computer networks, digital documentation, and data storage worldwide, a particular network was revealed by the Australian Inspector General of Intelligence and Security, Bill Blick: ECHELON (BBC 3rd November 1999). Described at the time as a global surveillance network that used "the world's most sophisticated eavesdropping technology [...] linked directly to the headquarters of the US National Security Agency" for data mining purposes, the British and American governments refused to admit that it existed (ibid.). Blick, however, revealed that the Australian Defence Signals Directorate (DSD) formed part of ECHELON (ibid.). The surveillance network's capabilities and objectives were described as follows:

> Every international telephone call, fax, e-mail, or radio transmission can be listened to by powerful computers capable of voice recognition. They home in on a long list of key words, or patterns of messages. They are looking for evidence of international crime, like terrorism.
>
> (ibid.)

A report commissioned by the European Parliament (EP) on the nature of ECHELON "produced evidence that the NSA snooped on phone calls from a French firm bidding for a contract in Brazil. They passed the information on to an American competitor, which won the contract" (ibid.). The reporter who revealed this act of industrial espionage, Duncan Campbell, argued what many civil rights groups stated then: ECHELON could "be used to intercept almost any electronic communication, be it a phone conversation, mobile phone call, e-mail message, fax transmission, net browsing history, or satellite transmission" (BBC 29th May 2001). The EP report, however, downplayed these claims. It stated that the majority of communications could not, due to technical reasons, be intercepted and that, when they could, it was possible only to do so at "a limited extent". No matter how extensive ECHELON's resources and capabilities could be, the mere volume of traffic made the exhaustive and detailed monitoring of all communications "impossible in practice" (European Parliament's Temporary Committee on the ECHELON Interception System 11th July 2001: 11).

Despite these conclusions, the report neither denied the existence of ECHELON nor that its member states did deploy global information and communications surveillance. It only contested the network's mass intercept capabilities, considered to be more "limited" than what was being revealed. And yet, the report would recommend: the promotion, development, and manufacture of European encryption technology; the promotion of open-source software to guarantee that no backdoors be built into computer programs; and, the systematic encryption of the digital communications (e.g., emails) of European institutions, of public institutions of member states, and of its citizens, so that encryption of communications ultimately become the norm (idem: 19). It also readily admitted several legal and governmental problems: EU citizens' data protection rights varied substantially from member state to member state and were hardly adequate in any case; the oversight of the activities of intelligence services required that member states' national parliaments have formally structured monitoring committees (idem: 13).

Nowadays it is known that ECHELON was but one of various surveillance programs that existed as a result of the United Kingdom—United States of America Agreement (UKUSA), which establishes cooperation in signals intelligence between the UK, the US, Canada, Australia, and New Zealand (European Parliament's Directorate General for Internal Policies 2013: 12; 5). Snowden's revelations evidence that the intelligence services of UKUSA member countries share technical surveillance capacities as well as vast troves of intercepted data (The Guardian 21st June 2013). They also evidence that the NSA and the British General Communications Headquarters (GCHQ) further their global mass surveillance programs by means of the voluntary and/or involuntary assistance of global telecommunications and internet corporations (Timm 2014). The reasons for intelligence services' profound interest in the data collected by corporations are economical: internet giants such as Google and Facebook, whose free services cater to billions of consumers, are the principal innovators of online browsing data trackers, the main proponents for the reduction of online anonymity, and the world's most important personal and targeted advertising services (Schneier 2013). In this sense, because surveillance is "the business model of the Internet", argues Bruce Schneier, intelligence services have adopted the data collection practices of corporations as their own (ibid.). A fundamental contribution of Surveillance Studies, in this respect, is its efforts to clarify how global surveillance is not only confined to intelligence agencies' deployment of surveillance technologies, but extends also to the very cultural and economic characteristics of contemporary society.

There was perhaps so little done, so paltry an outcry, after the ECHELON revelations because the thought of a global surveillance society was considered conspiratorial at the time. Some years before Edward Snowden would become a whistleblower, the renowned Surveillance Studies scholar David Lyon would write in his primer on the discipline that:

> To talk about global surveillance certainly sounds conspiratorial, but [...] [*s*]urveillance has become globalized just because economic and political processes are themselves globalized, for better or worse. [...] The globalization of surveillance, just as with all other globalizations, is both a phenomena in its own right and something that takes place in different ways in different countries, producing situations of complex inter-relations. In some ways, surveillance is "glocalized" as local circumstances make a real difference to general trends.
>
> (Lyon 2011: 134-135)

More recently, a Pew Research Center study that queried over 1400 experts on the internet showed that the majority of respondents shared the opinion that the greatest threats to the internet's potential are states and corporations, specifically: state-based security and political control; state and corporate surveillance; and, corporate-based control over internet architecture and flows of information (Pew Research Internet Project 3rd July 2014). Crucial to understanding why surveillance has become global are the facts that contemporary society is itself global and digital. Global economy results from the interconnectedness of the world's national economies, so reliant on each other that economic reforms enacted in the China can lead to the slowdown of the economies of the US and the European Union (EU) (The Guardian 24th March 2014). An embodiment of the global economy, the world equities market, has depended already for decades on the desktop terminals and communication networks developed by media corporations such as Bloomberg L. P. and Thomson Reuters Corporation; in more recent years, the financial markets have even come to be dominated by digital machine learning-driven technologies (Institutional Investor 30th January 2014), evidence of the digitalization and automatization of important aspects of contemporary society.

Surveillance policies and practices can also be considered global, argue Kirstie Ball and David Murakami Wood, because they are part of the everyday life of the world's various people (Ball and Murakami Wood 2013: 1). The global surveillance society has resulted from the dynamics of "state and corporate priorities". It is born from security and military functions, policing, and institutions such as the carceral and health and welfare systems. Ball and Murakami Wood explain, as does Schneier, that state concerns about security lead governments "to integrate the private sector into its goals as providers of intelligence on the consumers they serve […] [*and to*] annex corporate information systems into a securitised information infrastructure" (idem: 2-3). The synergy of state and corporate surveillance policies and practices, especially regarding information and communications, they argue, "have normalised and legitimised mass targeted surveillance deep within corporate, governmental and social structures" at the same time that "a blurring of the boundaries between public sector and private organisations" has occurred (idem: 2). In this sense, a multitude of "different practices of information management and surveillance" strengthen "a normalisation of surveillance as a life-practice" that is simultaneous to the use of "the products of surveillance through organisations and systems" by "a corporate-state nexus" (idem: 3). Ball and Murakami argue that this corporate-state nexus does so in order to "increase flows that create opportunities for exploitation and profit and at the same time reduce the uncertainties and risks that come from bad circulations" (ibid.). This coincides, they explain, not only with what Michel Foucault termed security, but also with "a kind of emerging neoliberal global government" where security is taken to be the basic function of government—understanding government in this context as something more contemporary, "pervasive and networked" (ibid.) than governments from the past. For these numerous reasons, Ball and Murakami Wood have recommended that Surveillance Studies give "more serious attention to the political economy of surveillance", especially to "the way in which surveillance works in and for government (in the broadest sense) at this global scale" (idem: 1-2). They recommend that an "integrated political economic analysis of surveillance" should engage seriously with the considerations of "policy and activist communities" so that the analysis can prove useful for "confronting and challenging the continued expansion and intensification of surveillance" (idem: 3).

2. Why a *political economy* of surveillance?

The previous section explained that our contemporary society, global and digital in scope, is also a global surveillance society. Not only states, but also corporations, deploy technologies that monitor global information and communications for different ends. The Snowden revelations evidence the extension of state and corporate surveillance to the social, political, and economic processes of civil society inasmuch as citizens and consumers. Although these threats are not entirely new, the ubiquitous role that information and communications technologies (ICT) have come to play in contemporary society is indeed a novel development. The fact that exact details about global mass surveillance are clearer to us than what they were a decade ago is also new. This section will clarify the way in which the technologies of power of our global surveillance society respond to the political economies of states and corporations.

There are three contemporary tendencies at present that best exemplify the most prominent global and national policies and practices by which states and corporations concerning ICT. These can be briefly summarized as follows:

- States securitize information and communications in the name of national security and defense priorities, developing and implementing local policies and practices that can also be enforced at the international, transnational, and global level by other states;

The ongoing reporting on the NSA and the GCHQ surveillance scandal provides an in-depth appreciation for the ways in which states can conjointly deploy policies and practices of securitization of information and communications. Another example of the transformation of the domain of information and communications into a matter of national security (Deibert 2011: 24) is the United Nations (UN) General Assembly resolution that the Russian Federation, China, Tajikistan, and Uzbekistan presented in September 2011. The resolution proposed a code of conduct for information security and the protection of national sovereignty in information and communications—this "could give any state the right to censor or block international communications for almost any reason" as well as "could even be used for trade protectionism in cultural industries" (Internet Governance Project 20th September 2011). The securitization of information and communications at the national level is a common enough policy, but their attempted securitization at the level of international politico-economic blocs is a much more recent tendency in global politics.

- States outsource prior state functions, such as surveillance, censorship, and policing of information and communications, to corporations; although numerous corporations perform these functions as their *raison d'être*, in the case of others, 'outsourcing' does not necessarily imply that the corporation in question is a contractor, since corporations can also be legally coerced to perform these functions under national security claims;

Snowden's revelations have evidenced that the NSA and the GCHQ collaborate with a number of global internet corporations, even if the exact terms in which these collaborations occur continue to be unclear (New York Times 7th June 2013). In addition, a number of corporations gather information and provide analyses and advice to states as commercial services—for example, Booz Allen Hamilton Inc and Lockheed Martin to the US government (New York Times 9th June 2013). Furthermore, an international surveillance technology industry is expanding: various corporations specialize in providing states with advanced communication surveillance technologies. This global trade, calculated to be worth 3 to 5 billion US dollars a year, has already reached an annual growth rate of 20 per cent (Amnesty International 4th April 2014). These facts show, without a doubt, a swelling neoliberalization of state functions, especially those concerned with security and intelligence, as well as a number of industries that commercialize the monitoring, collection, and meticulous processing of vast amounts of information and communications.

- States' economic and political interests and corporations' lobbying efforts are synergetic when it comes to the enactment of international treaties and legislations, which sidestep parliamentary discussion on ICT policies and practices as well as national consultation mechanisms with civil society on the same matters.

The most notable of these international treaties are bilateral free trade agreements, such as the infamous—and defeated—Anti-Counterfeiting Trade Agreement (ACTA). Ongoing negotiations on the Comprehensive Economic Trade Agreement (CETA), the Trans-Pacific Partnership (TPP), and the Transatlantic Trade and Investment Partnership (TTIP) are negotiated at a distance from existent multilateral trade institutions such as the World Trade Organization (WTO). These treaties are the results of efforts made by the US, the EU, and international corporations to establish their own preferences for global trade and their proposals for (de)regulation (New York Times 8th October 2013). Concerning information and communications, states and corporations share an interest in ever harsher and more restrictive intellectual property and copyright provisions (Cardoso et al. 2014: 5), so as to exert more control over the flow of ICT content. There is also the concern that they share an interest in attempting to trump existing data protection regulations (Ruddy 2014: 97), primarily driven by security and economic incentives. Several ACTA-based proposals that continue to be found in leaked draft documents of the ongoing treaties—for example, the CETA (La Quadrature du Net 20th October 2013) —cause significant worry, since they could lead to "global consequences for digital freedoms" (Electronic Frontier Foundation 2012).

Contemporary tendencies in state and corporate policies and practices concerning ICT include various aspects of securitization, censorship, and surveillance. Identifying these tendencies allows for clarifying the implications of what is emerging and developing quite rapidly in our contemporary surveillance society: a global political economy of surveillance. Kirstie Ball and Laureen Snider explain political economy as "the interconnection of social, economic, and political processes" (Ball and Snider 2013: 1) They share with this article the opinion that our global surveillance society is driven by the political economies desired by its most dominant players, which are also its two most "massive configurations of power": the state and the corporation (idem: 1-2). For this reason, Ball and Snider draw attention to "the embeddedness of surveillance processes within the activities and agendas of global capital and the state" (idem: 5).

Zygmunt Bauman et al. also emphasize that the global nature of capital flows and politics has led to "a complex interaction between public and private agencies, not least agencies of corporate and market capital rather than of liberal citizenship" (Bauman et al. 2014: 136). These complex state-corporate dynamics are brought upon, they argue, by "the conjunction of three processes that have become interwoven: transnationalization, digitization, and privatization." Global flows of privatized digital data, in turn, have led to "a much larger transformation affecting the way the boundaries of national security function" (idem: 126). In the same manner as corporations, states do not care to grasp only the information and communications data that is produced, distributed, and stored within their sovereign territorialities, but also those that flow through them and elsewhere.

Almost every nuance of the lives of individuals and the dynamics of populations is encoded in global privatized flows of digital traces. Therein resides corporations' economic interest in digital surveillance of internet users. Ball and Snider explain that this is why commerce has shaped and continues to shape surveillance, since corporations are those that "funded, designed, legitimized and built the machineries of surveillance" that exist nowadays (Ball and Snider 2013: 3-4) They argue that the development of cyberspace also spurred and continues to spur what Kevin Haggerty and Richard Ericson termed 'computerized dataveillance'. Digital surveillance is expanding not only for marketing purposes, but also because the digitalization of records allows for citizens, customers, employees, and those defined as 'criminals' to be "reconstructed through the aggregation of data collected in bits of information from a myriad of sources [...] [*to then be*] disassembled and reassembled to suit the priorities and interests of the institution involved" (idem: 4).

Until very recently, Ball and Snider remind us, these digital technologies focused on developing "new and better methods of controlling and punishing the designated 'other'" (idem: 5). The technology of power that is digital surveillance, they argue, has become a "key component of governance *and of* commerce". For Ball and Snider, "dataveillance of the Web allows the entire communication process to be turned into a commodity, packaged and sold" (ibid.); for this very reason, states also find it to be a particularly interesting technology of power. Bauman et al. explain that states have adopted the digital surveillance practices of corporations because:

> 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.
>
> (Bauman et al. 2014: 138)

What exactly is sought by states when they deploy economic digital surveillance continues to be unclear, but the strategic mission list that the NSA published in January 2007 states that "ensuring U.S. economic advantage and policy strategies" is among its priorities (International New York Times 2nd November 2013). Snowden's revelations have evidenced NSA surveillance of corporations such as Petróleo Brasileiro S.A. and China Telecom Corporation Limited as well as of prominent decision-makers in economic matters, Joaquín Almunia, Vice-President of the European Commission and Commissioner for Competition, among them (New York Times 20th May 2014). Other revelations indicate that NSA surveillance of the entire mobile telephony network of certain countries—for example, the renowned financial services center or "tax haven" that is the Bahamas (The Intercept 19th May 2014). Hence, for Bauman et al., "far from a seamless flow of information, power relations structure the game" (Bauman et al. 2014: 127) that states play by means of global mass surveillance: a structurally asymmetric balancing of political and economic interests that happens to occur under the guise of reciprocal international collaborations on antiterrorism.

Bauman et al. share Ball and Murakami Wood's argument that the corporate-state nexus deploys a neoliberal apparatus of security. The success of the complex interaction between states and corporations relies on "a security apparatus which, as Foucault 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" (idem: 139). Contemporary mass surveillance functions by exploiting a global ICT infrastructure in which information and communications content flows seamlessly and uninterruptedly through transnational networks. This recalls the laissez faire attitude of neoliberal political economies, which also wants capital to flow incessantly. Zeynep Tufekci has written, in relation to what she terms computational politics, that "modern social engineering operates by making surveillance as implicit, hidden and invisible as possible, without an observed person being aware of it"; for Tufecki, our contemporary surveillance society functions "in a manner opposite of the panopticon" (Tufekci 2014).

Tufekci's argument that our global surveillance society is also characterized by technologies of power that are neither disciplinary nor panoptical is an argument that this article shares. Global mass surveillance, even though it also deploys panoptical technologies of power, is biopolitical. The significance of the data contained in information and communications to state and corporate political economies, added to the fact that neoliberal governmentalities require what Foucault calls a regime of truth, justifies considering global mass surveillance as one of the technologies of power deployed by what can be understood as an emerging and rapidly developing biopolitics of information and communications.

3. Why a biopolitics of information and communications?

The previous section explained that global digital surveillance provides states and corporations with a technology of power that secures their economic and political interests. Within the context of a global and digital society, these political economies establish international and/or global policies and practices of surveillance of ICT, securitizing ICT infrastructure and networks as well as censoring their content so as to maintain political power and ensure economic profit. States and corporations develop and implement these either on their own, or by contracting/lobbying/coercing each other to do so, or by collaborating with each other due to economo-political synergies. The subjects of digital surveillance have economic and political utility and are fluid digital reconstructions, which can be framed as individuals within specific populations and as populations that are aggregates of specific individuals.

The concept of a biopolitics of information and communications results from understanding that biopolitics and governmentality—that is to say, "the governmental regime called liberalism" (Foucault 2008: 22) —are conceptually and theoretically intertwined. This is so because the central core of the problems they are concerned with is the same: the population (idem: 21). In addition, the concept sheds light on the fact that both governmentality and biopolitics are driven by the question of the economic truth within governmental reason (idem: 22). Foucault explains that governmentality can be understood as follows:

> The ensemble formed by the institutions, procedures, analyses and reflections, calculations, and tactics that allow the exercise of this very specific, albeit very complex, power that has the population as its target, political economy as its major form of knowledge, and apparatuses of security as its essential technical instrument.
>
> (Foucault 2007: 108)

Governmentality employs knowledge based on political economy to establish the logics and forms of governing that will most optimally exert power over the population through the deployment of apparatuses of security. This understanding of governmentality is what leads Foucault to conceptualize the contemporary state as "nothing but the mobile effect of a regime of multiple governmentalities" (Foucault 2008: 77). Such a notion of the state is of particular interest since it explains why a government, inasmuch as a fluidly protean assemblage of governmentalities, may develop and implement contradictory policies and practices of its "mechanisms of security", that is to say, contradictions in the interventions that have "the essential function of ensuring the security of the natural phenomena of economic processes or processes intrinsic to population" (Foucault 2007: 353). When we consider policies and practices concerned with information and communications, it is clear that a state may be committed to freedom of expression at the same time that it is committed to mass surveillance. This notion of the state, hence, allows for considering that contradictions in policy and practices may be the result of independently established governmentalities, which are at odds with each other due to the vast differences in their technologies of power, modes of knowledge, and intended populations. In this sense, we clarify that the objectives of policies and practices as well as the institutions employed to secure these can often conflict with each other for the same reasons.

Governmentality finds the need to establish a "particular regime of truth that finds its theoretical expression and formulation in political economy" (Foucault 2008: 29). For this reason, it establishes the market as the site of veridiction and the mechanism that allows it to "function with the least possible interventions precisely so that it can formulate its truth and propose it to governmental practice as rule and norm" (idem: 30). Contemporary biopolitics of information and communications also respond to the political and economic regime of truth of the global market. Bauman et al. urge us to carefully consider the "social and cultural shifts reshaping the acceptability of [...] new practices of communication, new modes of knowledge, and rapid shifts in the expression of personal identity [*because*] [...] they include the general shift to the market rather than state law as the ultimate measure of political and ethical value" (Bauman et al. 2014: 124). We have explained above that Schneier has a similar argument: he claims that the model for the information and communications industry, particularly for the internet industry, is that of surveillance.

David Murakami Wood and Alexander Galloway have reinterpreted the Foucauldian notion of biopolitics so as to better explain contemporary societies of control and surveillance (Murakami Wood 2013: 317-318; Galloway 2004: 81, 88). This article also reinterprets biopolitics, mostly to argue why global mass surveillance can be understood as state and/or corporate deployments of biopolitical technologies of power over information and communication. There are three central reasons for arguing that mass surveillance is biopolitical. The first is that biopolitics is a technology of power that is not "disciplinary" (Foucault 2003: 242), and hence, not panoptical in nature, since it is not "individualizing" but "massifying" (idem: 243). The second is that biopolitics is a "technology of security [...] or regulatory technology" (idem: 249) that deals "with the population as a political problem" (idem: 245) and that is concerned not only with "biological", but also "biosociological processes characteristics of human masses" (idem: 250). Pioneering scientific fields in natural science, such as biosemiotics, posit that semiosis— "the production of signs" — is fundamental to life and that, in this sense, each and every living system is a semiotic system (Barbieri 2008: 1-2). As with every other animal species, obtaining information and communicating relevant information to others can be considered among the most crucial of human beings' biosociological processes, fundamental to their individual and social dynamics. Biopolitics of information and communications represent a novel intrusion—without doubts or rival—into biosociological processes of acquisition and production of information and its circulation and distribution by the power of states and corporations.

The third and last reason is that biopolitics of information and communication allows states and corporations to deploy a security apparatus that dovetails sovereign and disciplinary technologies of power (Foucault 2003: 38-40) alongside its biopolitical technologies of power (Foucault 2003: 242; 2007: 107-108). Ball and Snider argue that surveillance is "the sociotechnical means through which the logic of juridical concepts articulate with social relations of commodity production, finding its expression in systems of public and private law". In their opinion, contemporary surveillance constitutes "the institutional goals and biopolitical dimensions of modernity" (Ball and Snider 2013: 3). Without a doubt, besides the regulation of processes that results from biopolitical technologies of power, the biopolitics of information and communication also deploy as technologies of power the concepts and rules that result from ICT legislation enacted by sovereign power as well as the norms that institutions enforce so that individuals discipline and normalize their information and communications. Bauman et al. warn us that "we should clearly be very wary of the prospect of novel forms of inclusion and exclusion enacted through new technologies of population control" (Bauman et al. 2014: 136).

States and corporations legislate, discipline and normalize, and regulate the flows of information and communication processes because in global and digital societies, Manuel Castells argues, control over the circulation of information and its communications is always an indicator of political and economic power (Castells 2000: 695). The rapid development of ICT and their creative use in contemporary society is profoundly rebalancing social, economic, and political power. For these reasons, states and geopolitical blocs, global and national corporations, terrorist organizations, organized crime cartels, and—at a slower rhythm, but as surely—civil society (Castells 2005: 10) (constituted by a kaleidoscope of individuals and groups that include non-governmental organizations, whistleblowers, civil society organizations, cultural jammers, hacktivists, activists, consumers, and others), who voice national and global concerns, continuously vie to expand whatever mechanisms of power they may have at their disposal. Tufekci's notion of computational politics, which illustrates contemporary social, economic, and political clashes over the power contained with information and communications, recalls Antonio Gramsci's concept of hegemony, "which emphasizes manufacturing consent, and obtaining legitimacy, albeit uses state and other resources in an unequal setting, rather than using force or naked coercion" (Tufekci 2014).

Foucault is similarly concerned about the fact that truth—produced "only by virtue of multiple forms of constraint" and capable of inducing "regular effects of power" —is in every society established in accordance to a "general politics" or regime of truth (Foucault 1980: 131). The characteristics of a particular biopolitics of information and communication depend on the regime of truth that exists within the society upon which it is deployed. A regime of truth is "a system of ordered procedures for the production, regulation, distribution, circulation and operation of statements", which is "linked in a circular relation with systems of power which produce and sustain it, and to effects of power which it induces and which extend it" (idem: 133). For Foucault, the regime of truth is "a condition of the formation and development of capitalism" (ibid.) and its neoliberal variant. Due to the fact that truth can be explained as "the ensemble of rules according to which the true and the false are separated and specific effects of power attached to the true", Foucault argues that contestation over the truth are concerned with the economic and political role the truth plays in our societies (idem: 132).

Hence, a "'political economy' of truth" establishes five important traits for veridiction in order to determine what is true in our contemporary societies. To be clear, truth: 1) is centered on the form of scientific discourses and the institutions that produce it; 2) is subject to constant economic and political incitement; 3) is the object, under diverse forms, of immense diffusion and consumption; 4) is produced and transmitted under the control, dominant if not exclusive, of a few great political and economic apparatuses; and, 5) is the issue of a whole political debate and social confrontation around which ideological struggle occurs (idem: 131-132). Most instances of the public debate on the development and implementation of state and corporate policies and practices, especially those that concern surveillance and collection of personal data, are: explained and justified merely with econometric and statistical forecasts; addressed only in governmental press conferences and in the public relations campaigns of corporate lobbying efforts; and, usually confined to mainstream or 'corporate media' and its reporting. Foucault recognizes that the political question of "constituting a new politics of truth", that is to say, of establishing a new "political, economic, institutional régime of the production of truth", is not a matter of emancipating the truth from the structure of power, but detaching the power of the truth "from the forms of hegemony, social, economic and cultural, within which it operates at the present time (idem: 133). The existence of a regime of truth leads states, corporations, and civil society to contest each other 'for truth'; however, the contestation is not 'on behalf' of truth, but—as explained above—concerned with the status of truth and the economic and political role it plays (idem: 132-133).

Ray Coleman and Michael McCahill clarify further the relation of regimes of truth to policies and practices of surveillance. They explain that surveillance, when deployed by a certain regime of truth, can also be quite deficient—especially when it comes to surveillance of that which is not in its own interest. State and corporate surveillance in those cases is a form of inspection that is "shaped less by discourses of censure, discipline and control, as is the case with conventional crime, and more by a language of accommodation and compliance concerning the powerful", which is to say: states and corporations can organize their policies and practices quite differently depending on the intended population, "each carrying different targeting strategies and messages in relation to the powerful and the powerless, respectively" (Coleman and McCahill 2011: 134). The population under surveillance and the technologies of power deployed upon them depend on the regime of truth that exists within that surveillance society. For this reason, surveillance policies and practices should be contested and resisted from a standpoint that analyzes modes of veridiction, techniques of governmentality, and practices of the self. For Foucault, the notion that allows for doing so is parrhesia, the ethical and political telling of the truth (Foucault 2011: 8-9).

4. Why a resistance of parrhesiastic sousveillance?

The previous section explained that global mass surveillance is a state and/or corporate deployment of a biopolitical technology of power that regulates the biosociological processes of information and communication. It also explained that the contestation of state and corporate control over the regime of truth is even more important when we consider that their policies and practices extend not only to ICT infrastructure, networks, and content, but also to entire citizenries and global consumer markets. The notion of parrhesia, Foucault clarifies, involves courageously speaking the whole truth without reserves, despite the fact that it may place the speaker at risk of violence at the hands of the authority that is contested (Foucault 2011: 6; 9; 11). The biopolitics of information and communications of states and corporations employ cutting-edge scientific and technological developments. These mechanisms of control are deployed so ICT data traces can be thoroughly monitored and examined in order to govern populations more efficiently in accordance to electoral calculations, market imperatives, and security concerns. In contemporary surveillance societies, parrhesiastic action has important sociopolitical implications because it contests the regime of truth that attempts to ensure the political, economic, and social regulation and compliance of civil society inasmuch as citizens and consumers.[1] Recent Snowden revelations evidence that GCHQ deploys covert tools over the internet to spread false information, manipulate the results of online polls, divert traffic to or away from websites and videos that are of their interest, and even permanently disable internet users' accounts by infiltrating their computers (The Intercept 14th July 2014). This is particularly worrying because "most conceptions of democracy", explain Bauman et al., "rest on some sense that people are able to think and make judgments for themselves" (Bauman et al. 2014: 137). Fortunately, the escalating development of ICT and their inventive use by civil society has also led to the emergence of numerous modalities of resistance that can contest the mechanisms of control of contemporary biopolitics of information and communication. Civil societies continue to develop their political agency and are learning to strengthen a nascent digital agency, both of which enable them to contest state and corporate regimes of truth as parrhesiastes that search for the resemantization of their social, economic, and political processes.

In consequence, there are various important individual and collaborative actions of parrhesia in contemporary society that did not exist only a few decades ago. In general terms, we find alternative media organizations and citizen journalism that employ internet websites and blogs as well as social media

[1] A recent example of research on the ways information and communications are spread through social media and the internet is the recently revealed study on "emotional contagion" that Facebook and Cornell University collaborated on in 2012. Others are several United States' Defense Advanced Research Projects Agency (DARPA) studies, started in 2011, which research social connections and communications in order to optimize informational warfare. The "emotional contagion" study was conducted on unwitting—and hence, uninformed—social media users, which were also subjects of information manipulation. Both studies were fundamentally interested in better understanding how to influence online communicative behavior in unaware populations. For more on these studies, do read: *The Guardian* 30th June 2014; and: *The Guardian* 8th July 2014.

networks to post and distribute their reporting. More specifically, there are whistleblowing organizations such as WikiLeaks have that globalized, online and offline, the revelations substantiated by carefully vetted materials sent anonymously to them by individuals and/or groups concerned by state and corporate wrongdoings and abuses. Quite recently, hacktivists and hacktivism collectives as well as collaborative networks that crowdsource open data analysis—which journalist Barrett Brown calls 'pursuances' (Brown 2012)—have shed light upon the strategies by which the state-corporate nexus deploys espionage and persona management (i.e., using online identities for purposes of astroturfing or disinformation) to infiltrate or hinder the activities of non-profit organizations and sociopolitical activism groups (Masnick 25th November 2013). Lastly, there are numerous national and international non-profit (NPO) and non-governmental organizations (NGO) committed to establishing radical transparency of the state, corporations, and the media. These organizations investigate, report, and publicize their findings on a broad scope of topics, that cover state and corporate corruption, free and fair elections, environmental impact, consumer rights, freedom of information and of the press, corporate lobbying, and digital rights—but to name a few.

Parrhesiastic contestation of the regime of truth is also embedded within the social, economic, and political processes of contemporary surveillance society. Because of its commitment to detaching the truth from the economic and political hegemonies that control it, we cannot consider an ICT-enabled parrhesiastic action to embody the very biopolitics of information and communications it contests. However, the commitment of parrhesia to transparency appears to require that it share the interest of surveillance in monitoring and collecting data on certain individuals and populations. In order to clarify whether this is the case, it is fundamental to consider whether what appears as surveillance is not in fact something altogether different.

Murakami Wood has questioned whether we should not begin to talk about "multiple and multiplying 'veillances'", rather than simply 'surveillance', in order to understand the reception, reaction, and resistance to global surveillance (Murakami Wood 2013: 324). Steve Mann conceptualizes and theorizes from the intersection of Surveillance Studies and his technical trailblazing in the development of wearable computing, especially those devices that involve computational photography. From the standpoint of this technico-conceptual crossroad, Mann posits an understanding of surveillance that, although "commonly used to refer literally to visual signals", also covers "other sensory signals and observational data in general" (Mann and Ali 2013: 243). Surveillance, for Mann, frequently exhibits the following traits: it is usually deployed from a fixed viewpoint, commonly architecture-centered, and attached to property; it establishes an "oversight" perspective, which watches from above; and, it is commonly initiated by property owners and/or its custodians, such as governments (Mann 2004: 626-627). Contemporary developments in wearable computing and ICT, such as "social networking, distributed cloud-based computing, self-sensing, body-worn vision systems, wearable cameras, and ego-centric vision" (Mann 2014: 605), lead Mann to propose an alternative or counterpart to surveillance, which he terms sousveillance. Sousveillance, for Mann, exhibits the following traits: it is usually deployed from a mobile viewpoint, commonly human-centered, and worn by a person; it establishes an "undersight" perspective, which watches from below; and, it is commonly less hierarchical and more rhizomic than its counterpart, surveillance (Mann 2004: 626-627). In this sense, sousveillance seems to explain parrhesia more correctly and more in detail than surveillance does. To be clear, it is not necessary to consider every instance of parrhesia an instance of sousveillance and vice-versa, but we can argue that they may coincide quite often. Mann and Ferenbok intuit the potential for parrhesia of sousveillance when they argue that in contemporary society "people can and will not only look back, but in doing so [*can and will*] potentially drive social and political change" (Mann and Ferenbok 2013: 24).

The notion of veillance that Murakami Wood considers could be helpful for certain Surveillance Studies research is the result of Mann's considerations on surveillance and sousveillance as counterparts. For Mann, these similar, but different, alternatives indicate that there is a politically neutral watching or sensing that does not necessarily involve social hierarchy (Mann 2014: 605). For this reason, this article shares the opinion that both of these conceptual understandings about the manners in which we monitor and store sensory signals and observational data are vital to the study of privacy, security, and trust. They serve to illustrate that in contemporary society, "we seek to measure, sense, display, and visualize veillance, regardless of whether it is surveillance or sousveillance" (ibid.). Mann and Adnan Ali posit that veillance is a purposeful action that produces an artifact. Such an artifact can be employed in socioeconomic contexts—for example, to enable greater trust in transactions, because it reduces the information asymmetry that exists between contracting parties (Mann and Ali 2013: 244). In this sense, this article posits that when veillance commits itself to political actions that contest the authority of a regime of truth it can also be understood as parrhesiastic. Mann and Ali argue that while surveillance monopolizes transactions for the party in a position of authority, sousveillance breaks down that same monopoly, since the distributed nature of sousveillance provides the contracting parties with multiple points-of-view and, hence, multiple perspectives that contest the authority's control over the transaction (idem: 245-246). The notion of veillance for Mann and Ali is a constant reminder that information asymmetries provide an authority with power, a conclusion that they share with Foucault and Tufecki, as we have explained above. Mann and Ali's understanding of power, to be clear, comes from Hannah Arendt's definition: "the ability to voluntarily regulate, control, and make decisions in a social context" (idem: 249). Because of this, they argue, it should not come as a surprise that authority reacts to a diminishing of information asymmetry, and hence to a diminishing of power, with violence, which they understand to be "a kind of simulacrum of genuine power" (ibid.). There are a number of instances of violence evident in the manners in which states and corporations react to the contestation of their authority over information and communications. Journalists, whistleblowers, sociopolitical activists, opposition representatives and dissidents, non-governmental organizations, and even ordinary citizens, are submitted to a number of abuses as a result of surveillance (United Nations' Human Rights Council 30th June 2014: 5-7): intimidation, discrimination, and incarceration; espionage and smear campaigns; chilling effects; information blackouts; legislation approved in conditions of emergency or secrecy; and, brutal repression, torture, and—lastly—murder.

For evident reasons, individual and collaborative actions of parrhesiastic sousveillance require strict countersurveillance strategies as well. Civil societies' use of encryption for their information and communications has expand considerably in the past year (Wired 16th May 2014), NGOs are pushing for very specific freedom of information requests and carefully argued lawsuits against governments are being filed in courts, and international organizations such as the UN are contesting policies and practices of mass surveillance on the grounds that it does not comply with international human rights law (GigaOM 16th July 2014). Civil societies across the world, thus, continue to contest the policies and practices of biopolitics of information and communications with which states and corporations attempt to ensure not only their economic and political power, but also their control over the access to and communication of information that can evidence and confront instances of abuses, unconstitutionalities, and corruption. The debate about states' discourses that dishonestly claim an either/or policy scenario for security and civil liberties as well as about corporate narratives that shroud the monetization of internet users' private data as a beneficial service is imperative for contemporary society. In a July 2014 interview, Snowden argues that the single most important factor that explains "the failures of oversight" that we have contemplated in most states should be thought about in terms of a lack of technical literacy. Every technology, he explains, is "a new system of communication, a new set of symbols, that people have to intuitively understand". In our contemporary societies, laments Snowden, technical literacy is "a rare and precious resource" (Snowden 17th July 2014).

The parrhesiastic and sousveillant contestation of global mass surveillance is based on the truthful fact that invasive and unlawful surveillance and collection of personal data from digital communications "may not only infringe on the right to privacy, but also on a range of other vital human rights" (Pillay 16th July 2014). These sociopolitical efforts are already providing contemporary societies with a more solid grasp on technical literacy, furthering their demand for the rule of law and democratic oversight, and strengthening their political agency along with a nascent digital agency. These threats and these achievements are the reasons why contemporary societies must remain seized on the debate, resolute in their legal questionings, steadfast in their socio-economo-political actions. As they continue to do so, they may prove Snowden right when he avows:

> Technology can actually increase privacy, but not if we sleepwalk into new applications of it without considering the implications of these new technologies.
>
> (Snowden 17th July 2014)

References

Amnesty International. 4th April 2014. "Q&A: Coalition Against Unlawful Surveillance Exports (CAUSE)." Accessed 22nd June 2015. http://www.amnesty.org/en/news/questions-and-answers-coalition-against-unlawful-surveillance-exports-cause-2014-04-03.

Ball, K.S and D. Murakami Wood. 2013. "Editorial: Political economies of surveillance." *Surveillance & society* 11 (1/2): 1-3. Accessed 22nd June 2015. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/editorial_1112/editorial_1112.

Ball, K.S. and L. Snider. 2013. *The surveillance-industrial complex: A political economy of surveillance*. New York: Routledge.

Barbieri, M. 2008. "What is biosemiotics?" *Biosemiotics* 1 (1): 1-3. Accessed 22nd June 2015. http://link.springer.com/article/10.1007/s12304-008-9009-1/fulltext.html

Bauman, Z., D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon and R.B.J.Walker. 2014. "After Snowden: Rethinking the impact of surveillance." *International political sociology* 8 (2): 121-144. Accessed 22nd June 2015. http://onlinelibrary.wiley.com/doi/10.1111/ips.12048/pdf

BBC. 3rd November 1999. "Echelon spy network revealed." Accessed 22nd June 2015. http://news.bbc.co.uk/2/hi/503224.stm

BBC. 29th May 2001. "Q&A: What you need to know about Echelon." Accessed 22nd June 2015. http://news.bbc.co.uk/2/hi/science/nature/1357513.stm

Brown, B. 29th March 2012. "The purpose of Project PM." Accessed 22nd June 2015. http://barrettbrown.blogspot.de/2012/05/purpose-of-project-pm.html

Cardoso, D., P. Mthembu, M. Venhaus and M. Verde Garrido. 2014. *The transatlantic colossus: Global contributions to broaden the debate on the EU-US free trade agreement*. Berlin Forum on Global Politics, Internet & Society Collaboratory, and FutureChallenges.org: Berlin. Accessed 22nd June 2015. http://bfogp.org/publications/the-transatlantic-colossus/

Castells, M. 2000. "Towards a sociology of the network society." *Contemporary sociology* 29 (5): 693-699. Accessed 22nd June 2015. http://www.jstor.org/stable/2655234

Castells, M. 2005. "Global governance and global politics." *PS: Political science & politics* 38 (1): 9-16. Accessed 22nd June 2015. http://www.apsanet.org/imgtest/2005global-castellas.pdf

Coleman, R. and M. McCahill. 2011. *Surveillance and crime*. London: SAGE Publications Ltd.

Electronic Frontier Foundation. 2012. "Anti-Counterfeiting Trade Agreement." Accessed 22nd June 2015. https://www.eff.org/issues/acta

Foucault, M. 2003. *"Society must be defended": Lectures at the Collège de France, 1975-76*. New York: Palgrave Macmillan.

Foucault, M. 2007. *Security, territory, population: Lectures at the Collège de France, 1977- 1978*. New York: Palgrave Macmillan.

Foucault, M. 2008. *The birth of biopolitics: Lectures at the Collège de France, 1978-1979*. New York: Palgrave Macmillan.

Foucault, M. 2011. *The courage of truth: The government of self and others II: Lectures at the Collège de France, 1983-1984*. New York: Palgrave Macmillan.

Foucault, M. 1980. "Truth and power." In *Power/knowledge: Selected interviews & other writings 1972-1977*, edited by Colin Gordon, 109-133. New York: Pantheon Books.

Deibert, R. 2011. "Towards a cyber security strategy for global civil society?" Accessed 22nd June 2015. http://www.giswatch.org/sites/default/files/gisw_-_towards_a_cyber_security_strategy.pdf.

European Parliament's Temporary Committee on the ECHELON Interception System. 11th July 2001. "REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)." Accessed 22nd June 2015. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

European Parliament's Directorate General for Internal Policies. 2013. "The US surveillance programs and their impact on EU citizens' fundamental rights." Accessed 22nd June 2015. http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf

Galloway, A. 2004. *Protocol: How control exists after decentralization*. Cambridge, MA: MIT Press.

GigaOM. 16th July 2014. "UN human rights report blows apart governments' pro-surveillance arguments." Accessed 22nd June 2015. http://gigaom.com/2014/07/16/un-human-rights-report-blows-apart-governments-pro-surveillance-arguments/

The Guardian. 24th March 2014. “Fear of slowdown in US and Eurozone as China’s factories cut input.” Accessed 22nd June 2015.” Accessed 22nd June 2015. http://www.theguardian.com/world/2014/mar/24/china-factories-cut-output-us-eurozone-slowdown

The Guardian. 14th April 2014. “Guardian and Washington Post win Pulitzer Prize for NSA revelations.” Accessed 22nd June 2015. http://www.theguardian.com/media/2014/apr/14/guardian-washington-post-pulitzer-nsa-revelations

The Guardian. 21st June 2013. “GCHQ taps fibre-optic cables for secret access to world’s communications.” Accessed 22nd June 2015. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

The Guardian. 30th June 2014. “Facebook reveals news feed experiment to control emotions.” Accessed 22nd June 2015. http://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds

The Guardian. 8th July 2014. “US military studied how to influence Twitter users in Darpa-funded research.” Accessed 22nd June 2015. http://www.theguardian.com/world/2014/jul/08/darpa-social-networks-research-twitter-influence-studies

Institutional Investor. 30th January 2014. “The race to topple Bloomberg.” Accessed 22nd June 2015. http://www.institutionalinvestor.com/Article/3303623/Banking-and-Capital-Markets-Corporations/The-Race-to-Topple-Bloomberg.html?ArticleId=3303623&single=true

The Intercept. 19th May 2014. “Data pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas.” Accessed 22nd June 2015. https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

The Intercept. 14th July 2014. “Hacking online polls and other ways British spies seek to control the Internet.” Accessed 22nd June 2015. https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/

International New York Times. 2nd November 2nd 2013. “Documents show N.S.A. efforts to spy on both enemies and allies.” Accessed 22nd June 2015. http://www.nytimes.com/interactive/2013/11/03/world/documents-show-nsa-efforts-to-spy-on-both-enemies-and-allies.html?_r=0#doc2

Internet Governance Project. 20th September 2011. “Russia & China propose UN General Assembly resolution on “information security.” Accessed 22nd June 2015. http://www.internetgovernance.org/2011/09/20/russia-china-propose-un-general-assembly-resolution-on-information-security/

La Quadrature du Net. 20th October 2013. “Will the Canada-EU trade agreement harm our freedoms online?” Accessed 22nd June 2015. https://www.laquadrature.net/en/will-the-canada-eu-trade-agreement-harm-our-freedoms-online

Lyon, D. 2011. *Surveillance studies: An overview*. Cambridge: Polity Press.

Mann, S. 2004. “‘Sousveillance’: Inverse surveillance in multimedia imaging.” Accessed 22nd June 2015. http://www.eyetap.org/papers/docs/acmmm2004sousveillance_p620-mann/

Mann, S. 2014. “The sightfield: Visualizing computer vision, and seeing its capacity to ‘see.’”. Accessed 22nd June 2015. http://www.cv-foundation.org//openaccess/content_cvpr_workshops_2014/W17/papers/Mann_The_Sightfield_Visualizing_2014_CVPR_paper.pdf

Mann, S. and M.A. Ali. 2013. “The inevitability of the transition from a surveillance-society to a veillance-society: Moral and economic grounding for sousveillance.” Accessed 22nd June 2015. http://www.eyetap.org/papers/docs/IEEE_ISTAS13_Veillance2_Ali_Mann.pdf

Mann, S. and J. Ferenbok. 2013. “New media and the power politics of sousveillance in a surveillance-dominated world.” *Surveillance & Society* 11 (1/2): 18-34. Accessed 22nd June 2015. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/veillance/veillance

Masnick, M. 25th November 2013. “Shameful business: Corporate giants target activists and non-profits for corporate espionage.” *Techdirt*. Accessed 22nd June 2015. https://www.techdirt.com/articles/20131122/01100925334/shameful-business-corporate-giants-target-activists-non-profits-corporate-espionage.shtml

Murakami Wood, D. 2013. “What is global surveillance? Towards a relational political economy of the global surveillant assemblage?” *Geoforum* 49: 317-326. Accessed 22nd June 2015. http://dx.doi.org/10.1016/j.geoforum.2013.07.001

New York Times. 7th June 2013. “Tech companies concede to surveillance program.” Accessed 22nd June 2015. http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?smid=tw-share&_r=1&&pagewanted=all

New York Times. 9th June 2013. “Leaker’s employer is paid to maintain government secrets.” Accessed 22nd June 2015. http://www.nytimes.com/2013/06/10/us/booz-allen-grew-rich-on-government-contracts.html

New York Times. 8th October 2013. “European officials consulted business leaders on trade pact.” Accessed 22nd June 2015. http://www.nytimes.com/2013/10/09/business/international/european-officials-consulted-business-leaders-on-trade-pact-with-us.html?pagewanted=all

New York Times. 20th May 2014. “Fine line seen in U.S. spying on companies.” Accessed 22nd June 2015. http://www.nytimes.com/2014/05/21/business/us-snooping-on-companies-cited-by-china.html

Pew Research Internet Project. 3rd July 2014. “Net threats.” Accessed 22nd June 2015. http://www.pewinternet.org/2014/07/03/net-threats/

Pillay, N. 16th July 2014. “Press conference on the right to privacy in the digital.” *Office of the High Commissioner for Human Rights*. Accessed 22nd June 2015. http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14874&LangID=E

The Pulitzer Prizes. 2014. “The 2014 Pulitzer Prize Winners: Public Service.” Accessed 22nd June 2015. http://www.pulitzer.org/citation/2014-Public-Service

Ruddy, T. 2014. “Regimes governing the re-use of personal data in the US and the EU: A primer on mass surveillance and trade” In *The transatlantic colossus: Global contributions to broaden the debate on the EU-US free trade agreement*, edited by D. Cardoso, P. Mthembu, M. Venhaus and M. Verde Garrido, 92-98. Berlin Forum on Global Politics, Internet & Society Collaboratory, and FutureChallenges.org: Berlin. Accessed 22nd June 2015. http://bfogp.org/publications/the-transatlantic-colossus/

Snowden, E. 17th July 2014. “Edward Snowden: ‘If I end up in chains in Guantánamo I can live with that’ - video interview.” *The Guardian*. Accessed 22nd June 2015. http://www.theguardian.com/world/video/2014/jul/17/edward-snowden-video-interview

Timm, T. 5th June 2014. “Four ways Edward Snowden changed the world – and why the fight’s not over.” *The Guardian*. Accessed 22nd June 2015. http://www.theguardian.com/commentisfree/2014/jun/05/what-snowden-revealed-changed-nsa-reform

Tufekci, Z. 2014. “Engineering the public: Big data, surveillance and computational politics.” *First Monday* 19 (7). Accessed 22nd June 2015. http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097

Schneier, B. 26th November 2013. “‘Stalker economy’ here to stay.” *CNN*. Accessed 22nd June 2015. http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html

United Nations’ Human Rights Council. 30th June 2014. “The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights.” *Office of the High Commissioner for Human Rights*. Accessed 22nd June 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Wired. 16th May 2014. “Encrypted web traffic more than doubles after NSA revelations.” Accessed 22nd June 2015. http://www.wired.com/2014/05/sandvine-report/