April 17, 2015

Hack or Be Hacked: The Quasi-Totalitarianism of Global Trusted Networks

Athina Karatzogianni
Martin Gak

HACK OR BE HACKED: THE QUASI-TOTALITARIANISM OF GLOBAL TRUSTED NETWORKS[1]

Athina Karatzogianni and Martin Gak

Abstract This article focuses on digital surveillance ideology by examining specific empirical examples drawn from media reports of the Snowden affair, in order to nuance the politics, ethics, values and affects mobilized by governments and corporate elites to justify the collect-it-all practices by a *ménage à trois of "trusted" global networks*. It charts this political space as a sphere of action emerging against the backdrop of what we call 'quasi-totalitarian' mechanisms, which are fostered by alignment, collusion and imbrication of the three trusted authoritative networks. This approach accounts for a particular vexing problem in the articulation of digital politics. That is, the process of political disenfranchisement by corporations looking to profit, governments looking to regulate information flows, and coopted groups in civil society looking to appropriate the legitimate concerns of users for their own political and financial subsistence. The distinct features of this quasi-totalitarianism include a. the monopoly of digital planning on surveillance resting on back-channel and secret communication between government, tech corporate elites and, sometimes, NGOs; b. the role of civil society NGOs as mechanisms for circumventing democratic processes c. enterprise association politics that ensures that the dual goal of state (security) and capital (profit) continues unabated and unaccounted; d. the unprecedented scope in the form of total structural data acquisition by western intelligence matrixes; e. the persecution and prosecution of journalists, whistle-blowers and transparency actors outside the scope of civil society groups and f. the significant if insufficient contestation by members of the public concerning the infringement on civil liberties.

Keywords surveillance, ideology, quasi-totalitarian, Snowden, digital networks, technological elites, governments, international relations, privacy, resistance, movements

The remains of a computer that held files leaked by Edward Snowden to the Guardian and destroyed at the behest of the UK government. Photograph: Roger Tooth[2]

Introduction

‘Who has the info on you? It’s the commercial companies, not us, who know everything – a massive sharing of data’[3] Sir Iain Lobban, Former Director of Director of the Government Communications Headquarters (GCHQ), UK.

The public reaction to recent revelations about state and corporate surveillance and control has ranged from general bemusement to marginal outrage both in the US and Europe.[4] The public has been slow to react and yet, the political fallout had to be addressed. Governments and tech elites accused each other of being responsible for the public loss of trust and of compromising privacy and the integrity of networks. The National Security Agency’s (NSA) programs were put in place and ran for seven years without public oversight or debate. The Obama administration justified the implementation of the military intelligence agency’s program--the NSA is part of the Department of Defense--by claiming that it has been crucial in successfully thwarting terrorist attacks. Such claims have been contested, but this has hardly made a difference in the continued deployment of these programs. In the trade off between privacy and security, governments have argued in favor for the need for exceptions from the legal framework, in order to protect the public.

Meanwhile, tech elites expressed exasperation, while remaining fairly opaque about their practices in relation to privacy and security. In order to guarantee their own income flows and their reputation as socially responsibly corporate actors, technocapitalists have struck a pose that has not been entirely consistent with their practices. A third group of dubious ancestry has also come to take a prominent role in the debate. Civil society organizations advocate transparency and open accessenabled deliberation, as well oversight of the processes involved, claiming for themselves to be the voice of the public. Their involvement has issued all manners of crusades in defense of putative democratic principles and constitutional guarantees, which are being circumvented by the governing bodies.

This *ménage à trois of "trusted" global networks* -- governments, corporations, and NGOs -- are holding the *de facto* mandate and the effective planning power in the digital field. They clothe themselves in a bastardized version of publicness and in such guise, usurp the political agency of individual members of society. In fact, these three supposedly trusted networks constitute an oligopoly, which dominates the space in which governance is negotiated. They relegate the individual to a place of marginality and a position of acute precariousness, from which they have to address the threat of surveilling agents to their privacy. And yet, it is the individual who has to pay for digital equipment, access and for the necessary digital literacy and in this way fund purchase, connectivity and training. It is also the individual who has to acquire skills and software to protect their privacy in digital homes built by tech elites and surveilled by governments (in the name of security) and corporations (for the sake of profit). The individual citizen is put in a rather impossible situation, in which they must simultaneously procure the tools for the enforcement of the legal guarantees presumably held by the state to protect their rights, and at the same time develop tools to enforce them. In this environment, in which the state undermines privacy in the name of security, commercial interests collude with the state while offering false shelter, and civil society groups hijack the very voice of political engagement, the individual has only one choice: *'hack or be hacked'*. It is, therefore, the precarious state of rights in the face of these developments that inspire and stand as the rationale for this article.

Hence, the main purpose of this article is to chart this political space as a sphere of action emerging against the backdrop of what we call ‘quasi-totalitarian’ mechanisms, which are fostered by alignment, collusion and imbrication of the three trusted authoritative networks. This approach accounts for a particular vexing problem in the articulation of digital politics. That is, the process of political disenfranchisement by corporations looking to profit, governments looking to regulate information flows, and coopted groups in civil society looking to appropriate the legitimate concerns of users for their own political and financial subsistence. The rearticulation of the current political landscape of the digital sphere, in terms of such dynamics, should also help to show that technosocial transformations of agency must promote a civil type of association inspired by radical democratic politics, which is capable of contesting the practices of these three trusted networks.

Adrift amid digital fiefs

The three networks (corporate, government, civil society) vie for control of the individual’s communication performance, but none of them has been entirely successful. Needless to say, these networks are not synonymous with particular political actors, and have structural and formal similarities in the form of a hierarchical, social and political economic logic based on reactive desire.[5] These authoritative networks are emergent properties of a dynamic of hierarchical power that can be found, with their indigenous properties, across the board.

Should this oligopoly of semi-centralized surveillance succeed in asserting control, only communications with intentions plainly visible to the networks would be licit. For the securitizing governmental power this amounts to a logic that takes every digital communicative act to be pernicious unless proven innocuous. For corporate power, this amounts to the commodification of each digital communicative act. And for civil society, this amounts to the political capitalization of the rights and obligations of the individual digital engagement in the face of the other two networks.

To demonstrate this point, let us draw an analogy to Hayek's argument on economic control and totalitarianism. In the 7th chapter of his *Road to Serfdom,* Hayek highlights *the common assumption that economic control does not affect freedom.* Something very similar can be said about the common assumption that digital control does not affect basic rights. This is what happens when one replaces the word *economic* with the word *digital*, in one of Hayek's most celebrated passages:

> The so called *digital* freedom which the planners promise us means precisely that we are to be relieved of the necessity of solving our own *digital* problems and the bitter choices which this often involves are to be made for us. Since under modern life we are for almost everything dependent on means, which our fellow men provide, *digital* planning would involve direction of almost our whole life. There is hardly an aspect of it, from our preliminary needs to our relations with our family and friends, from the nature of our work to the use of our leisure, over which the planner would not exercise his "conscious" control.[6]

As in economic matters, in digital matters, the tacit acquiescence of the agent to the unchecked power of “digital planners” -- in the form of international and national governing bodies, deep state policing surveillance and the technology developed by corporate actors -- are the crucial mechanisms of societies of control and ought to be the focal point of any discussions on the matter. The recent Snowden documents and Assange’s WikiLeaks cables leaked by Manning provide significant evidence in hundreds of thousands of documents, that operating in the shadows, there is a *U.S. led transnational authority comprised by global trusted networks* presently directing surveillance of digital networks almost in their entirety. This informal authority seems to have entailed the collaboration, albeit hesitant, of transnational corporate tech elites and ultimately the assent of civil society actors who also vie for a role in digital governance. Due to the ever-growing and ever-strengthening constitution of an oligopoly of surveillance, the power over information and communication this authority can exert, is nothing less than *control over both digital consumption and production.* Similar mechanics of digital control can be found in China and Iran for example, so this occurs at a global scale.[7]

Of interest, is not just the power and reach of this oligopoly of digital planners, but *the specific types of ideological positions* and logics of political and commercial necessity deployed to account for the source power and justify its exercise. The shaping control that the planners collectively exert over information and communication is visible in the programs of surveillance, as well as the relentless governmental crackdowns on movements in favor of transparency and advocacy of new alternatives.

The sense that these acts of control and usurpation are about ‘others but not me’ may serve as a partial confirmation of Wacquant’s supposition concerning the ‘desolidarizing’ impacts of ‘synoptic’ surveillance and ‘lateral’ surveillance.[8] The targeted individuals and groups in surveillant assemblages,[9] such migrants, protesters, school children, and individuals under probation, which McCahill and Finn[10] interviewed, despite facing relentless challenges imposed by surveillance, can develop *surveillance capital*:[11] ‘long-term activists utilized economic, social and cultural capital to evade or contest surveillance in various ways…the subjective experience of surveillance was often expressed in positive terms with many protesters describing their experiences in terms of “play”, “excitement”, and as “identity affirming”, rather than “oppression” or “coercion”.[12]

Nevertheless, in the aftermath of the Snowden affair, Wacquant’s desolidarization is politically evident across the board, while surveillance capital strategies are sure to be developed among the general population. This is because surveilling power is no longer one restricted to malfeasance, illegality, resistance or dissent. Surveillance is the very condition of civil engagement in the digital sphere and this requires a broader theoretical discussion.

Features of Totalitarianism

Despite the lofty conceptualizations of digital utopias and dystopias, the old modernist demands for power, participation and democracy still hold currency and, thus, race, gender, class and other mechanisms of hierarchizations are produced and reproduced in digital networks.[13] The alignment of technology corporations, government elites, civil society agents, and the passive acquiescence of the public amounts to a collective propensity, which resembles *totalitarianism.* This political ethos is built upon the tacit consensus and the covert prescription of individual and collective transparency. It is therefore critical to account for the traditional ideological and political categories driving the surveillance complexes in the United States, the UK and the west more generally, as well as in countries where alternative socio-political arrangements may be in place. The term quasi-totalitarianism used here is inscribed into a genealogical continuum in historical and political academic discussions that have dealt with various forms of authoritarianism and despotism (Fascism, Nazism, the Soviet regimes, semi-peripheral dictatorships in Latin America and the MENA region, post-totalitarianism and so on), both on the right and on the left.[14]

The totalitarian principle is this: the state exerts total control over its members. This does not mean merely performative control, but also cognitive control, both the doings and thoughts of citizens are determined by the state power. The term, coined by Carl Schmitt in *The Concept of the Political* corresponds to a state which embracing every domain of social life ultimately results in the indistinguishability of state and society. In such a state, according to Schmitt everything is in principle political.[15] The interpenetration of state and society--the hyperpolitization of the social--is the most salient characteristic of totalitarianism. Totalitarianism is not merely authoritarianism in which the power is exerted from above the social fabric. In this regard, Schmitt points out that ‘a state standing above society could be called universal but not total’.[16]

The mutual permeability of the political and the social means that in totalitarianism the *motus*[17]*politicus* tends to become--never fully is, though--indistinguishable from the *motus socialis*. The individual members of society become agents of the political demands of the state and the state becomes the space for promoting the social demands of the collective of individuals. Importantly, this correlates to the occupation of private space that in all forms of totalitarianism is submitted to political and collective scrutiny. [18]

In this regard, the current alignment of trusted networks and acquiescing subjects bears the hallmarks of the totalitarian inter-permeability of political and social agency. On the grounds of foretelling putative terrorist or criminal activity by organizations or individuals, forecasting market practices or modifying socio-cultural practices by changing the underpinning attitudes, governments, corporations and civil society actors collude in explicit and implicit normalization of the moral valuation of transparency.

Authors like Arendt and Popper, have taken a utopian agenda to be a distinctive mark of totalitarianisms. Popper takes totalitarianism to be instrumental practices oriented to the attainment of what he calls the *Ideal State.*[19] Totalitarianism is for him, a utopian engineering project constructed on the notion that the life of the polis is the instrumental implementation of norms oriented to the realization of a ultimate political goodness. Ultimately, for Popper, totalitarianism is intimately related to politics understood as soteriology.

However, the *masses,* as Arendt calls the contingent of individuals that totalitarian leaders expect to be the bearers of this political faith, are not natural adherents to political theologies, even if more often than not, totalitarian processes recruit and deploy ideas of an ultimate political state that can already be found somewhere among the population. For this, the totalitarian agent deploys mechanisms of inculcation. Propaganda is central to the construction of the political imaginary of the public.[20] Mechanisms of inculcation are central to totalitarian states and must be broadly understood as longitudinal processes of cognitive control. Propaganda is not aimed at what individuals do, but rather at what individuals think and feel. Propaganda is designed to inculcate among the *mass* the commitment of faith to the *Ideal State*. Finally, then, surveillance of communicative acts is not merely a way to probe, predict and prevent certain actions, but it is, insofar as it assesses the content of thought and sentiments, a way to test the efficiency of propaganda. Therefore, Friedrich and Brzezinski' s 1956 totalitarianism has the following salient elements: ideology of perfect final state of mankind, a single mass hierarchical party, monopolistic control of the military and communications, terroristic police control, and central control and direction of the economy. In Deleuze and Guattari,[21] it is the state machine, which captures social flows and assemblages decomposing their horizontal connections along the way.

Now the consensus of our three trusted networks with the tacit acquiescence of the individual user share several features of these mechanisms. For example, in most political communities, the emergence of a broad political consensus is bound to the emergence of a status quo that demarcates the gravitational center of a polity. In fact, the tacit consensus is undergirded by the fusion of the *motus politicus* with the *motus socialis*. Whereas the 20th century saw this kind of coalescence in ideas of national purity and ethno-cultural exclusivity on which they built their *Ideal State*, in the dawn of the 20th century and early 21st, neo-liberals and social democrats have become the designers of accounts of the *ideal state* that have permeated every aspect of the social fabric. Since the mid-twentieth century, even in most despotic states the ideological construction of the *ideal state* has responded to variations of these two socio-political imaginaries. The strange new political animal is something along the lines of a progressive neo-liberal version of totalitarianism: A Quasi-totalitarianism.

Quasi-Totalitarianism and the Oppression of Tacit Consent

The centers of digital planning and of surveillance networks are steeped in an ideology which has markedly totalitarian features, but which is not instantly recognizable as part of the historical events, regimes, political practices that during the 20th century have been built on the total politicization of everyday life.

There are two important variations. Quasi-totalitarianism is not dependent on the account of an *Ideal State*, though the justifications for the policy measures devised and deployed on the networks will be presented as instrumental to a putative critical end: security, growth or better socio-cultural habits. But a caveat is in order here, in the alignment of the three networks, it is to a large degree civil society the one that systematically appeals to an *ideal state* discourse to promote its own agendas. Hardly will we find users who earnestly take a Manichean approach to life in the digital sphere. It is rather, agents of the public sector who insist in depicting the digital space as either an utopian dream or a dystopian nightmare.[22]

The second way in which quasi-totalitarianism differs from its ancestor concerns the direction of the construction of an ideological consensus. With the exception of civil society, the “trusted networks” are not in the business of peddling a narrative of a future “ideal state”. Corporations, as private institutions merely need to promote their products and services and sustain the conditions that had already brought them to commercial dominance and government agencies operating in the shadows need no assent form the *mass.* It is rather the strategy of political consensus of the totalized center that scaffolds the planning schemes of the networks.

It is the emergence of the center consensus among civil actors that seems to dictate the ideological constitution of power and not the other way around. In this sense, quasi-totalitarianism recruits and deploys some of the mechanisms inherent in democratic process. In some ways, the rule is of the people. Yet, as in totalitarianism there is a movement towards the interpenetration of the social and the political. Perhaps the most illuminating mechanism that ought to be underscored is the banal enforcement of the policies that help to propagate the socio-political consensus of the center.

The banal repetition of the tasks that are assigned by the trusted networks which seem to have little or no connection to the determination of political practices--opening one’s laptop, logging onto a network, sending a phone message, etc--are the agglomeration of actions that individuals perform unreflectively to sustain the status quo and its mechanisms of socio-political cohesion.[23] The preservation and promotion of the status quo is also the preservation and promotion of the center. In digital practices, this ideological hybrid is peddled by the ample and collective center in the form of the centralized networks, which negotiate their respective need to surveil, profit from and, perhaps curiously, also act on behalf of the putative freedom of users.

Forms of Association in Quasi-Totalitarianism

The difference between the ideological role that the *ideal state* plays in the totalitarian model and the quasi-totalitarian model may be best explained by Michael Oakeshott's two accounts of political enterprises in *On Human Conduct.* For Oakeshott, it is in Aristotle's account of the fellowship of the polis that we can best see how a relation of peers may best sustain a political association impervious to instrumentality.[24] As opposed to an enterprise association that gathers to guarantee the attainment of an aim--profit, conquest, production, etc--the fellowship of *civility* can be sustained without a common goal. According to Oakeshott, the civil association (the fellowship of civility) is grounded on the internal coherence of the mutual recognition and completeness of being members of each other's group. [25]

Each of the three trusted networks emerges from agglomerations of groups with manifest and extrinsic substantive purposes. The corporate group amounts to a 'fellowship of the bread in the bin'. That is to say, an instrumental grouping of agents. Government is a set of associations whose enterprise is household management (*economos),* while civil society actors are essentially associations of political enterprise--in the vulgar sense of the political. At the same time, it is the idea of the preservation of a fellowship of mutual recognition and belonging that--at least in word--the networks are supposed to be intended on preserving and promoting. It is the integrative idea of the center, which fulfills for these networks the justificatory role of the *ideal state.* But this ideal state, rather than being extrinsic--a utopian future--is in some sense already achieved and must be preserved. What the integrative idea of the center justifies is then a vast number of suspensions of the hard-won legal and political instruments that have been deployed precisely to ensure the civility of the center's consensus. The trusted networks justify the supposedly intermittent violation of privacy, free association, freedom of expression by asserting the instrumental need of structural data acquisition, surveillance, digital network infringement, with the added disruption of computer security and encryption.

In the context of intensely networked societies, it has not been enough to mobilise arguments about constitutionalism and democratic principles against the control of big data and digital network infrastructures by state, corporate actors and civil society actors who collaborate in governance. It is obvious, that the digital network machine is entangled within state and corporate-controlled network environments and with civil society networks, which certify their behavior by providing something like political quality control. In this regard, association in the digital public sphere is taking place mostly within the confines of corporate platforms (geared toward enterprise), even when the association involves civil functions, such as political participation and dialogue, as is the case with civil society actors.

The story of the rather vast catalogue of legal violations that have flooded the public sphere as a result of the Snowden leaks show that indeed the legal principles, on which democratic life has been built, have been insufficiently protected from the ulterior motives of the three incorporated networks. Within the context of these debates, the term 'quasi-totalitarian' explains the resemblance of the collect-it-all practices of the governments and corporate actors to historical practices of the past, without trivializing the historical experiences of totalitarianism.

Moreover, on another level, the quasi-totalitarianism of the center, points to the "Center" of the ideological spectrum. Traditionally, the center has been occupied by liberals and social democrats of some description or another in democratic systems. Nevertheless, the ideological center in non-democratic states is in turn the ideological center in the specific spectrum of the political culture in country-specific contexts. The quasi-totalitarianism of the center refers here to a second layer in relation to centralized hierarchical organizations, even if they are networked, because the sociopolitical logic remains hierarchical despite the use of network communications. The centers of digital planning and of surveillance networks are quasi-totalitarian in character.

This is exactly why liberals and social democrats, parliamentarians and others in the Western ideological center find it preposterous a suggestion that ubiquitous surveillance (the digital planners' control over global networks) is a totalitarian practice. This version of totalitarianism draws its ideological content *from the ideological center of the political system.* In this sense, surveillance complexes are the direct genealogical offsprings and mirror the political ideology dominant in any given political system.

However, the paradox in the present case scenario is that neither neo-liberalism or social democracy, which are the two dominant ideologies in contemporary liberal democratic states, are the ideologies by which digital control is exercised in practice. Who can forget Chris Hune, Secretary of State for Energy and Climate Change from 2010 to 2012 and his exasperation about having no idea about GCHQ activities? 'Cabinet was told nothing about this.'[26] This quasi-totalitarianism relies on a type of enterprise association to flourish, in contrast to civil association, which was until recently the most common ideal type of association in traditional representative politics and fed in favor or in opposition the totalitarianism of the left, the right, and the liberal and social democratic varieties of the past.

Association in the digital public sphere is taking place mostly within the confines of corporate platforms (geared toward enterprise), even when the association involves civil functions such as political participation and dialogue. *Civil association,* as a self-authenticating practice of practices, which has no corporate aggregate purpose, except to keep politics open and the discussion going, and can serve both as a response to the above critique and as a powerful new vision for the network *res publica*, which is presently dominated by human conduct primarily geared toward forms of enterprise association.

The conflict is succinctly explained by Noel O'Sullivan who underscores 'a tension between the rule of law to which civil association is committed and the subordination of it to the administrative powers of governments bent on imposing substantive conceptions of the good society.'[27] It is important to underscore the fact that the principle of civility that is entailed in the political assertions and propositions of the center is often, if not regularly, co-opted by the enterprise associations who present their own aims as instrumental necessities of the preservation of the civil associations. So, in a sense, the task at hand for the radicalization of a democratic model is to foreclose the usurpation of civil associations at the hands of enterprise associations. In other words, the work consists in resisting the articulation of the fellowship of civility as an endangered model whose safeguard can be readily confused with an *ideal state.* The fellowship of civility is not a state of attainment such as the holding of a profit or the end of conflict. It is, rather, the form of a political performance so it cannot be captured in an ideal state without negating its non-instrumental nature.

Indeed, as Noel O'Sullivan has pointed out, a charitable reading of Oakeschott's accounts of civility in the face of the instrumentalization of the political may be well-suited to the rearticulation of democratic fellowship against the impingement and usurpation of civility by the political intromission of enterprise associations. He writes: 'Chantal Mouffe, a sympathetic critic, has suggested that Oakeshott's narrowly conceived concern with civil association might be overcome by *relocating the civil model within a radical democratic framework* that would encourage active participation in politics, thereby removing Oakeshott's reliance on what may prove to be a minority consensus about forms and procedures'.[28] Significantly, the danger of not recognizing the transformation of a civil into an enterprise state is a crucial problem in present politics: 'Even though the transformation of a civil into an enterprise state may be acceptable on occasion, insofar as it is necessary to defend or maintain civil association itself, the price to be paid must be clearly recognized: it is that the rule of law ceases to be the bond of citizens, and thus the state, for the time being, is no longer a free one.' [29]

Snowden's Conduct as Civil Association

Edward Snowden's leaks of hundreds of thousands of National Security Agency documents is positioned against enterprise association. Notwithstanding the conspiratorial tone, the group Anonymous' response to Snowden's attempt to put surveillance under public scrutiny shows quite poignantly the reaction to the revelations by movements instinctively opposed to quasi-totalitarian models of the digital public sphere:

> Your privacy and freedoms are slowly being taken from you, in closed door meetings, in laws buried in bills, and by people who are supposed to be protecting you…. Download these documents, share them, mirror them, don't allow them to make them disappear. Spread them wide and far. Let these people know, that we will not be silenced, that we will not be taken advantage of, and that we are not happy about this unwarranted, unnecessary, unethical spying of our private lives, for the monetary gain of the 1%.[30]

In its communiqués, Anonymous often portrays itself as a bearer of the values of civil association, as protectors of the fellowship of civility. Understandably, the articulation of this un-trusted network's commitment is advanced in moral terms and more often than not they present themselves as a new surreptitious actor who engages in global political vigilantism in order to mount resistance against surveillance, censorship, perceived injustice and corruption and in solidarity with movements fighting repressive and authoritarian governments. Anonymous and Snowden serve to demarcate the space of resistance to the hidden mechanics of thoroughgoing political penetration of the social and in so doing, unconceal the totalitarian mechanisms, which they both claim to resist.

According to *The Guardian*, one of the main media organisations with which Snowden collaborated, the NSA's Prism program is the biggest single contributor to its intelligence reports that the American leaked. Prism was a 'downstream' program, which means that the agency collected data from Google, Facebook, Apple, Yahoo and other US internet giants. One slide showed that the agency had 'direct access' to the companies' servers. This, however, has been hotly disputed by the tech giants, who maintain that they only complied with lawful requests for user data.[31] The documents also exposed the existence of Tempora, a program established in 2011 by UK's GCHQ. This program gathers en mass data from phone and internet traffic by tapping into fiber-optic cables. GCHQ shared most of its information with the NSA.

The documents, marked top-secret, came in the wake of other high-profile disclosures attributed to Snowden since he first started collaborating with the Guardian for articles published beginning June 6 2013. The United States government has since indicted Snowden under the Espionage Act, which prompted him to request asylum from no fewer than 20 nations. Ironically, it was in the end Putin, who obliged and provided him with asylum.

The relationship between NSA and tech giants is indeed a complicated one. According to *The Guardian*, from June to July 2010, data from Yahoo generated by far the largest number of NSA intelligence reports. This was followed by Microsoft, and then Google. All three companies are fighting through the courts to be allowed to release more detailed figures for the numbers of data requests they handle from US intelligence agencies. The agency is allowed to travel 'three hops' from its targets — who could be people 'who talk to people who talk to people who talk to you'. In Facebook, where the typical user has 190 friends, three degrees of separation gives a user access to a network bigger than the population of the state of Colorado (approx. 5.260.000 people). According to internal documents cited by journalists, Microsoft 'developed a surveillance capability' that was launched "to deal" with the federal authorities who were concerned that they'd be unable to wiretap encrypted communications conducted over the web in real time. The response from Microsoft Vice President, John Frank was*:* 'We continue to believe that what we are permitted to publish continues to fall short of what is needed to help the community understand and debate these issues'.[32]

Two French human rights groups filed a legal complaint targeting the U.S. National Security Agency, the FBI and seven technology companies they say may have helped the United States snoop on French citizens' emails and phone calls. The complaint denounced U.S. spying methods as revealed by Snowden and filed against 'persons unknown', but names Microsoft, Yahoo, Google, Paltalk, Facebook, AOL and Apple as 'potential accomplices' of the NSA and FBI. The International Federation for Human Rights (FIDH) and the French Human Rights League (LDH) argued that 'This blatant intrusion into individuals' lives represents a serious threat to individual liberties and, if not stopped, may lead to the end of the rule of law' (LDH).[33] Reports point also to 'alliances with over 80 major global corporations supporting both missions'. In NSA jargon, "both missions" refers to defending networks in the US, on the one hand, and monitoring networks abroad, on the other. The companies involved include telecommunications firms, producers of network infrastructure, software companies and security firms'.[34]

Mark Zuckerberg, CEO of Facebook and Marissa Meyer, CEO of Yahoo defended their companies against critics who charged tech companies with doing too little to fight off NSA surveillance. Mayer said executives faced jail if they revealed government secrets. Yahoo unsuccessfully sued the foreign intelligence surveillance (FISA) court, which provides the legal framework for NSA surveillance. In 2007, it asked to be allowed to publish details of requests it receives from the spy agency. Mayer reportedly said that 'When you lose and you don't comply, it's treason. We think it makes more sense to work within the system', while Zuckerberg said the government had done a ‘bad job’ of balancing people's privacy and its duty to protect with his now famous quote: ‘Frankly I think the government blew it’.[35]

The escalation of tensions between corporations and government, whether earnest or fabricated for public consumption, points to decision-making processes that sit clearly beyond governance by democratic methods and principles. It involved back-channel negotiations between state and corporate elites under a veil of secrecy cast by legal provisions banning the divulgation of information even about the existence of the requests made by the NSA.[36] That would be treason, as Meyer pointed out.

The Stop Watching Us campaigns and 11 February global campaign against surveillance, as well as Privacy groups such as the Electronic Privacy Information Center and the Electronic Frontier Foundation launched lawsuits that have led to disclosure of hundreds of pages of FISA Section 215 subpoenas, which since 1988 gave the government the authority -- with the courts previous approval—to obtain records in the course of foreign intelligence investigations. GCHQ and NSA surveillance is facing a legal challenge at the European Court of Human Rights from Big Brother Watch, English PEN and Open Rights Group. Google, Microsoft and Yahoo, facing a backlash from their users in the US and overseas over mass surveillance, are fighting to be allowed to be more transparent about their dealings with the intelligence agencies. These companies, along with Facebook, Apple and AOL have also written to Senate an open letter demanding reform. In fact the review by the Obama administration was conducted as a response and did little to satisfy critics.

Western governments in liberal democracies operate under statutes prohibiting espionage conducted against their own populations. But as the large-scale study by the Center for European Policy Studies published in November of 2013 shows, the solidity of the provisions and the efficiency of oversight mechanisms to uphold the law vary from country to country. Referring to a The Guardian article from August of that year, the study says:

> This would point to a potential scenario of privacy shopping by services to exploit regimes with the weakest protection/oversight or with the greatest legal loopholes. Such a scenario is to some extent reflected in reports indicating that GCHQ marketed itself to the NSA on the basis of the UK's weak regulatory and oversight regime.[37]

Governments are not allowed to spy on their own populations but they can spy on foreign nationals. The US views as second parties the UK, Australia, Canada and New Zealand (the five eyes), and other countries such as Germany and France as third parties, which it can spy upon. This included the EU and notoriously Angela Merkel's mobile phone:

> On an average day, the NSA monitored about 20 million German phone connections and 10 million internet data sets, rising to 60 million phone connections on busy days, the report said. In France, Der Spiegel reported, the United States taps about 2 million connection data a day. Only Canada, Australia, Britain and New Zealand were explicitly exempted from spy attacks.[38]

And yet, the reaction in European capitals of US and UK spy activities has been underwhelming. French President Francois Hollande condemned the practice saying, 'We cannot accept this type of behavior between partners and allies' and the hacking was not necessary for anti-terrorism efforts. 'I do not think that this is in our embassies or in the EU that this risks exist'.[39] Germans watched, as their Chancellor barely seemed to protest at the revelations. In a Der Spiegel article, 'The Cancellor and the NSA: Merkel has abandoned the Germans', the author argues: 'And this about our loyalty to America. Or international terrorism. Or even the role of intelligence services. Everyone has their own opinion about that. This is about our rights being violated without us being able to resist it. We stop being citizens and turn into subjects'.[40]

A second mechanism that seemed to have been in place to create this matrix of surveillance in addition to the exploitation of legal loopholes by a supranational intelligence fiefdom was an economy of favors among agencies: 'Britain's GCHQ intelligence agency can spy on anyone but British nationals, the NSA can conduct surveillance on anyone but Americans, and Germany's BND foreign intelligence agency can spy on anyone but Germans. That's how a matrix is created of boundless surveillance in which each partner aids in a division of roles.' [41]

To a large degree, the logic of surveillance led by the American government and carried out in the matrix of this transnational intelligence fiefdom is a logic of war intelligence. It stands to reason, then, that the central body deploying the strategy of surveillance--the NSA--would be a military signal intelligence unit. Both the system and the actors who carried out the NSA program were, unsurprisingly, operational inheritances of the Iraq war. Greenwald, one of the journalists who brought the Snowden story to public attention, discusses here a profile on the former Director of the NSA, Gen. Keith B. Alexander by the Washington Post:

> The Post explains how Alexander took a "collect it all" surveillance approach originally directed at Iraqis in the middle of a war, and thereafter transferred it so that it is now directed at the US domestic population as well as the global one: "…. *And, as he did in Iraq, Alexander has pushed hard for everything he can get*: tools, resources and the legal authority to collect and store vast quantities of raw information on American and foreign communications."[42]

The subversion of the law, the perversion of democratic rule and the suspension of deliberative consultation was not merely noticed by European researchers and opinion-makers. Bowing to the pressure of civil society actors that smell blood in the water and prepared for a political feeding frenzy and to corporations intent in rescuing their reputation and the loyalty of its public, Obama issued one of the most notable statements of unrepentant repentance in political history:

> Obama "... I called for a review of our surveillance programs. Unfortunately, rather than an orderly and lawful process to debate these issues and come up with appropriate reforms, repeated leaks of classified information have initiated the debate in a very passionate but not always fully informed way…I'm also mindful of how these issues are viewed overseas because American leadership around the world depends upon the example of American democracy and American openness, because what makes us different from

> other countries is not simply our ability to secure our nation. It's the way we do it, with open debate and democratic process."[43]

All evidence to the contrary. The military signal intelligence programs deployed against civilians at home and abroad were entirely lacking in open debate and respect for the procedural principles that underpin democratic rules. The putative legality of the programs showed simply that the US jurisprudential structure had become rife with loopholes and subterfuges that built in a state of exception justified by the so called war on terror had given legal cover to policing practices that had been entirely verboten such as torture, disappearance and secret incarceration and which were now being deployed to justify the largest system of violation of privacy the world had ever seen.

The Third Network: NGOs

Beneficiaries of the debacle have been civil society actors, who as in the case in the aftermath of the catastrophic earthquake that destroyed Haiti, were now also perfectly positioned to take advantage of the momentous occasion. Under the rubric of civil society actors these groups, which are mostly associated to a semi-covert network of American and European foundations dispensing the money of very wealthy corporate actors, projected themselves as the rightful voices of civil associations and the fellowship of civility. The political reach of these groups is predicated on the construction of institutions that are directly dependent on the financial and organizational support of the other two networks.

For instance, Hivos -- a funder of NGOs working on cyber security among other issues -- is regularly funded by the Dutch government.[44] The State Department has a long list of initiatives and funding for groups promoting democratic principles and human rights.[45] Ökotárs Foundation which dispenses funds from the Norwegian government has been accused by the Fidez government in Hungary of doing the bidding of foreign governments.[46] This along with the crackdown on NGOs in countries like Russia,[47]Egypt[48] or Azerbaijan[49] shows that far from being understood as members of the respective countries' civil societies, these groups are seen as state and corporate actors by unfriendly governments.

Perhaps one of the most interesting cases concerning the usurpation and concealment of corporate and government interests under the cloak of civil association is the case of the sudden ascension of Pierre Omidyar to the parnassus of para-political funding. Having began his philanthropic activities in the late 90s, by early 2014 Omidyar had given out 1 billion dollars to all sorts of organizations and projects. Only in 2013, his organizations gave 225 million dollars. In addition, to personal donations, the funding is done through three organizations: the Omidyar Network Fund, HopeLabs, and Humanity United. Michael Gentilucci from Inside Philanthropy points out that 'We're dealing with an archipelago here, not a solid land mass, and the overarching entity is The Omidyar Group'.[50] The Omidyar group is a not a non-profit organization.

The NGOs funded by Omidyar include Change.org, Center on Democracy, Development, and the Rule of Law, Global Integrity, Fundacion Ciudadano Inteligente, Global Voices, Media Development Investment Fund, The Open Data

Institute, Open Government Partnership, Project on Government Oversight (POGO), Sunlight Foundation, The Transparency and Accountability Initiative, The Foundation for Ecological Security, the Endeavor Foundation and Ashoka.

And then Omidyar, whose American record includes contributions to the presidential campaign of Wesley Clark and co-investment with the CIA's venture capital firm IN-Q-TEL and Booze Allen Hamilton[51] (NSA subcontractor and former employer of Edward Snowden), became the guardian of the Snowden papers. With a pledge of 250 million dollars, Omidyar started in 2013 to build himself a media network under the name First Look Media. His first three hires were Glenn Greenwald, Laura Poitras and Jeremy Scahill. Following the organizational pattern in his philanthropic work, First Look Media spun off in only a few months a second media structure under the name of The Intercept, which was launched in February of 2014. The online publication was devised to publish the unredacted Snowden documents and to 'produce fearless, adversarial journalism across a wide range of issues'.[52]

While the question of the legitimacy of political intervention for foundations and NGOs has been a perennial question in the conversations about non governmental actors and foundations, the peculiarity of the new landscape is that it is precisely the NGOs armed with the financial firepower of political parties that can now take consultative roles under the guise of being the legitimate representatives of civil association. In this way, they render an invaluable service to corporate and government agents interested in circumventing democratic principles of governance and public administration.

Conclusion

The photograph of the smashed servers, which held the NSA papers in The Guardian's basement, seems plainly incompatible with the principles and processes of a democratic state. It rather *resembles* some of the worse elements of mid-20th century mechanisms of control under totalitarian regimes. The destruction of the vessels of information--letters, books, recordings, etc--were critical instruments of control of political meaning. Indeed, it is Edward Snowden himself, who best explained the political scope of his venture and the aim of his conduct and professed ideological enemy:

> On 12 July 2013 Edward Snowden met with a number of human rights organizations at his temporary refuge in Moscow's Sheremetyevo International Airport. Here are a few of the points he made:– Through his working connection to the National Security Agency, Snowden found that he "had the capability without any warrant to search for, seize, and read your communications. Anyone's communications at any time. That is the power to change people's fates."– Snowden also concluded that the daily use of this capacity by the NSA was a "serious violation of the law. The 4th and 5th Amendments to the Constitution of my country, Article 12 of the Universal Declaration of Human Rights, and numerous statutes and treaties forbid such systems of massive, pervasive surveillance."– "My government [U.S.] argues that secret court rulings, which the world is not permitted to see, somehow legitimize an illegal affair. . . .The immoral cannot be made moral through the

> use of secret law.”– Appalled by this situation, Snowden took to heart the 1945 Nuremberg principle that says, “Individuals have international duties which transcend the national obligations of obedience. Therefore individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring.”– Having concluded that the NSA’s real and potential secret access to the communications of almost every American, and a growing number of non-citizens, was criminal in nature (perhaps totalitarianism in the making), he leaked the classified information that would bring the NSA’s activities into public view. “That moral decision to tell the public about spying that affects all of us has been costly, but it was the right thing to do and I have no regrets.”[53]

The mechanisms of surveillance, control and coercion exposed by the Snowden affair point precisely to a machinery which in many ways resembles the mechanisms of totalitarian regimes. The ideological underpinnings that were translated into the *ideal states* in traditional totalitarian regimes seem to be absent in the alliance of trusted networks. Yet, the ideological underpinnings for the preservation of the system’s economic and political health are there and plain to see. They essentially belong to a discourse of centrist consensus, which puts a premium on ideas of civil associations and the fellowship of civility. But the fellowship of civility is not always amicable to the intentions and dispositions of enterprise associations, so it is precisely the role of the industry of civil society, the third and newest trusted network, to take the place of democratic civil actors and certify the doings of the other two groups.

The distinct features of the current alignment of forces and players include a. the monopoly of digital planning on surveillance resting on back-channel and secret communication between government, tech corporate elites and, sometimes, NGOs; b. the role of civil society NGOs as mechanisms for circumventing democratic processes c. enterprise association politics that ensures that the dual goal of state (security) and capital (profit) continues unabated and unaccounted; d. the unprecedented scope in the form of total structural data acquisition by western intelligence matrixes; e. the persecution and prosecution of journalists, whistle-blowers and transparency actors outside the scope of civil society groups and f. the significant if insufficient contestation by members of the public concerning the infringement on civil liberties.

Lastly, the quasi-totalitarian practices of enterprise associations conducted by these global trusted networks and led by the United States, has to be urgently reconsidered and new methods for challenging it, devised. Short of a structural solution to the occupation of the political space in digital environments by the three networks, the individual citizen is left in a condition of political, legal and possibly existential precariousness, in which the only choice is to hack the agglomeration of authoritative networks to assert her own rights and the networks' ethical obligations.

Endnotes

[1] Athina Karatzogianni would like to acknowledge the Liberty Fund conference 'Totalitarianism, Democracy, and Liberty", October 23-26, Krakow, Poland, as a significant intellectual experience for the formulation of ideas developed for this article. Also, to acknowledge the Economic and Social Research Council (ESRC), which funded the project 'The Common Good: Ethics and Rights in Cyber Security' Grant Ref: ES/L013177/1 and the meeting with Martin Gak to co-author this article in November 2013. We also owe thanks to Noel O' Sullivan, Richard Aldrich, Luke O'Sullivan, Andrew Robinson, Jeremy Gilbert and the journal's anonymous reviewers for their extensive feedback.

[2] Borger, J. 'NSA Files: Why The Guardian in London Destroyed Hard Drives of Leaked Files'. The Guardian. Online available at: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london

[3] Moore, Charles. (11 October 2013) 'This is not Blitz Britain. We sure as hell can't lick terrorism on our own'. The Daily Telegraph. Online available at: http://www.telegraph.co.uk/news/uknews/defence/11154322/GCHQ-This-is-not-Blitz-Britain.-We-sure-as-hell-cant-lick-terrorism-on-our-own.html

[4] Associated Press-NORC Center for Public Affairs Research. 'Balancing Act: The public's take on Civil Liberties and Security A Trend Study'. (2013) Online available at: http://www.apnorc.org/PDFs/Balancing%20Act/AP-NORC%202013_Civil%20Liberties%20Poll_Topline_Trend.pdf Since the NSA revelations, Americans have become more opposed to government surveillance that infringes on civil liberties.

[5] Karatzogianni, A. and Robinson, A. (2010) Power, Conflict and Resistance: Social Movements, Networks and Hierarchies, London and New York: Routledge.

[6] The original text had the word 'economic' where here we replaced with the word 'digital' to enforce the point. The original text is from Hayeck, Friedrich A. The Collected Works of F.A. Hayek, Volume II: The Road to Serfdom –Text and Documents –The Definitive Edition. Ed. Bruce Caldwell. Chicago: The University of Chicago Press, 2007, p. 127.

[7] Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (Cambridge: Polity Press, 2012); Christian Fuchs, *Foundation of Critical Media and Information Studies* (London and New York: Routledge, 2011); David Harvey, *Rebel Cities: From the Right to the City to the Urban Revolution* (New York: Verso, 2012); Geert Lovink, *Networks Without a Cause: A Critique of Social Media* (Cambridge: Polity Press, 2012); Evgeny Morozov, *The Net Delusion: How Not to Liberate the World* (London: Allen Lane, 2003); Clay Shirky, 'The Political Power of Social Media', *Foreign Affairs* 90, no. 1 (2011): 28-41.

[8] Wacquant, L. (2008) Urban Outcasts: A Comparative Sociology of Advanced Marginality, Cambridge: Polity quoted in McCahill, M. and R. L. Finn (2014), *Surveillance, Capital and Resistance: Theorizing the Surveillance Subject*, London: Routledge.

[9]Ibid., p.9.

[10] McCahill, M. and R. L. Finn (2014), *Surveillance, Capital and Resistance: Theorizing the Surveillance Subject*, London: Routledge.

[11] McCahill and Finn, p. 4.

[12] Ibid., p.80

[13] See for instance: Karatzogianni, A. (2006) *The Politics od Cyberconflict*, London and New York: Routledge; Karatzogianni, A. (ed.) *Cyber Conflict and Global Politics*, London and New York: Routledge; Karatzogianni, A. and Kunstman, A. (eds.) (2012) *Digital Cultures and the Politics of Emotion*, Basingstoke: Palgrave.

[14] Talmon, J.L. (1961) *The Origins of Totalitarian Democracy*, London: Mercury Books; Arendt, H. (1951) *The Origins of Totalitarianism*, New York: Harcourt, Brace and Co, 333-370; Friedrich, C. and Brzezinski, A.K. (1956) *Totalitarian Dictatorship and Autocracy*, Cambridge: Harvard University Press; Siegel, A. (ed) (1998) *The Totalitarian Paradigm after the End of Communism*. Amsterdam: Radopi. pp. 9-35; Rupnik, J. (1988) 'Totalitarianism Revisited' in *Civil Society and the State*, ed John Keane, pp. 263-290; *Zizek, S. Did Somebody say Totalitarianism?*, London: Verso, pp. 4-7.

[15] Schmitt, C. *The Concept of the Political*, p. 22.

[16] ibid., p.24.

[17] By motus we mean the motor that moves a system.

[18] See for instance, Gabriel's *Public-Private Relations in the Totalitarian State* and, of course, Hannah Arendt's *The Origins of Totalitarianism* and Foucault's *Discipline and Punish.*

[19] Popper, K. (1971) *Open Society and its Enemies*, Princeton University Press, p. 157.

[20] Arendt, H. (1951) *The Origins of Totalitaritarianism*, New York: Harcourt, Brace and Co., pp.341-363.

[21] Deleuze, G. and Guatarri, F. (1983) *Anti-Oedipus*, London: Athlone. See also Karatzogianni, A. and Robinson, A. (2013) 'Schizorevolutions vs. Microfascisms: A Deleuzo-Nietzschean Perspective on State, Security, and Active/Reactive Networks' Available at: http://works.bepress.com/athina_karatzogianni/19

[22] For an extensive analysis, see Yar, M. (2014) *The Cultural Imaginary of the Internet: Virtual Utopias and Dystopias*, Palgrave.

[23] This is a reference to Arendt's Eichmann in Jerusalem. While her concern is with the mechanisms that underpin great acts of political perversity, it may be useful to extend the indictment against lack of reflective reckoning to digital behavior. Not only to account for the evil that may be produced but to account for the way in which these acts of political happy oblivion can be exploited by the planners and the trusted networks.

[24] Aristotle, Politics. Book I.

[25] Oakeshott, M. *On Human Conduct,* p. 110.

[26] Hopkins, N. and Taylor, M. (6 October 2013) 'Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne'. Online available at: http://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne

[27] Ibid., p. 310.

[28] O'Sullivan, N. 'Oakeshott on Civil Association' in P. Franco and L.Marsh (eds) *A Companion to Michael Oakeshot*t, University Park: Pennsylvania State University Press, p. 306. Our italics.

[29] ibid., p. 296.

[30] http://revolution-news.com/anonymous-releases-private-nsa-documents/

[31] The Guardian (1 November 2013) 'NSA Files Decoded: What the revelations mean for you'. Online available at: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

[32] RT. (11 July 2013) 'Microsoft Helped the NSA Bypass Encryption, New Snowden Leak Reveals'. Online available at: http://rt.com/usa/microsoft-nsa-snowden-leak-971/

[33] Huet, N. (11 July 2013) 'French Lawsuit Targets NSA, FBI, Tech Firms Over Prism'. Reuters. Online available at: http://www.reuters.com/article/2013/07/11/us-usa-security-france-idUSBRE96A0OF20130711

[34] http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609-3.html

[35] Rushe, D. (12 September 2013) 'Zuckerberg: US Government "Blew It" On NSA Surveillance'. Online available at: http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

[36] This is an extract from reports about a Google executive collaborating with US Intelligence contractor Stratfor: 'Documents published last year by WikiLeaks obtained from the US intelligence contractor Stratfor, show that in 2011 Jared Cohen, then (as he is now) Director of Google Ideas, was off running secret missions to the edge of Iran in Azerbaijan. In these internal emails, Fred Burton, Stratfor's Vice President for Intelligence and a former senior State Department official, describes Google as follows: "Google is getting WH [White House] and State Dept support and air cover. In reality they are doing things the CIA cannot do…[Cohen] is going to get himself kidnapped or killed. Might be the best thing to happen to expose Google's covert role in foaming up-risings, to be blunt. The US Gov't can then disavow knowledge and Google is left holding the shit-bag". In further internal communication, Burton subsequently clarifies his sources on Cohen's activities as Marty Lev, Google's director of security and safety and..Eric Schmidt. WikiLeaks cables also reveal that previously Cohen, when working for the State Department, was in Afghanistan trying to convince the four major Afghan mobile phone companies to move their antennas onto US military bases. In Lebanon he covertly worked to

establish, on behalf of the State Department, an anti-Hezbollah Shia think tank. And in London? He was offering Bollywood film executives funds to insert anti-extremist content into Bollywood films and promising to connect them to related networks in Hollywood. That is the Director of Google Ideas. Cohen is effectively Google's director of regime change. He is the State Department channeling Silicon Valley. Google was right in saying it doesn't have a backdoor for government; its front door is wide open.'

[37] Bigo, Didier et al. (06 November 2013) 'Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law' (CEPS). Available at: http://www.ceps.eu/book/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law (pg 17)

[38] http://www.reuters.com/article/2013/06/30/us-usa-germany-spying-idUSBRE95T04B20130630

[39] Schow, A. (1 July 2013) 'US Government Declares Hacking An Act of War, Then Hacks Allies'. Washington Examiner. Online available at: http://washingtonexaminer.com/article/2532594

[40] Augstein, J. (16 July 2013) 'The Chancellor and the NSA: Merkel Has Abandoned the Germans'. Spiegel. Online available at: http://www.spiegel.de/international/germany/editorial-merkel-has-left-germans-high-and-dry-a-911425.html#spLeserKommentare

[41] Poitras, L., Rosenbach, M. Schmid, F., Stark, H. and Stock, J. (1 July 2013) 'Cover Story: How the NSA Targets Germany and Europe'. Spiegel. Online available at: http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html

[42] Greenwald, G. (15 July 2013) 'The Crux of the NSA Story in One Phrase: "Collect It All'. The Guardian. Online available at: http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all

[43] Friedersdorf, C. (12 August 2013) 'The Surveillance Speech: A Low Point in Barack Obama's Presidency'. Online available at: http://www.theatlantic.com/politics/archive/2013/08/the-surveillance-speech-a-low-point-in-barack-obamas-presidency/278565/

[44] Hivos institutional profile: https://www.ihrfg.org/funder-directory/hivos

[45] Examples of State Department's Funding in Security, Democracy and Human Rights : http://www.state.gov/j/prm/funding/

[46] Balogh, E. (23 October 2014) 'The Hungarian Government Turns Up The Heat On The NGOs' Available online at: https://hungarianspectrum.wordpress.com/2014/10/23/the-hungarian-government-turns-up-the-heat-on-the-ngos/

[47] The Crackdown On NGOs In Russia (1 December 2014) Online at Radio Free Eueopr. Available at: http://www.rferl.org/section/crackdown-on-ngos-in-russia/3272.html

[48] (22 September 2014) “Egypt NGOs 'robbed of independence' Online available at: http://www.aljazeera.com/news/middleeast/2014/09/egypt-ngo-law-crackdown-2014913121624569527.html

[49] Farchy, J. (22 September 2014) “Concern Grows over NGO crackdown in Azerbaijan” Online available at: http://www.ft.com/intl/cms/s/0/aec6a9b2-4247-11e4-a9f4-00144feabdc0.html#axzz3KZgToDG9

[50] Gentilucci, M. (27 March 2014) “Can't Get a Grip on Omidyar Philanthropy? You're Not Alone, So Take This Guided Tour” Online available at: http://www.insidephilanthropy.com/tech-philanthropy/2014/3/27/cant-get-a-grip-on-omidyar-philanthropy-youre-not-alone-so-t.html

[51] List of InnoCentive strategic partners. http://www.innocentive.com/about-innocentive/our-innovation-partners

[52] Rice, a. (October 2014) ‘The Pierre Omidyar Insurgency’. Online available at: http://nymag.com/daily/intelligencer/2014/10/pierre-omidyar-first-look-media.html

[53] Davidson, L. (16 July 2016) ‘A National Debate About Government Spying?’ NYTexaminer.com. Online available at: http://www.nytexaminer.com/2013/07/a-national-debate-about-government-spying