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

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 explore the politics, ethics, values and affects mobilised by governments and corporate elites to justify the collect-it-all practices of the three ‘trusted’ global networks that dominate this field - corporations, governments and co-opted civil society groups. It charts this political space as a sphere of action emerging against the backdrop of what we call ‘quasi-totalitarian’ mechanisms that are fostered by the alignment, collusion and imbrication of these networks. This approach illuminates a particular problem in the articulation of digital politics: the process of political disenfranchisement brought about by corporations looking to profit, governments looking to regulate information flows, and co-opted 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: the monopoly of digital planning on surveillance that rests on back-channel and secret communication between government, tech corporate elites and, sometimes, NGOs; the use of civil society NGOs as mechanisms for circumventing democratic processes; ‘enterprise association’ politics, aimed at ensuring that the dual goal of state (security) and capital (profit) continues unabated and with little unaccountability; the unprecedented scope offered by total structural data acquisition on the part of western intelligence matrixes; the persecution and prosecution of journalists, whistle-blowers and transparency actors outside the scope of civil society groups; and 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

Introduction

Who has the info on you? It’s the commercial companies, not us, who know everything - a massive sharing of data

Sir Iain Lobban, Former Director of GCHQ, UK
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. But though the public has been slow to react, the political fallout has had to be addressed. Governments and tech elites have thus each accused the other of being responsible for the public loss of trust, and of compromising privacy and the integrity of networks.

A key area of concern following the Snowden revelations have been the programmes of the National Security Agency (NSA) - which is an intelligence agency that is part of the Department of Defence. These had in fact been already running for seven years without public oversight or debate at the time of the revelations. The Obama administration justified its actions by claiming that they had been crucial in successfully thwarting terrorist attacks (such claims have been contested). But all this has made little difference to the continued deployment of these programmes. In the trade-off between privacy and security, governments have argued the need for exceptions from the legal framework, in order to protect the public. Meanwhile, tech elites expressed exasperation at what has happened, while remaining fairly opaque about their practices in relation to privacy and security. In order to guarantee their own income flows, as well as their reputation as socially responsibly corporate actors, technocapitalists have struck a pose that has not been entirely consistent with their practices. The third group that has come to take a prominent role in the debate - civil society organisations (some of dubious ancestry) - has advocated transparency and open access-enabled deliberation, as well oversight of the processes involved, claiming for themselves a role as the voice of the public. Their involvement has issued all manners of crusades in defence of putative democratic principles and constitutional guarantees.

This ménage à trois of ‘trusted’ global networks - governments, corporations and NGOs - are holding a de facto mandate, and effective planning power, in the digital field. They clothe themselves in a bastardised version of publicness, and in this guise usurp the political agency of individual members of society. In fact, these three supposedly trusted networks constitute an oligopoly that dominates the space in which governance is negotiated. They relegate the individual to a place of marginality, from where they are only able to address the threat of surveilling agents to their privacy from a position of acute precariousness. It is the individual has to pay for digital equipment, access, and their own necessary digital literacy, thereby funding the processes of

2. Associated Press-NORC Center for Public Affairs Research, ‘Balancing Act: The public’s take on Civil Liberties and Security A Trend Study’, 2013: http://www.apnorc.org/PDFs/Balancing%20Act/AP-NORC%202013_Civil%20Liberties%20Poll_Topline_Trend.pdf.

The remains of a computer that held files leaked by Edward Snowden to the Guardian, which was destroyed at the behest of the UK government

Photograph: Roger Tooth
purchase, connectivity and training; and it is also the individual who has to acquire the necessary skills and software to protect their privacy in the digital homes that are 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 the precarious state of rights in the face of these developments that is the inspiration and rationale for this article.

This article seeks to chart this political space as a sphere of action emerging against the backdrop of what we call the ‘quasi-totalitarian’ mechanisms that are fostered by the alignment, collusion and imbrication of the three networks. This approach explores a particular problem in the articulation of digital politics: the process of political disenfranchisement by corporations looking to profit, governments looking to regulate information flows, and co-opted groups in civil society looking to appropriate the legitimate concerns of users for their own political and financial subsistence. The re-articulation of the current political landscape of the digital sphere in terms of such dynamics should also help to show that there is a need to respond to these techno-social transformations of agency by promoting a civil type of association, inspired by radical democratic politics that is capable of contesting the practices of these three trusted networks.

ADrift AMID DIGITAL FIEFS

The three networks (corporate, government, civil society NGOs) 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; but they have structural and formal similarities in the form of a hierarchical, social and political economic logic based on reactive desire. Their emergent characteristics are symptomatic of a dynamic of hierarchical power that can be found in all of them, though with features peculiar to the nature of each network.

Should this oligopoly of semi-centralised surveillance succeed in asserting control, only communications with intentions plainly visible to the networks would be recognised as legitimate. For the securitising 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 it amounts to the political capitalisation of the rights and obligations of the
individual in relation to digital engagement, in the face of the other two networks.

To demonstrate this point, let us draw an analogy with Hayek’s argument on economic control and totalitarianism. In the seventh 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.4

As in economic matters so 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 - is the crucial mechanism 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 US-led transnational authority comprised of global trusted networks that presently direct 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 nature of this oligopoly of surveillance, the power over information and communication that this authority can exert is nothing less than control over both digital consumption and production. Similar mechanics of digital control can be found elsewhere, in China and Iran for example, so this is something that occurs at a global scale.5

It is not just the power and reach of this oligopoly of digital planners that is of interest: so too are the specific types of ideological positions and logics of political and commercial necessity that are 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 programmes of surveillance, as well as in the relentless governmental

4. We have replaced the original text’s ‘economic’ with the word ‘digital’ to enforce the point. Friedrich Hayek, ed. Bruce Caldwell, The Collected Works of F.A. Hayek, Volume II: The Road to Serfdom - Text and Documents - The Definitive Edition, The University of Chicago Press, Chicago 2007, p.127.

5. Manuel Castells, Networks of Outrage and Hope: Social Movements in the Internet Age, Polity Press, Cambridge 2012; Christian Fuchs, Foundation of Critical Media and Information Studies, Routledge, London and New York 2011; David Harvey, Rebel Cities: From the Right to the City to the Urban Revolution, Verso, New York 2012; Geert Lovink, Networks Without a Cause: A Critique of Social Media, Polity, Cambridge 2012; Evgeny Morozov, The Net Delusion: How Not to Liberate the World, Allen Lane, London 2003; Clay Shirky, ‘The Political Power of Social Media’, Foreign Affairs 90, No 1 2011: 28-41.
crackdowns on movements in favour 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 argument concerning the ‘desolidarising’ impacts of ‘synoptic’ surveillance and ‘lateral’ surveillance. But McCahill and Finn argue that some of the people they interviewed - who can be regarded as being among the targeted individuals and groups in surveillant assemblages referred to in Urban Outcasts (p9), such as migrants, protesters, school children and individuals under probation - despite facing the relentless challenges imposed by surveillance, are able to develop surveillance capital:

... 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’ ([p80]).

Nevertheless, in the aftermath of the Snowden affair, Wacquant’s desolidarisation is politically evident across the board, though ‘surveillance capital’ strategies are sure to be developed among the general population. This is because the exercise of surveilling power is no longer 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 lofty conceptualisations of digital utopias and dystopias, the old modernist demands for power, participation and democracy still hold currency; and race, gender, class and other mechanisms of hierarchy are all produced and reproduced in digital networks. The alignment of technology corporations, government elites and civil society agents, and the passive acquiescence of the public, together amount to a collective propensity that resembles totalitarianism. This political ethos is built upon a tacit consensus, and the covert prescription of individual and collective transparency. It is therefore a critical part of any account of the traditional ideological and political categories that are 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.9

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, first coined by Carl Schmitt in 1927 in The Concept of the Political, refers to a state which, in 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.10 The interpenetration of state and society - the hyper-politicisation 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’ (p24).

The mutual permeability of the political and the social means that in totalitarianism the motus politicus (the motor that drives the political system) tends to become - though never fully is - 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, which in all forms of totalitarianism is submitted to political and collective scrutiny.11

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 on the part of organisations or individuals, forecasting market practices, or modifying socio-cultural practices by changing underpinning attitudes, governments, corporations and civil society actors collude in explicit and implicit normalisation 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 characterised by instrumental practices oriented to the attainment of what he calls the Ideal State.12 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 realisation of an ultimate political goodness. Ultimately, for Popper, totalitarianism is intimately related to politics understood as the search for salvation.

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 of 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). To win over the masses, the totalitarian agent deploys mechanisms of inculcation. Propaganda is central to the construction of the political imaginary of the public. Mechanisms of inculcation are central to totalitarian states and must be

9. J.L. Talmont, The Origins of Totalitarian Democracy, Mercury Books, London 1961; H. Arendt, The Origins of Totalitarianism, Harcourt, Brace and Co, 1951, 333-370; C. Friedrich and A.K Brzezinski, Totalitarian Dictatorship and Autocracy, Harvard University Press, Cambridge 1956; A. Siegel (ed), The Totalitarian Paradigm after the End of Communism, Radopi, Amsterdam 1998, pp9-35; J. Rupnik, ‘Totalitarianism Revisited’, in John Keane (ed), Civil Society and the State, 1988, pp263-290; S. Zizek, Did Somebody say Totalitarianism?, Verso, London 2002, pp4-7.

10. C. Schmitt, The Concept of the Political [1927], University of Chicago Press, 1995, p22.

11. 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.

12. K. Popper, The Open Society and its Enemies, Princeton University Press 1971, p157.
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 a commitment to faith in the ‘ideal state’. Finally, then, surveillance of communicative acts is not merely a way to probe, predict and prevent certain actions; it is also, insofar as it assesses the content of thought and sentiments, a way to test the efficiency of propaganda. Friedrich and Brzezinski’s 1956 definition of totalitarianism has the following salient elements: an ideology of the potentially 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. For Deleuze and Guattari, this is the state machine, which captures social flows and assemblages, decomposing their horizontal connections along the way.\textsuperscript{13}

The consensus of our three trusted networks, with the tacit acquiescence of the individual user, shares 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 centre of a polity. In fact, the tacit consensus is undergirded by the fusion of the \textit{motus politicus} with the \textit{motus socialis}. Whereas the totalitarians of the mid-twentieth century saw this kind of coalescence in ideas of national purity and ethno-cultural exclusivity - it was these that formed the basis on which they built their ‘ideal state’ - neoliberals and social democrats alike are the current designers of the accounts of the ‘ideal state’ that now permeate every aspect of the social fabric. Since the mid-twentieth century, even in the most despotic states, the ideological construction of the ‘ideal state’ has corresponded to variations of these two socio-political imaginaries. This has produced a strange new political animal that seems to be a progressive neoliberal version of totalitarianism: a quasi-totalitarianism.

**QUASI-TOTALITARIANISM AND THE OPPRESSION OF TACIT CONSENT**

The centres of digital planning, and of surveillance networks, are steeped in an ideology which has markedly totalitarian features, but this ideology is not instantly recognisable as being connected to the historical events, regimes and political practices that during the twentieth century were built on the total politicisation of everyday life.

There are two important differences between quasi-totalitarianism and its predecessors. Quasi-totalitarianism is not in the same way dependent on an account of an ‘ideal state’, although justifications for the policy measures that have been devised and deployed in relation to the networks can be understood as instrumental to a putative critical end: security, growth or better socio-cultural habits. A caveat is in order here, however: it is to a large degree only the civil society part of the \textit{menage} that systematically appeals

\textsuperscript{13} G. Deleuze and F. Guattari, \textit{Anti-Oedipus}, Athlone, London 1983. See also A. Karatzogianni and A. Robinson, ‘Schizorevolutions vs. Microfasmas: A Deleuzo-Nietzschean Perspective on State, Security, and Active/ Reactive Networks’, 2013: http://works.bepress.com/athina_karatzogianni/19.
to an ideal state discourse to promote its own agendas. There are not many users in the digital sphere who earnestly take a Manichean approach to life. It is, rather, agents of the public sector who insist on depicting digital space as either a utopian dream or a dystopian nightmare.\textsuperscript{14}

The second way in which quasi-totalitarianism differs from its ancestor concerns the overseeing of the construction of ideological consensus. With the exception of the civil society groups, 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 have already brought them to commercial dominance, while government agencies operating in the shadows need no assent from the mass. It is, rather, the strategy of political consensus of the totalised centre that scaffolds the planning schemes of the networks.

It is the emergence of a centre consensus among civil actors that seems to dictate the ideological constitution of power, rather than the other way around. In this sense, quasi-totalitarianism recruits and deploys some of the mechanisms inherent in the 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 here is the banal enforcement of the policies that help to propagate the socio-political consensus of the centre. 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 – together make up the agglomeration of actions that individuals perform unreflectively to sustain the status quo and its mechanisms of socio-political cohesion.\textsuperscript{15} And the preservation and promotion of the status quo is also the preservation and promotion of the centre. In digital practices, this ideological hybrid is peddled by the large-scale collective centre in the form of the centralised networks, each of which negotiates its respective need to surveil, profit from and - perhaps curiously - act on behalf of, the putative freedom of users.

\textbf{FORMS OF ASSOCIATION IN QUASI-TOTALITARIANISM}

The difference ideological roles played by the ideal state in the totalitarian model and the quasi-totalitarian model may be best explained by Michael Oakeshott’s two accounts of political enterprises in \textit{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.\textsuperscript{16} In contrast to an enterprise association, which gathers together in order 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

\begin{flushright}
14. For an extensive analysis, see M. Yar, \textit{The Cultural Imaginary of the Internet: Virtual Utopias and Dystopias}, Palgrave 2014.

15. This is a reference to Arendt’s \textit{Eichmann in Jerusalem}. It may be useful to extend her indictment of a lack of reflective reckoning to digital behaviour, to account not only for the evil that may be produced but also for the way in which these acts of happy political oblivion can be exploited by the planners and the trusted networks.

16. Aristotle, \textit{Politics}, Book I.
\end{flushright}
Each of the three networks we have been discussing 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 (εκονομος), 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 intent on preserving and promoting. It is the integrative idea of the centre that fulfils 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 centre 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 centre’s consensus. The networks justify the supposedly intermittent violation of privacy, free association and freedom of expression by asserting the instrumental need for structural data acquisition, surveillance and digital network infringement, as well as 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 behaviour 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 rather vast catalogue of legal violations that have flooded the public sphere as a result of the Snowden leaks shows that the legal principles on which democratic life is built have indeed 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 trivialising the historical experiences of totalitarianism.

Moreover, on another level, the quasi-totalitarianism of the centre points to the ‘centre’ of the ideological spectrum. Traditionally, in democratic systems the centre has been occupied by liberals and social democrats of some description or another. Nevertheless, the ideological centre in non-democratic states is equally the ideological centre in the specific spectrum of the political

---

17. M. Oakeshott, *On Human Conduct*, p110: http://doi.org/7fc.
culture in any given country-specific context. The quasi-totalitarianism of the centre refers here to a second layer in relation to centralised hierarchical organisations, even if they are networked: the socio-political logic remains hierarchical despite the use of network communications. The centres 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 centre find it preposterous when it is suggested 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 centre of the political system. In this sense, surveillance complexes are the direct genealogical offspring of, and mirror the political ideology dominant in, any given political system.

However, the paradox in the present case scenario is that neither neoliberalism nor 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 the exasperation of Chris Huhne, UK Secretary of State for Energy and Climate Change from 2010 to 2012, in the face of lack of information about GCHQ activities?: ‘Cabinet was told nothing about this’.18 This form of quasi-totalitarianism relies on an enterprise association to flourish - rather than a civil association, which was until recently the most common ideal type of association in traditional representative politics. 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, has no corporate aggregate purpose, except to keep politics open and the discussion going, and can serve both as a response to the critique we have outlined and as a powerful new vision for the network res publica; but it is presently dominated by human conduct primarily geared toward forms of enterprise association.

The conflict is succinctly explained by Noel O’Sullivan, who points to ‘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’.19 It is important to underscore the fact that the principle of civility that is entailed in the political assertions and propositions of the centre is often, if not regularly, co-opted by enterprise associations who present their own aims as instrumental necessities for the preservation of the civil associations. So, in a sense, the task at hand for the radicalisation of a democratic model is to foreclose on the usurpation of civil associations by enterprise associations: to resist the articulation of the fellowship of civility as an endangered model whose safeguarding is represented as an ideal state. The fellowship of civility is not a state of attainment, in contrast to, say, the holding of a profit or the end of conflict. It is, rather, a form of a political performance, and it cannot therefore

18. N. Hopkins and M. Taylor, ‘Cabinet was told nothing about GCHQ spying programmes, say Chris Huhne’, Guardian, 6.10.13.

19. Ibid, p310.
be captured in an ideal state without negating its non-instrumental nature.

Indeed, as Noel O’Sullivan has pointed out, a charitable reading of Oakeshott’s accounts of civility in the face of the instrumentalisation of the political may be well-suited to the re-articulation 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.20

Significantly, the danger of not recognising 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 recognised: 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 (p296).

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 response by the group Anonymous 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%.21

In its communiqués, Anonymous often portrays itself as a bearer of the values of civil association, as protector of the fellowship of civility. Understandably, the articulation of this un-trusted network’s commitment is advanced in moral

20. N. O’Sullivan, ‘Oakeshott on Civil Association’, in P. Franco and L. Marsh (eds), A Companion to Michael Oakeshott, Pennsylvania State University Press, University Park, p306. Our italics. http://doi.org/7fc.

21. http://revolution-news.com/anonymous-releases-private-nsa-documents/.
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 reveal the totalitarian mechanisms which they each claim to resist.

According to one of the main media organisations with which Snowden collaborated, the Guardian, the NSA’s Prism programme is the biggest single contributor to the intelligence reports that were leaked. Prism was a ‘downstream’ programme: i.e. 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.22 (The documents also exposed the existence of Tempora, a programme established in 2011 by the UK’s GCHQ. This programme gathers en-masse data from phone and internet traffic by tapping into fibre optic cables. GCHQ shared most of its information with the NSA.) The relationship between the NSA and the tech giants is indeed a complicated one. According to the Guardian, in June and July 2010 data from Yahoo generated by far the largest number of NSA intelligence reports. Microsoft were in second place, followed by Google. The NSA is allowed to travel ‘three hops’ from its targets - i.e. this can mean 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 (approximately 5,260,000 people).

According to internal documents cited by journalists, Microsoft ‘developed a surveillance capability’ that was launched ‘to deal’ with the concern of the federal authorities that they would 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’.23 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.

Two French human rights groups have filed a legal complaint targeting the NSA, the FBI and seven technology companies that, they say, may have helped the United States snoop on French citizens’ emails and phone calls. The complaint denounced US spying methods as revealed by Snowden, and was filed against ‘persons unknown’, but named 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

---

22. ‘NSA Files Decoded: What the revelations mean for you’, Guardian, 1.11.13.

23. ‘Microsoft Helped the NSA Bypass Encryption, New Snowden Leak Reveals’, RT, 11.7.13: http://rt.com/usa/microsoft-nsa-snowden-leak-971/.
individuals’ lives represents a serious threat to individual liberties and, if not stopped, may lead to the end of the rule of law’. Reports have also referred to ‘alliances with over 80 major global corporations supporting both missions’ (the two ‘missions’ being defending networks in the US, and monitoring networks abroad). The companies involved include ‘telecommunications firms, producers of network infrastructure, software companies and security firms’.25

Both Mark Zuckerberg (CEO of Facebook) and Marissa Mayer (CEO of Yahoo) defended their respective companies against the criticism that tech companies were doing too little to fight off NSA surveillance. According to Mayer, executives would face jail if they revealed government secrets. Indeed, 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 commented: ‘When you lose and you don’t comply, it’s treason. We think it makes more sense to work within the system’; meanwhile Zuckerberg’s view that the government had done a bad job of balancing people’s privacy and its duty to protect was apparent in the now famous statement: ‘Frankly I think the government blew it’.26

The escalation of tensions between corporations and government - whether or not it is earnest, or merely something fabricated for public consumption - points to decision-making processes that clearly sit beyond governance by democratic methods and principles. They appear to involve back-channel negotiations between state and corporate elites carried out 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.27 That too would be treason, as Mayer 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, have launched lawsuits that have led to the disclosure of hundreds of pages of FISA Section 215 subpoenas, which since 1988 have given the government the authority - with the courts previous approval - to obtain records in the course of foreign intelligence investigations. And 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 an open letter to the Senate demanding reform. In fact the review by the Obama administration was conducted as a response, but it 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 vary from country to country. Referring to a *Guardian* article from August 2013, 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.28

Governments are not allowed to spy on their own populations but they can spy on foreign nationals. The US views countries such as Germany and France as third parties, which it is therefore acceptable to spy upon - most notoriously in the case of 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 ... In France ... the United States taps about 2 million connection data a day. Only Canada, Australia, Britain and New Zealand were explicitly exempted from spy attacks.29

And yet the reaction in European capitals has been underwhelming. French President Francois Hollande did make a statement condemning the practice, arguing that the hacking was not necessary for anti-terrorism efforts. ‘I do not think that it is in our embassies or in the EU that these risks exist’.30 But Angela Merkel barely seemed to protest at the revelations. A *Der Spiegel* article carried the headline ‘The Chancellor and the NSA: Merkel has abandoned the Germans’.31

In addition to the exploitation of legal loopholes by supranational intelligence agencies, this surveillance-matrix fiefdom also appears to have functioned through an economy of favour swapping 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.32

To a large degree, the surveillance that is led by the American government and carried out through this transnational intelligence fiefdom is based on a logic of war intelligence. It stands to reason, then, that the central body deploying the strategy of surveillance - the NSA - is a military signal intelligence unit. Both the system and the actors who carried out the NSA programme were, unsurprisingly, operational inheritances of the Iraq war. Greenwald, one of the journalists who brought the Snowden story to public attention, discusses

28. Didier Bigo et al, ‘Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law’, CEPS, 06.11.13, p17: www.ceps.eu/book/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law.

29. Reported in www.reuters.com/article/2013/06/30/us-usa-germany-spying-idUSBRE95T04B20130630.

30. A. Schow, ‘US Government Declares Hacking An Act of War, Then Hacks Allies’, Washington Examiner, 1.7.13: http://washingtonexaminer.com/article/2532594.

31. J. Augstein, ‘The Chancellor and the NSA: Merkel Has Abandoned the Germans’, *Der Spiegel*, 16.7.13: http://www.spiegel.de/international/germany/editorial-merkel-has-left-germans-high-and-dry-a-911425.html#spLeserKommentare.

32. L. Poitras, M. Rosenbach, F. Schmid, H. Stark and J. Stock, ‘Cover Story: How the NSA Targets Germany and Europe’, *Spiegel*, 1.7.13: http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html.
here a profile in the Washington Post of the former Director of the NSA, General Keith B. Alexander:

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.33

Bowing to pressure from civil society actors who could smell blood and were preparing for a political feeding frenzy, as well as from corporations intent on rescuing their reputations and the loyalty of their publics, Obama issued one of the most notable statements of unrepentant repentance in political history:

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.34

All the evidence is to the contrary. The military signal intelligence programmes 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 programmes simply showed that the US jurisprudential structure was full of loopholes and subterfuges, many of them arising from the state of exception that had been justified by the ‘war on terror’, which had given legal cover to policing practices that had previously been entirely unacceptable, such as torture, disappearance and secret incarceration. These were now being deployed to justify the largest system of violation of privacy the world had ever seen.

THE THIRD NETWORK: NGOS

Civil society actors have been among the beneficiaries of this debacle; as happened in the aftermath of the catastrophic earthquake that destroyed Haiti, these organisations were now perfectly positioned to take advantage of the momentous occasion. Donning the guise of civil society actors, organisations that were in the main associated with a semi-covert network of

33. G. Greenwald, ‘The Crux of the NSA Story in One Phrase: “Collect It All”, Guardian, 15.7.13: http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all.

34. C. Friedersdorf, ‘The Surveillance Speech: A Low Point in Barack Obama’s Presidency’, 12.8.13: http://www.theatlantic.com/politics/archive/2013/08/the-surveillance-speech-a-low-point-in-barack-obamas-presidency/278565/.

35. Hivos institutional profile: https://www.ihrfg.org/funder-directory/hivos.

36. Examples of State Department’s Funding in Security, Democracy and Human Rights: http://www.state.gov/j/prm/funding/.

37. E. Balogh, ‘The Hungarian Government Turns Up The Heat On The NGOs’, 23.10.14: https://hungarianspectrum.wordpress.
American and European foundations that dispense money from 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 organisational support of the other two networks discussed in this article.

For instance, Hivos - a funder of NGOs working on cyber security among other issues - is regularly funded by the Dutch government.\(^3^5\) The US State Department, too, has a long list of initiatives and funding for groups promoting democratic principles and human rights.\(^3^6\) The Ökotárs Foundation, which dispenses funds from the Norwegian government, has been accused by the Fidez government in Hungary of acting at the bidding of foreign governments.\(^3^7\) This, along with the crackdown on NGOs in countries like Russia, Egypt and Azerbaijan, shows that, far from being understood as members of their respective countries' civil societies, these groups are seen as state and corporate actors connected to unfriendly governments.\(^3^8\)

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 ascent of eBay founder Pierre Omidyar to the highest levels of para-political funding. Having begun his philanthropic activities in the late 1990s, by early 2014 Omidyar had given out $1 billion to all sorts of organisations and projects. In 2013 alone, his organisations gave out grants of $225 million. As well as personal donations, its funding is organised through three organisations: the Omidyar Network Fund, HopeLabs and Humanity United. Michael Gentilucci of Inside Philanthropy has argued that: ‘We’re dealing with an archipelago here, not a solid land mass, and the overarching entity is The Omidyar Group’.\(^3^9\) 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. Omidyar’s American record includes contributions to the presidential campaign of Wesley Clark, and he is a co-investor with the CIA’s venture capital firm IN-Q-TEL and Booze Allen Hamilton (a NSA subcontractor and former employer of Edward Snowden).\(^4^0\)

This was the man who eventually became the guardian of the Snowden papers. In 2013, with a pledge of $250 million dollars, Omidyar had started a media network under the name First Look Media. His first three hires were Glenn Greenwald, Laura Poitras and Jeremy Scahill. In February 2014 First Look Media spun off a second media structure under the name of The Intercept. This online publication was devised in order to publish the unredacted Snowden documents and to ‘produce fearless, adversarial journalism across a wide range of issues’.\(^4^1\)

The issue of the legitimacy of political intervention by foundations and
NGOs is a longstanding one, but the peculiarity of the new landscape is that NGOs, armed with the financial firepower of political parties, are now able to take on consultative roles under the guise of being the legitimate representatives of civil society. In this way, they render an invaluable service to corporate and government agents interested in circumventing democratic principles of governance and public administration.

CONCLUSION

Images of smashed servers in the Guardian’s basement plainly seem incompatible with the principles and processes of a democratic state. They rather resemble some of the worse elements of mid-twentieth century mechanisms of control under totalitarian regimes, in which the destruction of vessels of information - letters, books, recordings, etc - was a critical instrument 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, when he met with a number of human rights organisations at his temporary refuge in Moscow’s Sheremetyevo International Airport on 12 July 2013.

Through his working connection to the NSA, Snowden had 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’.

He believed that the daily use of this capacity by the NSA was a ‘serious violation of the law’: ‘My government argues that secret court rulings, which the world is not permitted to see, somehow legitimise an illegal affair … The immoral cannot be made moral through the use of secret law’. He affirmed the 1945 Nuremberg principle that individuals have international duties that transcend the national obligations of obedience and therefore the duty to violate domestic laws to prevent crimes against peace and humanity from occurring. Having concluded that the NSA’s monitoring activities were criminal in nature, he had therefore leaked the classified information that would bring its 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.’

The mechanisms of surveillance, control and coercion exposed by the Snowden affair point to a machinery which in many ways resembles the mechanisms of totalitarian regimes. The ideological underpinnings that were translated into the ‘ideal states’ of traditional totalitarian regimes seem to be absent in the alliance of trusted networks that we have been discussing. But 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 amicably disposed to the intentions and dispositions of enterprise.

42. L. Davidson, ‘A National Debate About Government Spying?’ NYTexaminer.com, 16.7.16): http://www.nytexaminer.com/2013/07/a-national-debate-about-government-spying. All further quotes in this paragraph are from this report.
associations, and so the role of the industry of civil society - the third and newest trusted network - arises, 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: the monopoly of digital planning on surveillance operating through back-channel and secret communication between government, tech corporate elites and, sometimes, NGOs; the use of civil society NGOs as mechanisms for circumventing democratic processes; an enterprise-association politics that ensures that the dual goals of state (security) and capital (profit) continue unabated and with little unaccountability; the unprecedented scope offered by total structural data acquisition to western intelligence matrixes; the persecution and prosecution of journalists, whistle-blowers and transparency actors outside the scope of civil society groups; and the significant, if insufficient, contestation by members of the public concerning the infringement on civil liberties.

There is an urgent need to reconsider the quasi-totalitarian practices of these enterprise associations conducted by the three global trusted networks and led by the United States, and new methods for challenging it need to be devised. Without a structural solution to the occupation by the three networks of the political space in digital environments, 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, in order to assert her own rights and the networks’ ethical obligations.

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.

Athina Karatzogianni is a Senior Lecturer in Media and Communication at the University of Leicester. Her research focuses on the politics of digital media. Her latest monograph is Firebrand Waves of Digital Activism 1994-2014, Palgrave Macmillan 2015. All her publications can be read at: http://works.bepress.com/athina_karatzogianni/. She can be contacted at athina.k@gmail.com. Martin Gak is an independent scholar who holds a Ph.D. in philosophy from The New School for Social Research. The focus of his research interest lays at the intersection of ethics and metaphysics. He writes on politics, religion and jurisprudence, and their relation to moral adjudication.