Chapter Three: The Fourth Phase: 2010-2014 Digital Activism Invades Mainstream Politics

3.1 WikiLeaks: Ideological and Organizational Tensions

The WikiLeaks revelations in my view became the symbol of the mainstreaming and popularization of digital activism in the public sphere and this is why I view this the start of a fourth phase in digital activism. WikiLeaks was in a sense a continuity for online collaborative communities, such as the FLOSS movement, as was explained in the first chapter. I started thinking about how affect theory could contribute to the study of the first reactions to the WikiLeaks revelations when I was preparing a chapter for the edited volume we published with Adi Kunstman in 2012. I am reusing material from that chapter here (Karatzogianni, 2012). By using affect theory, which I explain in-depth in a theoretical section chapter four (4.4 The Affect problematique), I sought to enrich cyberconflict theory beyond the identity, media representations, discourse, conflict analysis and resource mobilization elements I utilized in previous studies.

WikiLeaks is a continuation of a tradition of an overall information age ideology adhering to 'information wants to be free', wanting to change the world through making government open and accountable, through fostering some kind of alternative to capitalist relations, and through peer production and collaborative networks. There are dozens of groups others political and others less so. The peer production and open source groups have given us an array of beautiful products and have proven that human collaboration outside and in parallel with the capitalist system is both possible and sustainable. Indeed, there is a longer tradition of civil disobedience, political dissidence and social movements in the historical narrative, which various hacktivist groups might be drawing from as well, which have been present already at the very first phase of digital activism (1994-2001). The criminalisation of protest and hacktivism, cracking down on the freedom of expression, their portrayal as threats to global security and as terrorism, is a tactic, which was a backlash from the second phase due to 9/11 (2001-2007).

The reactions to the WikiLeaks in terms of content, but more importantly I think in terms of what the organization itself stands for, are swamped by strong feelings and by intense flows of affect, which eventually over-spilled to cause revolutionary change in countries in the Middle East and the potential of more change elsewhere. If you are to discuss the psycho-political formations digital movements and antagonistic organizations tap into, you only have to look at the reactions to the WikiLeaks saga: Authoritarian leaders urging their subjects not to listen to Assange portraying him as a western stooge; liberal democratic governments talking of threats to national security and fear for soldiers' lives; the call by mainstream conservatives in the US for Assange to be trialled as a traitor and executed; in other left wing and radical quarters to be treated as a hero and an icon for the digital revolution for some, and criticism regarding his leadership style, for not being accountable, decentralized or rhizomatic enough for others.

In Assange's case, the mainstream media narrative followed a spectrum which coincided with the initial portrayal of Assange by his chosen partners in leaking Cablegate to the world (The Guardian, New York Times, Der Spiegel), only to shift

like a pendulum in the opposite direction, with criticism of his personality and personal life, when the reactions by governments, especially the U.S. and the hunt for his demonization started by mainstream media and governments around the world. This shift in the narrative produced even stronger affective reactions, polarizing the feelings around Assange and creating instant enemies and supporters, some of whom demonstrated their feeling with a wide variety of actions, from asking for his death penalty, to hacking banks and online outlets for not enabling Assange's financial support. Undoubtedly, it is difficult to tell whether affect creates the events and the subsequent media coverage, or it is the original media coverage of WikiLeaks and the Cablegate scandal, which created the feelings which impacted on the digital virtual and enabled the upsetting of the status quo around the world, thereby acting not as a cause, but as an accelerating factor along with social media to the Middle East revolutions. It is these affective flows toward WikiLeaks and Assange played out by individuals, governments and organizations, both in the actual and the digital virtual, which when overflowed, accelerated the overthrow of authoritarian leaders in Tunisia, Egypt, Libya, Yemen, Syria, and elsewhere in the Middle East.

Julian Assange, the founder of WikiLeaks, in various interviews and in the WikiLeaks site has expressed the ideology behind WikiLeaks as an amalgam of principles, those underlying the Founding Fathers and the American Revolution, freedom of expression, open government, and the right of the people to hold accountable their leaders in a democracy. In his own words, 'So as far as markets are concerned I'm a libertarian, but I have enough expertise in politics and history to understand that a free market ends up as monopoly unless you force them to be free. WikiLeaks is designed to make capitalism more free and ethical' (Greenberg 19 November 2010). Assange himself is arguing that there is 'a deliberate attempt to redefine what we're doing not as publishing, which is protected in many countries, or the journalist activities, which is protected in other ways, as something which doesn't have a protection, like computer hacking, and to therefore split us off from the rest of the press and from these legal protections' (ibid.). Despite Assange's effort to distance WikiLeaks from the hacker movement, in order to promote it as a publishing outlet with the legal cover that provides, it is obvious that it has had a wide influence on Assange's own ideology. Therefore, add to libertarianism the baggage of free culture, hacker culture where Assange is coming from, and you have the ideology of many plateaus and systems of thought ranging from liberal, to libertarian to elements of anarchist thought and free culture all really comfortably attuned to what has been called information age ideologies.

The free culture movement and hacker culture encompass different types of ideology: some political, others apolitical, some truly revolutionary in both philosophy and practice and others less so, which have been examined extensively especially over the last decade (Castells, 2001; Weber, 2004; Lovink, 2007; Taylor and Jordan, 2004; Raymond, 2001; Williams, 2002). There seems to be an issue with attaching any online collaborative project, whether it would be a software project, a free culture offering, or a social media-enabled protest movement to a specific ideology. On the one hand, there are ideologues who deliberately seek to realise the revolutionary potential of technology and enhance the effects in the political economic, social and cultural process to change the system as a whole, such as the ideology of free/libre software movement (Stallman 2009). Nevertheless, often, the commercial viability of a project means that the ideology of activism is played down to create focus on the

value of the product offered. In this sense free-software was revamped as open-source to dissociate from the ideological components (ibid.). Currently, ideology is often mixed with activism, with activist entrepreneurs and entrepreneurial activists, an obvious example would be China and social activism mixing with internet companies, and riding the band wagon of activism to attract more hits on commercial sites for profit purposes (Yang 2009b), as explained already in the previous chapter on Chinese dissent.

There is a wide ideological spectrum in information age ideologies, ranging from neo-liberalism to cybercommunism, to libertarianism and to anarchist thought. In a way, ideology is almost transferred through those old lenses of the traditional political thought and applied to the political economy, culture and society of the digital virtual. In many ways although the medium is postmodern, the aims and desires are still of the modernist variety. The groups engaging in cyberconflicts are still fighting for power, participation, democracy, but are using an accelerated process and a postmodern medium that enables asymmetries, empowering the previously marginalised or repressed, causing shifts in our understanding of identity and community, accelerating feelings and political attachments to foster unprecedented social and political change. The internet encourages networked organization and mobilization, a version of the commons that is ungoverned and ungovernable, either by corporate interests or by leaders and parties. We have seen the empirical confirmation of this trend to include social networking in the revolutions, which took place in the Middle East. Some of these groups, which are informed by a more postmodern reading of ideology are calling for the transfer of some of the features of the digital virtual to the actual world, and they are doing this by mixing and matching several elements of traditional political thought to express this affect for change. It seems that WikiLeaks is part of that creed.

In close proximity to problems stemming from the ideological platform are organizational problems in FLOSS communities, which have been discussed extensively (Dyer-Witherford, 1999; Weber, 2004; Benkler, 2006; Karatzogianni and Michaelides 2009). Assange admitted that the growth of WikiLeaks was too rapid to allow for adjustments in organizational terms. This is where the initial failure to support Manning with funds, or to respond to global attacks actual, mediated or digital can be partially explained.

We know from social movement theory (Snow et al. 1980: 790-797), that the fewer and weaker the social ties to alternative networks, the greater the structural availability for movement participation and, movements which are linked to other groups expand at more rapid rate than more isolated and closed movements (Snow et al. 1980: 790-797). This is why the network effect is responsible for WikiLeaks and Assange being supported by such diverse actors. Various celebrities helped pay his bail in the sexual assault case, a former soldier offered him residence in the UK, and Daniel Ellsberg, a whistle-blower of international status spoke in his defense. Journalists and media organizations, politicians and academics from various fields reacted almost emotionally to Assange and his organization, as did social movements, NGOs, human rights protesters, hacktivist groups, such as Anonymous, various file-sharing communities, and information age pioneers and ideologues. All these individuals and groups adhere to different ideologies and have a wide-ranging race, class, gender and nationality backgrounds. They are, in a bizarre way, the multitude in

Hardt and Negri's sense (2004) of players, which have to express their particular affect, nevertheless, drawing from their individual causes and systems of belief. Through diametric opposite flows of affects, they either render Assange a hero or villain and his organization a revolution in the media ecology or an anathema to global security. In a way, Assange and his organization are this empty signifier filled ideologically to reflect the discursive mood of the movement or the individual, supported by different forces which outpour their feelings on different facets of the WikiLeaks story, be it digital rights, freedom of expression, internet censorship, international legal issues, national security, civil rights, privacy, whistle-blowing against multinational corporations and governments, and the list is endless.

This was the difficulty of adhering to an organizational model for WikiLeaks that would satisfy the image and ideology of such disparate forces. Assange has called himself the 'boss' that fired Daniel Domscheit-Berg, although it is obvious that WikiLeaks started with an information age philosophy, which according to some, was compromised, when it all went global and mainstream, with mainstream media given leaks and deals made by the 'Leader', often without consent or knowledge from his WikiLeaks base.

The leadership and organizational tensions evident in WikiLeaks is witnessed since the advent of the digital. In other groups, the threat of forks forced organization choices to be made to solve structural chaos and force sustainability by either forking or creating crypto-hierarchies or open hierarchies. Recall this problem already appearing in the first chapter of the book. An Icelandic parliamentarian and former WikiLeaks spokeswoman Brigitta Jonsdottir --the U.S. subpoenaed Twitter to hand over her personal details-- has tellingly described the organizational problems thus and notice how her affect and emotion is pouring from that account:

There is not enough transparency within the organization about decisions and not good enough communication flow and in order for a good communication flow, you have to have good structure and know whose role is appointed to each other. I just wanted to have a debate about this with sort of the core group of volunteers and I couldn't. I tried for a long time and it didn't happen. One of the biggest criticisms on WikiLeaks, just like WikiLeaks criticizes government for their lack of transparency, there was a big criticism of WikiLeaks for not being transparent enough about their financial system, their donations. It would have just been so easy to make that just completely open instead of defending it all the time and having these speculations.

(McMahon, 15 January 2011)

The OpenLeaks fork was caused by disagreements over Assange's leadership style and the centralization of the organization, although his trouble with Swedish authorities over sexual assault allegations did not help either. It is often a charismatic leader who can inspire the community involved, and we have seen the failure to inspire positive affect in forks across software communities with threatened forks in Linux, and actual forks elsewhere. The OpenLeaks is in fact very close ideologically to the open source movement, in that it keeps the traditional ideological constraints out of the picture to concentrate on improving the process and the product. It is projected as a neutral conduit of people interested in exposing injustices: 'Our intention is to function, as much as possible, as a mere conduit (akin to the telephone

exchange and the post) between the whistleblower and an organization of their choice. This means that OpenLeaks does not accept submissions or publish leaked material directly' (openleaks.org).

In the WikiLeaks' case, Assange has a broad spectrum of ideological influences and he is very careful not to alienate by alluding to more radical systems of thought, even if his hacker culture background might mean he has certain beliefs which point to non-mainstream influences. Nevertheless, it is partly the concentration of leadership in his hands that caused the OpenLeaks fork: 'OpenLeaks is based on a more decentralized concept. We do not seek to publish information ourselves, but rather to enable third parties to do so' (openleaks.org). Smári McCarthy has been involved in various socio-technical initiatives (for more see <http://www.smarimccarthy.com/> and <http://planet.fabfolk.com/>), and was a candidate for the Icelandic parliament. He was initially involved in WikiLeaks, and in his own words had to spend 'a lot of time trying to clear up the unfortunate aspects of my erstwhile connection to them'. He had this to say about the ideological issues: 'The stated ideology of WikiLeaks has very little in common with its organization. One of the reasons the Openleaks fork is important is because it allows the localization of the information politics, where WikiLeaks has been attempting to amplify itself and go for global impact, but falling very short of that due to the fact that their group's skillset is very western-biased' (Email interview with the author, 15 February 2011).

So far, the focus has been the WikiLeaks ideological and organizational tensions which caused difficulties in the perception of WikiLeaks, in terms of what it was officially meant to be representing and with its dealings with other protagonists, its base of supporters; its inability to address the issues as they were arising, due to organizational tensions; a too broad and confused ideological platform that could not reconcile ideology, philosophy, and organisation of the founding organization with the more centralized approach, whereby the personality focused on its leader, Julian Assange, his personal life story, and his trouble with the sexual assault charges in Sweden. The next session looks at the impact of the WikiLeaks phenomenon on scholarship.

3.2 WikiLeaks: Impact on communication and International Relations scholarship

Subsequent to this work exploring affect, ideological and organizational tensions in WikiLeaks I teamed up with my long-term co-author Andrew Robinson to look at the impact of WikiLeaks on academic scholarship in 'Digital Prometheus: WikiLeaks, the State-Network Dichotomy, and the Antinomies of Academic Reason' (a shorter version of this work was published at the *Journal of International Communication*, see Karatzogianni and Robinson, 2014). We focused on the academic reinscription of the WikiLeaks affair, examining the different receptions received within different literatures and fields.

The WikiLeaks affair – with or without its hypothesised connections to the Anonymous collective and the Arab Spring – has had massive ruptural effects on aspects of the global political system. A small, movement-based website has inflicted a tremendous informational defeat on the world's last superpower, revealing the

possible emergence of a global networked counter-power able to mount effective resistance against the world-system, possibly even the emergence of the state-network conflict as the new great-power bipolarity after the Cold War. Therefore, in many respects, and notwithstanding WikiLeaks' relatively closed political structures, the WikiLeaks affair expresses the power of networked, decentred social movements to disrupt hierarchical arrangements of state and capitalist power. WikiLeaks has struck a tremendous blow for the power of transnational activist networks, against the power of states. How this blow – and the corresponding redistribution of global power – is perceived, will depend fundamentally on how the commentator feels about the current distribution of global power in favour of states. Perspectives can thus be divided, not only by discipline, but also by the author's position on the state-network dichotomy. Furthermore, different academic disciplines can be mapped in terms of their relative closeness to the statist or network side of the controversy.

As we saw from the previous section, diverse affects and subject-positions mobilised by WikiLeaks through the 'Revolutionary Virtual' – the field of construction in which zones of affect are selected and actualized. As a creation of new zones or assemblages of affect, the WikiLeaks affair can be seen as an event, and like all events, it is controversial. From a Badiouian perspective, one might divide scholars' responses into those who are in fidelity to the WikiLeaks Event, and those who react against it as representatives of the established situation. The study of the academic reception of WikiLeaks is thus a study of the reverberation of an Event through the social field.

WikiLeaks can be viewed through the figure of Prometheus – the archetypal Internet troll of Greek mythology. Prometheus is a trickster figure, bringing life to clay (to create humans) and fire to humanity (to create civilisation), in defiance of the fatalistic order of the Gods. Tricksters in mythology are typically on the side of creativity and chance, and crucially, aligned with the rebel who defies and escapes the order of Fate: 'the hero – for example, Prometheus – challenges fate with dignified courage, fights it with varying fortunes, and is not left by the legend without hope of one day bringing a new law to men' (Benjamin 1995, p. 294). WikiLeaks here stands for exactly such a gesture: within the world of neoliberalism, the fatalistic advancement of global capital, and of the State as the bearer of Fate (ibid. pp. 285-6), has been interrupted by a technological 'progress' long forecast by the fatalists, but detoured decisively from their fatalistic narrative of progression. Instead, this Promethean flame is an uncontrollable force of networked power, which seems chaotic from within the statist order of Fate. Hence the attempts of the state to punish Prometheus, to sentence him to eternal punishment as did Zeus, for rupturing the divine order. But here the accounts of the myth diverge: did Heracles free Prometheus from his enchainment? Perhaps digital social movements are the Heracles in this scenario, flexing their own muscle (such as the Anonymous DDOS attacks) to protect Prometheus from the order of Fate. It remains an open question whether Zeus will have his revenge, or whether Heracles will ultimately prevail.

In discursive terms, these two stances can be mapped along two axes of intellectual controversy, which arise in the literature. In International Relations (IR) and related disciplines, including foreign policy studies, comparative politics and law, the main focus is on *transparency* versus *secrecy*: the ethics of whistleblowing versus national security, the impact of leaks on the 'war on terror' and American foreign policy, and so on. In disciplines more closely aligned to the social, such as cultural studies,

media studies and sociology, the major debate is between *openness* and *control*. Issues include the relationship between WikiLeaks and the hacker ethic, the constraint of overwhelming state power, the emergence of a global public sphere, the changing relationships between old and new media, and the emergence of shifts in social relationships marked by the current wave of social movements. These differences emerge for a particular reason: the framing of the state- (social-movement-) network conflict through the gaze of the state, or from an interpretive standpoint framed by the attempt to understand the social.

Furthermore, they express the anxieties and orientations of particular authors. As Foucault (1977) rightly argues, power and knowledge directly imply one another, and the success and survival of different academic schools and disciplines may hinge on the balance of global power (p.27). Advocates of disciplines threatened by a diffusion of information are likely to be far more alarmed at the WikiLeaks affair than those working in disciplines, which flourish on networked methods. We see in some accounts the voice of Zeus seeking to silence and torture the digital Prometheus, in some the voice of a Promethean force, and in some the voices of those who would draw on the Promethean force to revitalise the order of Fate.

Methodologically, we analyze the ideology in academic scholarship by mapping along two axes of the intellectual controversy, which arise in the academic literature immediately after the Collateral Damage video in July 2010. We used Google Scholar to capture academic scholarship and opinion from the summer of 2010 to December 2012, with an original sample of 40 articles, which then extended to snowball sampling stemming from the original sample. Of these, we chose to focus only on the two disciplines. Moreover, we chose that specific timeframe for sampling and did not include the years 2013–2014, an effect of the journal review timeline process, and further, it would take the scope of the study to another level altogether, considering the academic literature involving several subfields. Unfortunately, this means we left out *the most significant academic contribution in relation to the WikiLeaks phenomenon thus far by Brevini, Hintz, and McCurdy (2013) and other important works from 2013–2014, which could be examined in future studies*. Thus, the work, reflexive of its limitations, presents a broad meta-analysis of the debates surrounding academic scholarship within a specific timeframe, and does not pose itself as an overall meta-analysis of all fields affected by the WikiLeaks phenomenon to this day.

International Relations Scholarship: The Right to a Cover-Up?

The first standpoint to examine here is that of the state, or Zeus. Like any good trickster, Prometheus is a prolific troll. He has successfully trolled Zeus, who is now, in online terminology, ‘butthurt’. This is a source of endless *schadenfreude*, or ‘lulz’, for Prometheus and his allies. But the state's reactive affects, directed against the trickster, take the horrifying form of divine vengeance. In academia, the standpoint of the state, and the order of Fate, is borne mainly by mainstream scholars within International Relations and security studies. These scholars are bearers of the desire to chain and torture Prometheus – variously manifested as declaring WikiLeaks a terrorist group, assassinating Assange or jailing him as a spy, torturing Chelsea

Manning, and rounding up Anonymous and other hacktivists as ‘criminals’ or even ‘enemies’.

Statists generally minimize the benefits done by WikiLeaks to maximize its alleged harms. From the statist point of view, the events exposed in the WikiLeaks cables are unsurprising. Anarchy is theorized by realist IR scholars as the absence of a global centralized government, which views the state—despite its evils—as a necessary guarantee of a worthwhile life. Further, for realists, it is normal for states to use Realpolitik to achieve their objectives. Indeed, the content of the cables may strengthen realists against rivals such as liberals and constructivists, who maintain that states can be constrained by norms and ethics. The realist objection to WikiLeaks is not, therefore, to the information revealed, but to the violation of a state privilege, which is taken to amount to an anarchist destruction of the state (Lim, 2010). Steinmetz (2012) explains the American state’s responses—such as threatening to prosecute Julian Assange for espionage, labelling WikiLeaks a terrorist group, and calling for the execution of whistleblowers—the following way:

Realpolitik explains why those events – and others – may have occurred and why the government became so upset when revealed. It is posited here that the United States was largely not concerned with maintaining foreign policy relations for ethical or moralistic reasons. Rather, these relationships were manipulated and maintained for the state’s own interests.

(Steinmetz, 2012, p. 22)

Steinmetz admits a real danger that the government can use secrecy to cover up wrongdoing (ibid., pp. 23-4). Steinmetz demonstrates through his analysis of secondary data sources that the government officials’ public statements ‘attempt to manipulate public opinion in a manner conducive to realpolitik governance’ (ibid. 27). His analysis points to the U.S. arbitrary rhetoric of supporting government transparency and whistleblowing, but considering WikiLeaks an organization seeking to undermine national security. In this way ‘the U.S. reserves the right to define who is and who is not a whistle-blower and seeks ways to prosecute those who are not categorized as such’ (ibid. 35), while this ‘process of employing arbitrary rhetoric then deciding who is covered is a result of intense realpolitik’ (ibid. 36). Realism simultaneously exposes and condones the double standard whereby America attacks WikiLeaks while condemning China for its actions against Internet dissidents (Karatzogianni, 2010) and while operating its own cyberwar capabilities, including arguably the networks which DDoS’ed WikiLeaks.

There are two views of cyberspace and its relationship to society: a view that cyberspace must conform to existing institutions and a view that cyberspace is re-ordering society and unleashing new possibilities for human freedom (Sterner, 2011, p. 1). These two views can be summarized as a state and a network perspective, respectively. Not surprisingly, Sterner is broadly sympathetic to the former view, maintaining that WikiLeaks has harmed American national security and typifying Internet freedom advocates as ‘expansionists’ (ibid., p. 3). This follows a long tradition in IR of accusing new political formations of aggression and revisionism, disrupting the stable balance of world peace. So-called expansionists ostensibly

believe that 'large institutions and organizations, such as governments, are not entitled to privacy or secrecy' (ibid., p. 4). On the other side, proponents of imposed conformity are typified as instrumental, seeing cyberspace as a 'tool of society' which 'should conform to established relationships, values and laws' (ibid.). Despite this assessment, Sterner also sees WikiLeaks as part of a trend which is here to stay, based in the culture of the Internet and which will 'undermine the long-term utility of the Internet for commerce and governance' (ibid., p. 3). He sees the two sides engaged in an intensifying conflict which is playing out in courts and legislatures across fields such as Internet neutrality and intellectual property (ibid.). Nevertheless, this idea of expansionism is seriously problematic.

Sterner's criticisms of so-called expansionists are twofold. Firstly, attacks on the 'instrumental view of cyberspace' are taken to undermine 'trust', which makes cyberspace less useful for 'conducting activities'. Secondly, if large institutions and corporations 'step back from the use of cyberspace because they lose trust', its revolutionary potential is also diminished (ibid. p.7). The subtext here is blatant: cyberspace is valuable, only if global elites can still exploit it, without which, it becomes useless. By an act of verbal acrobatics, Sterner thus portrays a process of corporate and state enclosure of an autonomous zone as a status quo threatened by aggressive attacks. The scenario of complete de-commodification of the Internet, which he posits is unlikely, unless accompanied by a thoroughgoing move towards networked, peer-to-peer production structures. Outside such a context, a less corporate-friendly Internet would see capitalists forced to reach compromises and conform to Internet culture, rather than altering it. It would take more than a reduction in trust to prevent their exploitation of whatever profit opportunities they can find, since as we know from the subprime mortgages affair, capitalists are not necessarily averse to risk. In any case, the biggest threat to the trustworthiness of online transactions is doubtless the state's attempts to break encryption systems through means such as quantum computing, a process which poses very real risks of rendering e-banking and secure purchasing obsolete.

The idea of 'expansionism' is seriously problematic. As suggested by various scholars (Christofoletti & Oliveira, 2011; Flew & Liu, 2011; Ludlow, 2010), WikiLeaks has its ideological origins in the hacker ethic. Since the hacker ethic is as old as the Internet, and arguably provides the constitutive power generating the Internet's emergence and evolution, claims of 'expansionism' are poorly directed. Rather, it is the state's attempts to striate or encroach on the Internet as an autonomous networked terrain, largely due to the expansion of corporate and conformist assemblages online, which entails 'expansion' and the revision of the status quo.

It is worth contrasting Sterner's work with another work from a similar angle. From a cybersecurity perspective, Betz and Stevens (2012) argue for a less repressive approach to the governance of cyberspace. The state must accept the autonomy of cyberspace in order to benefit from its economic potential. The division among statist scholars shows a key dilemma of state power, between the addition of axioms and tolerance of autonomy so as to exploit it, and the subtraction of axioms and repression of autonomy so as to suppress lines of flight (Karatzogianni & Robinson, 2010, pp. 50-2). The expansion of capital, and thus of state power, depends on exploitation of flows of creativity, but tolerating or enabling these flows requires a relaxation of the pervasive desire for control. In seeking to make cyberspace 'safe' for itself, the state

risks killing the goose that lays the golden eggs. Ultimately the Promethean fire of constitutive power underpins the order of Fate, and Zeus is at risk of destroying himself along with his 'enemy'.

The WikiLeaks phenomenon is a line of flight, or as put by Saunders (2011), a hacktivist challenge to the diplomatic system. Saunders argued that the cables on the whole revealed little more than gossip – such as the scandalous leaks about Berlusconi, Qadaffi and Putin -- or else affirmed unsurprising facts about American foreign policy, such as Yemen's collusion in drone strikes, NATO plans to defend the Baltic States and Poland, and American anger at Armenian arms sales to Iran. A few leaks, he admits, were genuinely revealing, such as American complicity in Ukrainian tank sales to Southern Sudanese militias, and Hillary Clinton's orders to spy on key UN officials (ibid. p. 6). More broadly, he sees the WikiLeaks affair as a 'crisis' which threatens 'traditional forms of diplomatic power in the international system, particularly those that are dependent on closed networks, reliable distinctions between public/private information and established geopolitical narratives' (ibid. p.2). This challenge comes from emergent structures of digitised global communication: 'Perhaps at no time in history have ordinary citizens possessed so much power in the field of global politics' (ibid. p. 9).

Overall, however, Saunders' verdict rules out the participation of new political formations in global diplomacy. 'While Julian Assange & Co. proved that even the most clandestine exchanges might be plastered across the front page of the New York Times, no member of the WikiLeaks will ever be called upon to solve the Israeli-Palestinian crisis, negotiate trade agreements between Azerbaijan and Russia, or set environmental policy for the G-20' (ibid. p.9). This importance is not only ethical, but strategic: since diplomatic elites can shape mainstream media discourse, they will continue to rule the roost (ibid.). What this account misses is that social movements and networks *do* seek to act on all these issues, from mass resistance to unequal trade agreements in Korea and Bolivia, to ecological protests, which have forced strong concessions in regions such as Uttarakhand and the Penan territories, to grassroots conflict transformation initiatives such as those of *La Ruta Pacifica*. States are, of course, more effective in finding statist solutions which benefit elites, but social movements are very much players in all of these fields, often in a highly public way. The transfer of power from states to networks may alter the balance of power towards social movements in many of these fields, ensuring more socially just and sustainable outcomes than statist diplomacy would have realised. In addition, the revelation of what is already known or suspected is itself significant, in that it removes the deniability behind which power can otherwise hide.

And yet, Bronk (2011) emphasises the rise of 'cyber-enabled diplomacy', in which cyberspace is itself used for diplomatic purposes by the US government. He suggests that the WikiLeaks affair triggered the US state's decision to install a 'cyber coordinator' (ibid. p. 4), but also suggests that the incident is ultimately unimportant, since similar information breaches are unlikely to be repeated in similar ways (ibid. p. 13). The Edward Snowden leaks in the summer of 2013 have spectacularly refuted this argument. In Bronk's case, it is the technical, tactical, operational emphasis which creates the chain connecting scholar to state: by seeing WikiLeaks saga solely in terms of a technical failure to prevent a 'breach' (defined as such from the state's point of view), Bronk is a typical 'problem-solving theorist', bracketing out the

broader frames within which technical problems are embedded. The WikiLeaks 'event' in effect becomes invisible, reduced to a failure of the coordination of elements in the existing situation.

On a similar note, Erbacher (2011) uses the WikiLeaks affair as the basis for a discussion of technical means of preventing further leaks – deemed in the usual fear-inflated language as 'insider threats'. He proposes the use of procedures which will expose 'significant irregularities' so as to identify threats (p. 1). As Erbacher admits, such profiling has traditionally been avoided because it both fails to detect actual threats and accuses too many innocent people. In the authoritarian drive for a threat-free, totally controlled world, Erbacher glorifies the use of data mining techniques, which effectively can breach both privacy and encryption and criminalise difference. The NSA and GCHQ surveillance operations as revealed by Edward Snowden are a case in point of the pitfalls of such approach and the potential for abuse.

French critical scholars Devin and *Törnquist-Chesnier* (2010) argue that diplomacy is evolving into a new configuration in which the public-versus-secret dichotomy no longer operates, and the relation to nonstate actors becomes more important. This 'opens up new fields for research by questioning the intra-systemic relations of a "diplomatic community"' conceived in expanded terms, examining networks of diplomacy in terms of vertical and horizontal connections' (ibid., p. 73). They call for a move toward a 'new diplomacy' that is multilateral, public, and itinerant instead of secretive, sedentary, and individualized, a transition arguably aided by WikiLeaks, which is a symptom of the newfound vulnerability of states to nonstate actors (ibid., p. 71).

Diplomacy discussions also involve fears that diplomacy, as currently constituted, is at risk. According to its advocates, the diplomatic privilege and the confidentiality of diplomatic communications are supposed to allow 'states to communicate with each other in open and candid ways, and also for important figures to say things they think true, but too politically damaging or physically dangerous for publication' (Page & Spence, 2011, p. 237). Page and Spence argue that the system is flawed and requires change. The leaks should inspire caution in America's sources, as well as raising concern over the boundaries between diplomacy and espionage. Nevertheless, they feel that in the longer term diplomacy will not change and, if anything, will become more secretive rather than less (ibid.). Governments are more likely to respond to the risk of leaks through increasing self-censorship, secrecy, and the use of oral briefings, which 'will lead to worse decisions and less accountability for the decisions that are made. It seems a high price to pay for gossip' (Chesterman, 2011, p. 4). One can perhaps revisit the irony of such visions of diplomacy, with Assange living under diplomatic asylum in the Ecuadorian embassy since June 19, 2012, and with the British government threatening to violate diplomatic norms to get him out.

On the basis of the WikiLeaks phenomenon, Rosenzweig (2011) argues that the U.S. needs an online counterinsurgency strategy. He sees WikiLeaks as 'launching an assault on state authority' (pp. 1–2), expressing an enemy ideology which is shared by groups such as Anonymous. He also suggests that Anonymous' vulnerability to counterattack is likely temporary. He calls for attacks to 'isolate fringe actors from the general populace and deny them support and refuge' (ibid., p. 5). Though differentiated from a purely technical response, this approach still fails to engage with

the adversary on anything other than an operational level. The technical means used are simply broader (and more dangerous to civil liberties). The possibility that actions against a secretive and repressive state might be justified is simply framed out of this kind of analysis, which takes the legitimacy of the global system for granted and sees any means which preserve it as justified.

Strong statist positions have also appeared in the ethical theory literature. For instance, Somerville (2010) had argued that leaking is a wrong means, which is not outweighed by good ends, as well as arguing that it poses large risks such as global war. She argues that it poses such a threat to America's 'social capital'—such as trust in the government—to be considered harmful. In other words, government wrongdoing should be covered up so as to maintain the basis for social support for the dominant system. Responding to Somerville's view, media and propaganda theorist Marlin (2011) argues that WikiLeaks is on the whole a good thing for media ethics. This does not simply mean that ends justify means, but a higher ethical good negates the wrongness of the means. Hence, Marlin maintains that WikiLeaks is deontologically—not only consequentially—defensible. WikiLeaks is a counterforce against antidemocratic forces in the contemporary world, providing "the raw material that the public often needs to form sound judgements" (ibid., p. 5). WikiLeaks could also lead to great goods, such as making it harder to fabricate the basis for going to war (Ibid.). He concludes that 'some drastic means are needed to push back against the increasing inequalities favouring the very rich' (ibid., p. 6). Marlin thus embraces power redistribution from concentrated to diffuse forces, which WikiLeaks entails, whereas Somerville construes it as a threat. There is a significant irony here. In other contexts, the state is all for what Virilio (1997) terms 'telepresence,' supporting surveillance with the duplicitous claim 'nothing to hide = nothing to fear.' The inversion of telepresence, the sudden exposure of the state to the ease of visibility in the information age, thus exposes the hypocrisy of its own reactions, seeking a special exception from the vulnerability to visibility it imposes on others.

In this logic, Radó (2011) argues that WikiLeaks opens up questions of the inside and outside of the public and private spheres in a digitally networked world. Using concepts such as sense/nonsense, materiality/simulation, state/nonstate and participation/spectatorship, she asks whether the current system should fear the collapse of the public sphere and dominant forms of diplomacy, or whether WikiLeaks instead portends the expansion of the public sphere. Her position is that 'WikiLeaks presents an in-between phenomenon, in which case its appearance on the stage of world politics already signifies that there is a move from a traditionally conceptualized "public sphere" towards the operation of the sphere of "publicity" in the terrain of politics' (Radó, 2011: 6). WikiLeaks thus portends, not an apocalyptic scenario of uncontrolled harm, but a rebalancing of the relationship between society and state towards a more participatory regime of power.

Overall, critical IR scholars emphasize the outpouring of violent rhetoric and repressive actions by the American regime, from threats to assassinate Assange or designate WikiLeaks a terrorist group, to the attempts to have Assange extradited. Such responses are taken to show the worst about sovereign power, as they 'amount to a profound showing of authoritarianism' (Springer et al., 2012). The broader context of WikiLeaks is one in which the U.S. is attempting to reproduce a climate of global war. Strategic analysts such as Miskimmon, O'Loughlin, and Roselle (n.d.)

offer a constructivist account of the situation. These authors suggest that strategic narratives are ‘a means for political actors to construct a shared meaning of international politics to shape behaviour of domestic and international actors’ (ibid., p. 8). The argument that ‘American identities are deeply embedded and remain heavily imbued with racial, religious and imperial features’ also challenges any transformational claims of the Obama national security strategy (Parmar, 2011, p. 153). To put it bluntly, the U.S. state is seeking to keep alive the ‘war on terror’ strategic narrative, even while seeking multilateral engagement (Gray, 2011).

Between Human Rights and Sovereign Exception: Legal Scholarship

Also broadly within the state domain, but more alert than most to the abuse of power and concerned to protect the professional niche of law from the expansionist national-security apparatus, legal scholars have responded by focusing on the ambiguities thrown up by the affair. In the American literature, the WikiLeaks affair reignited ongoing debates between the liberal commitment to transparency – enshrined in the First Amendment and the Freedom of Information Act (FOIA) – and the nationalist obsession with preserving security at any cost. Legal scholars have called for clarification or reform of existing laws to determine what information is protected and what is prohibited (Oppen, 2011, pp. 240-1), though in the current climate this is likely to lead to a securitarian outcome. American regime commentators have been quick to distance WikiLeaks from First Amendment precedents such as the Pentagon Papers case, instead seeking to frame WikiLeaks within the ‘global war on terror’, as espionage, terrorism or security threat. This expresses a contradiction within law, which is becoming increasingly salient in the context of securitization, and which is highlighted especially by Agamben: the contradiction between the claim to legal inclusion, such as human and civil rights, and the ‘sovereign exception’ on which law is secretly based, the arbitrary decision to divide the world into bare life and politically-recognised life, that is between the state as orderly life and as divine vengeance. Pro-regime commentators have been quick to seek to portray WikiLeaks as “bare life”, unprotected by media freedom, whistleblowing precedents or the American First Amendment, whereas supporters of WikiLeaks emphasise its fundamental continuity with other cases of whistleblowing, and the arbitrariness of the sovereign exception. As Wall (2011) suggests in relation to the Anonymous collective, the defence of human rights in a contemporary period is ‘anti-sovereign’, occurring across the boundary between liberal rights and a radical theory of the multitude. It involves the enforcement of human rights by networks, against states.

Legal scholars have generated a backlash against the militarisation of the WikiLeaks affair which stands somewhere between a strong statist perspective and a pro-network position, as one might expect from the position of lawyers as part of the included stratum, seeking to constrain but not undermine the state. Criticising the expansion of sovereign power to cyberconflict, military legal specialist Dunlap (2011) argues against the common view that there is a lack of international law governing cyberconflict, suggesting that the difficulty is, rather, in establishing the facts necessary to apply the law. He suggests that a less tolerant ‘national security’ framework is being used, in which force is used to eliminate perceived threats and is ‘intolerant of any injury’, instead of a ‘law enforcement’ framework, which uses force

to detain suspects for trial (p. 84). Dunlap suggests that online incidents such as the WikiLeaks affair are insufficient to qualify as use of force or to justify acts of war, both because the harm caused is insufficiently great, and because the actors involved are not representatives of states. This places the issue within the field of law enforcement. Such an approach would certainly pare back discourses of national security, but still seems to suggest an ultimate primacy of states over social movements. He fails to see the social factors – i.e. the emerging power of networks, and their ability to act autonomously from states – which repressive ‘national security’ regimes seek to suppress.

In Australia, while political responses have been conflictual as to what international whistleblowing might entail, there is a developing pressure ‘for a new whistleblowing framework, so that current unworkable presumptions against any disclosure are removed, and conflicts are more manageable’ (Brown, 2011). Such apparent legal ambiguities arise from the conflict between the state's expansive demand for logistical control of territory and the restrictions placed on this demand by other social forces in the course of history. The difficulty is in fact an effect of the dual structure of neoliberal law, in which a regime of rights coexists with expansive sovereign exceptions grounded on security. Since the twin dynamics of movement-led opening and state-led closure construct the material field in which the conflict of values occurs, it seems utopian and dangerous to trust to one of the contenders – the state – to arrive at a fair ‘balance’.

Another legal scholar, Fenster (2011) suggests that WikiLeaks calls into question the meaning and effect of the suppression and disclosure of government information on a level more about power than law. With networked technologies creating an age of transparency, the relationship between government and citizens is changing. Fenster suggests that the information revealed by WikiLeaks is less important than the fact that government officials can no longer assume that their communications will remain confidential.

The WikiLeaks disclosures both represent and portend enormous changes in how secret documents become public, and in the meaning and extent of transparency in a wired, digital age. The celebrity suggests that disclosure matters – that, in some combination, the documents have enlightened the public, affected the ability of state actors to perform their jobs, and created risks for the ongoing efforts that the documents revealed.

(Fenster, 2011, p. 15).

In short, the rise of discloseability in a wired age portends changes in the balance of power between states and other actors – a recurring claim across all perspectives.

A particularly strong counterpoint to security perspectives in legal scholarship comes from those seeking to protect transparency, free speech and media inquiry from what they see as government censorship. For Benkler (2011b), there is no constitutional basis to prosecute Assange in America. The US government has overstated the dangers of the leaks, and the media has been complicit in this, engaging in self-censorship. Benkler likens the case to the Pentagon Papers release. He suggests that the attempt to single out WikiLeaks as a singularly irresponsible media actor distinct

from mainstream media is simply government rhetoric. He cites WikiLeaks' activities and media commentary on them as evidence that it is an instance of exemplary investigative journalism. In contrast, he calls for prohibitions of private operators' withdrawal of service to a target of government or public outcry, on the grounds that the present arrangement of privately-ran communication provision leaves dissidents vulnerable to what he terms "vigilante responses" by allies of the government.

'We Told You So': Sociology, Media, and Communication Studies

What is for statist a matter of loss of control in the project of protecting national security is for social scholars a matter of potentially emancipatory change. Scholars of diplomacy have a vested interest in the preservation of diplomatic records necessary to the pursuit of their own craft and, hence, in the availability of untainted records in 30 years, rather than instant records now and a risk of no records tomorrow. Scholars in other fields, in contrast, have found the WikiLeaks cables an invaluable source of data. Social scientists, particularly scholars in media studies and 'Internet and society', start from similar observations to other scholars: WikiLeaks emerges from digital social networks, and expresses a growing power of, and emerging culture of, digital networks counterposed to (certain forms of) state power. However, they are generally either sanguine or excited about the prospects for change, which this redistribution entails. To be sure, few of these scholars write purely from the side of Prometheus. Many are liberal-democrats, seeking to insert greater accountability, transparency and responsiveness to popular power into the existing system, or to bring it in line with new technologies. Nevertheless, their closeness to the Promethean flame, and ambivalence regarding the Order of Fate, are clear markers of their closeness to the networked, societal side of the WikiLeaks divide.

For instance, human geographers find the data revealed to be a treasure trove for mapping contemporary conflicts (O'Loughlin et al., 2010). Similarly, el-Said (2012: 1) suggests that the leaked cables show a 'bleak picture' of American imposition of intellectual property laws on the global South. He uses the WikiLeaks cables on the American-Jordanian Free Trade Agreement negotiations to reveal America's manoeuvres and agenda, with the US pushing on behalf of pharmaceutical lobbyists to impose their patents on Jordan, to the detriment of the Jordanian health system. El-Said's research on Jordan is echoed by Sarikakis (2012: 16), who shows that WikiLeaks exposed American lobbying for repressive anti-piracy laws in France and Spain. WikiLeaks has provided a valuable trove of data, which, due to its publicity, can be mined by academics as well as journalists and activists.

At the core of the media-communication debate, the broader issue of transparency versus privacy is a recurring theme. Citizen journalist Heather Brooke (2011) frames the WikiLeaks phenomenon as part of a wider information war in which grassroots activists challenge the control over information exercised by the ruling establishment. She suggests that this movement could determine whether the Internet empowers people or ushers in a new age of surveillance. Ludlow (2010) emphasizes the role of hacker ethics in WikiLeaks, particularly the idea of sharing information, and ridicules the posture of statist who seek an evil mastermind behind the organization. In contrast, Rosen (2011) frames the issue in terms of the death of privacy in an era of

enforced visibility. Arguably, this debate about values is something of a smokescreen for the real stakes, which are about diffuse versus concentrated power. It might be suggested that the values of transparency or secrecy are actually split: Neither state secrecy nor the transparency of social action to state surveillance are positive phenomena. Correspondingly, both individual anonymity, or small-group invisibility, and 'sousveillance' against the powerful are liberatory. The dispute's real stakes are not between two generic values applied in a classless way but rather, in a conflict between concentrated and diffuse forms of power.

Although many social scholars are interested in the revolutionary potential of new technologies, some are more interested in how this potential can be recuperated. From a citizenship and participation perspective, (Bruns, 2012) suggests that the 'self-organising community responses' shown by the Anonymous actions and WikiLeaks' mirroring project show the ability for networked groups to 'bypass or leapfrog, at least temporarily, most organisational or administrative hurdles' (p. 35). WikiLeaks is itself sustained by citizen-to-citizen connections, drawing on a sense of directly 'fighting the system' (ibid., p. 46). As befits someone interested in citizen integration, however, he is also concerned that the dynamic is 'too decentralised,' 'outside the social compact of society,' and lacking means for citizen–government negotiation (ibid., p. 47).

A key contribution to this debate comes from Benkler (2011), who argues that the Internet renders media more censorship-resistant, altering the power distribution among actors in an actor-network (p. 723). He suggests that the Internet makes actors such as WikiLeaks freer than they would otherwise be, which in turn constrains actors such as the U.S. government:

WikiLeaks can be said to be an exercise in counter-power, because it disrupts the organizational-technical form in which governments and large companies habitually control the flow of information about their behavior in ways that constrain the capacity of others to criticize them. (ibid., p. 728)

The Internet provided Chelsea Manning with information about the Army and a means to disseminate information, which gave her increased power (Benkler, 2011, p. 722). Alleyne's (2011) discussion emphasizes that WikiLeaks acted as a focal point for a global community of hackers and open-source activists, using methods that Alleyne emphasizes are hardly new and not at all reducible to the personality of Assange.

Furthermore, WikiLeaks can be 'seen as the pilot phase in the evolution toward a far more generalized culture of anarchic exposure beyond the traditional politics of openness and transparency' (Lovink, 2011, p. 177). Lovink views WikiLeaks as a small player in global affairs, which is nevertheless able to exercise power through media attention and spectacular revelations, bypassing the formal 'one-world' structures that bind most civil society groups into existing forms of state power (ibid., p. 178). He also suggests that the U.S. state is a relatively soft target, compared to more authoritarian or culturally diverse states, or to corporations. In retrospect, his argument holds considerable weight in light of the Snowden revelations in the summer of 2013. The structural difficulties with WikiLeaks stem from its position

somewhere between a mere conduit for data and a media agency selecting and publicizing content. Lovink also emphasizes the impact of 1980s hacker culture and problems with Assange's 'sovereign' role in the organization (ibid.). Against the image of Internet expansionists, Lovink suggests that statist are seceding from a previous libertarian consensus that kept regulation at arm's length. This is occurring because the outcomes of growing social networking are not what corporate rulers wanted (ibid.).

Network power now escapes the apparatus of power, much more than does traditional journalism (Castells, 2010). Attempts to shut down WikiLeaks by cutting its connections have failed because of the proliferation of mirror sites, showing the structural prevalence of freedom of information today. 'No security is at stake for states. At issue is the right of citizens to know what their governments are doing and thinking. Hence, the WikiLeaks affair is an instance of cyberwar between states and civil society' (ibid., paras. 6–7). In a later work, Castells (2012) embeds WikiLeaks in a broader account of technologically mediated social change. Observing that Internet use increases people's valuation of autonomy and also discussing the Arab Spring, Castells suggests that WikiLeaks is part of a broader 'mass insurrection against secret information'. What is important about WikiLeaks is the reaction against it, not WikiLeaks itself. This reaction is so excessive because WikiLeaks attacks the heart of contemporary power: control over information. The state–network conflict exemplified by WikiLeaks is what Balász Bodó (2011) understands as a manifestation of the counterpower of networks. 'The ability to place the state under surveillance limits and ultimately renders present day sovereignty obsolete. It can also be argued that WikiLeaks (or rather the logic of it) is a new sovereign in the global political/economic sphere.' Bodó suggests that the repressive response to WikiLeaks raises questions about how networked power can sustain itself when states attack. WikiLeaks was attacked through its connections to a world system vulnerable to statist and corporate intervention—its access to the global payment system, Web hosting, and use of the domain name system. This happened without any legal charges or due process. Network power still suffers from vulnerabilities relative to the state, and to state uses of networked power to their own advantage. Such vulnerabilities are already being addressed through projects such as the PirateBay plan to operate servers from mobile drones, the emergence of BitCoin, and the creation of radio-based Internet transmission to combat state blackouts. Bodó also repeats the criticisms of WikiLeaks' organizational model, which is clandestine and far from transparent, suggesting that it shares too much of its social logic with its adversaries and could be becoming a new sovereign. This reveals a possible tension between the hacker ethic and the goal of a public, networked world.

Despite this tension, Christofletti and Oliveira (2011) view WikiLeaks as the most potentially transforming journalism since the rise of Twitter and a part of a growing and irreversible trend. Analyzing it as a crossover between journalistic ethics and hacker ethics, they argue that it is a positive force for uncovering information in the public interest (ibid.). Chadwick (2011) uses WikiLeaks as a case study of an emerging hybridity between old and new media, which throws into question the separation of the two within media studies. WikiLeaks is part of 'broader networks of affinity' defined by 'libertarian hacker culture' (ibid., p. 17) and is best defined as a 'sociotechnical assemblage' (ibid., p. 21). Further, collaboration with old-media partners is used as a way to increase impact and recognition (ibid., pp. 24–25),

leading to a 'symbiotic' relationship to traditional media (ibid., p. 26). On the other side, traditional media used a custom search engine to mine the massive trove of data provided by WikiLeaks (ibid.). Chadwick also refers to constant attempts by journalists to boundary-police their relationship to WikiLeaks, falsely claiming to be more responsible or that WikiLeaks was 'just a source' (ibid., p. 35), claims which leave WikiLeaks vulnerable, in violation of older precedents of media rights (ibid.). In contrast, he argues that WikiLeaks 'occupies an important boundary space between old and new media' (ibid., p. 36).

WikiLeaks has also been cautiously welcomed in postcolonial studies. Yamaguchi (2012) argues that, before WikiLeaks, few scholars exposed the functioning of American state decision-making relative to its spaces of exception, suggesting that this is an effect of a pervasive Orientalism, which reinforces the construction of exception. It has also been noted, however, that the value of transparency is culturally relative (Southern Perspectives, 2011), while some leftist commentators have questioned the valuation of transparency over secrecy (Birchall, 2011). Discussing the impact on the Middle East, al-Karoui argues that the WikiLeaks phenomenon could only happen in societies, which place a high value on transparency. Nevertheless, it was framed through a false dichotomy of 'a tradeoff between the security of citizens and society on the one hand, and sacrificing transparency on the other' (p. 1). However, it should be noted that similar hacktivist methods *are* used in countries such as China and Iran, as ways to fight censorship. The similarities between these movements and the western campaign for WikiLeaks is shown by the support offered by hacktivist collective Anonymous to the Iranian 'green revolution' and the Arab Spring. Ironically, it was WikiLeaks that exposed Chinese hacking against the Dalai Lama (Simmons, 2011, p. 592), while another group, the Hong Kong Blondes, similarly disrupted Chinese networks in the 1990s (Ludlow, 2010). In short, the relationship between WikiLeaks, western values and 'transparency' is not as easily linked. The empowering effects of diffuse technologies for otherwise weak social actors are obviously not exclusively observed in western liberal democratic societies.

Conclusion

The receptions of the WikiLeaks phenomenon across (and on the margins of) academia are thus diverse, and reflect different subject-positions in relation to the eventual effects, both of the WikiLeaks phenomenon itself and of the broader redistribution of social power that it expresses and portends. The WikiLeaks phenomenon is a characteristic instance of an irruptive event that disrupts an existing power order. The reactionary response of statist seeking to preserve or restore a status quo ante manifests itself in a series of panicked outpourings calling for the restoration of order. In contrast, scholars sympathetic to emerging social networks—whether as a source of a revolutionary, peer-to-peer social alternative, a source of constraint on overempowered elites, or a source of energies and innovation to be exploited by capital—have embraced WikiLeaks as an expression of fundamentally positive changes. Internet and network scholars have been unsurprised at the phenomenon, which demonstrates the validity of their existing work on emerging forms of networked power, while media scholars have welcomed the new informational openness enabled by digital media.

Overall, then, what are the prospects that the Digital Prometheus can be unchained from the Law of Zeus? Ultimately, the persistence and expansion of networked power does not come down to the contributions of scholars. It is an effect of the innovations made by social movements and dissidents on the one hand and logistical controllers on the other. It can be questioned whether scholarly commentary can really do much more than interpret the forces at play, arguably aiding their recuperation. Nevertheless, different streams of scholarship are feeding rather differently into the balance of forces. While securitarian statist scholars provide a veneer of respectability to the repressive backlash, social researchers frequently contribute to the comprehensibility of the WikiLeaks phenomenon, inserting it in a wider social context and showing its wider social effects. By rebutting the statist hysteria, helping the transmissibility of emergent forces to new domains, reducing fear of the unknown, and showing the enormous positive potential of networked social forces, it is hoped that scholars can play a role in the process of unchaining Prometheus.

To conclude, this article was researched during 2010–2012 in order to understand the immediate impact of WikiLeaks in the relevant academic fields. Since then, Edward Snowden, by revealing the massive surveillance operations of the U.S. government, has opened further, and in a spectacular manner, the debate about ethics and privacy in cybersecurity and Internet governance, which earlier WikiLeaks inevitably forced on the academe. It is our view that this is healthy and vital, however many antinomies it generates, for academics involved in the debates explored here and elsewhere, to engage in debates with practitioners that could still unleash creative energies to a new world, where individual privacy is protected and where social justice, solidarity, and transparency are enmeshed in free, open, and inclusive social networks.

3.3 The ‘Arab Spring’ Uprisings

Gillian Youngs asked me to offer a critical analysis of the Arab Spring uprisings in 2011, which situates its digital elements within a historical, geosociopolitical and communications context for her book *Digital World Connectivity, Creativity, and Rights* (2013). I revisited my cyberconflict framework to seek support for such an analysis.

At the first instance, a cyberconflict perspective on the Arab Spring discusses the environment of cyberconflict. This would include situating the different countries ‘swept’ by the ‘Arab Spring’ in the world-systemic, *geopolitical and international relations context*, and the regional, and national socio-political and economic positions and relationships these countries have historically held. To put it simply then, to understand the impact of the similarities and differences and identify the common threads in the diffusion and spread of the uprisings across so many different settings, beside the obvious social media acceleration, diffusion and transnationalism hypothesis, which is offered relentlessly in the global mediascape.

A second cluster of issues involves the *political economy of communications* in each country, and particularly e-governance issues and digital infrastructure development. Arab Spring countries were in different stages of digital development. The regimes involved took different steps to cut the digital lifelines from the protesters. Digital

networked everyday media and social media networks were used in creative ways to connect the protest both internally and externally to international players, media actors and global opinion, and to plan and accelerate protest mobilizations, in line with previous empirical evidence in a long decade of academic scholarship in ICTs social movements and activism. And yet, the role of social media and digital networks were mediatised in the global public sphere as an unprecedented phenomenon. Here established *mainstream media coverage* of the events, the protesters and the governments involved is still relevant. For example, what ideologies, constructions of social and political identities, representations of and by protesters can be located, what is the level of regime censorship, alternative sources and media effects on policy, who is winning the political contest – the international buy-in, and how this is accomplished.

A major component of new media theory in conjunction with internet studies would also have to be employed to situate the tech/digital/online/cyber activism of the Arab Spring in the wider *history of protest, resistance and digital activism*. Here, there is need to place this Arab ‘digital’ resistance within wider networks of discontent and protest against the neo-liberal capitalist order in a time of global financial crisis. For example, the use of social media, and media movements/protests in Europe against austerity in Greece, Italy, Spain, Portugal and the Occupy movement assemblage). Inevitably, to ask questions about what type of democratization can occur in such a context. Indeed, the debate whether digital media were a cause or just a tool in the Arab Spring is a superficial one, considering a long history of online activism starting with the Zapatistas in the mid-1990s against neo-liberal capitalist expansions and accumulation by dispossession in an alienating hierarchical order operating on the social logic of state and capital. It is therefore critical to probe deeper.

Further, a cyberconflict analysis would involve a third cluster of issues employing social movement and resource mobilization theories: *the effect of ICTs on mobilization structures, organizational forms*, participation, recruitment, tactics and goals of protesters, as well as changes in framing processes and the impact of the political opportunity structure on resistances (the latter critical because of the ‘wave’ character of the diffusion of protests in different countries resembling Europe in 1989, where the window in the structure opened with the collapse of the USSR). Also, digital media and social networking as enabling resistance through *hacktivism* (or invariably termed digital, tech, cyber, network activism) and information warfare would have to be discussed in a variety of settings, especially in relation to media movements, ad hoc assemblages and collectives engaging during the Arab Spring (e.g. Anonymous cyberattacks in support for the uprisings). Lastly, in relation to *ethnic, ethnoreligious and cultural conflicts* occurring simultaneously with the uprisings, how group identities are constructed in relation to ethnic/religious/cultural difference or in this case also *gender difference*, and structural mapping discussed in the first instance above. This section concentrates only on a few of what are -- in my view -- the critical issues found in these clusters of cyberconflict analysis which might prove relevant to future theorizations of the Arab spring. Some of the threads left out can be equally critical, for example there was no space to delve into the Palestinian issue, which is at the heart of Arab concerns. Before delving into the analysis, a very brief description of the Arab Spring is required.

This so called Arab ‘awakening’ is the third of its kind with two previous occurring one in the late 1800s with Christians, parliamentarians and lawyers seeking to reform

politics and separate religion and state, while ‘the second occurred in 1950s and gathered force in the decade following. This was the era of Gamal Abdel Nasser in Egypt, Habib Bourguiba in Tunisia, and the early leaders of the Baath Party in Iraq and Syria’ (Ajami, 1 March 2012). As Ajami describes it, the political environment in the Arab world before the revolutions materialized was sterile and miserable, with consent drained out of public life and the only glue between ruler and ruled was suspicion and fear:

There was no public project to bequeath to a generation coming into its own and this the largest and youngest population yet And then it happened. In December, a despairing Tunisian fruit vendor named Mohamed Bouazizi took one way out, setting himself on fire to protest the injustices of the status quo. Soon, millions of his unnamed fellows took another, pouring into the streets. Suddenly, the despots, seemingly secure in their dominion, deities in all but name, were on the run.

Tunisians took central squares in Tunisian cities and Ben Ali fled into exile January 14 ending twenty-three years in power. His extravagant lifestyle and that of his family were documented in cables leaked earlier that year by WikiLeaks and were made available through media partners to a worldwide audience (prompted the ‘WikiLeaks revolutions’ mediatization). The summer of 2010 is when what I have called the Revolutionary Virtual began its rapid materialization. On the 25th of January protesters in Egypt took to the streets enraged by the death of a blogger in a mobilization organized by a Facebook site:

On 6 June 2010 Khaled Said, an Egyptian blogger, was dragged out of a cybercafe’ and beaten to death by policemen in Alexandria, Egypt. The cafe’ owner, Mr Hassan Mosbah, gave the details of this murder in a filmed interview, which was posted online, and pictures of Mr Said’s shattered face appeared on social networking sites. On 14 June 2010 Issandr El Amrani posted the details on the blog site Global Voices Advocacy (Global Voices Advocacy, accessed on 24 June 2011). A young Google executive Wael Ghonim created a Facebook page, ‘We Are All Khaled Said’, which enlisted 350,000 members before 14 January 2011 (Giglio, 2011, p. 15).

(Khondker, 2011)

Protesters took to removing Mubarak from office in sustained action for eighteen days and concentrated in Tahrir Square:

On February 11, Mubarak stepped down and turned power over to the army. Waves of protest continued to develop throughout the Middle East. After Tunisia and Egypt, protest emerged in Bahrain, Algeria, Libya and then Morocco, Yemen, Jordan, Syria as well as Lebanon, Oman and Saudi Arabia. Protest is still in motion in most of these countries...In addition, this succession of unpredictable revolutionary episodes took place in what Migdal (1988) would label “‘strong states and weak societies”’.

(Dupont and Passy 2011).

The different regimes, the support and opposition they faced were not similar and so the results of the uprisings were also diverse. In Tunisia an Islamist party took over, while in Egypt Mubarak was toppled and the military took over with protests continuing till in turn democratic elections occurred with renewed occupations of Tahrir in late November 2012:

Democracy is all very well, but how do you cope when the judges belong to the old regime, the army protects its privileged position, society is deeply divided, the Christian Coptic minority are up in arms, the more extreme Salafists are snapping at your heels and a constitution has still to be written?

(Hamilton, 29 November 2012).

In Libya foreign interventions helped the outing of Qaddafi. Unrest continues in various countries in the Arab world. Syria continues at the time of writing (late November 2012) to be in civil war – China and Russia will not approve intervention, while Israelis and Palestinians have had a week of war exchanging rocket attacks with dozens of people dead and the diplomatic community visiting Gaza eventually managed to negotiate a ceasefire. Remarkably, Palestine was also recognized by the United Nations as a non-member observer state.

Further, most countries saw Islamist parties take over. This in part can be explained by the loss of the population's trust in secular parties and the belief that religious parties are more ethical and not corrupt. The Islamic version of democracy is imported without Western liberal values, and rests on Islamic values (Interview with Cohen-Almagor, 19 November 2012). Islam and politics are seen as historically inseparable by those framing non-religious rule as illegitimate: 'The challenge of political Islam to secular modes of government is a recent phenomenon although it is presented by its advocates as a prolongation of an extended tradition in Islamic political thought' (Al Otaibi, M. and Thomas, 2011: 138).

Consequently, it is counterproductive thinking about democratization and rights in Western terms and the debates on liberalism, republicanism and deliberative democracy in contemporary political thought (for examples of these debates see Benhabib's 1996 volume on *Democracy and Difference*). In this sense, it is arguable that the Spring that brought procedural democracy with popular sovereignty, but with Islamic values, which continues for example to place women in the home and not welcomed in politics (more about this below), can be really thought of as similar to what is understood *normatively* as a Western style of liberal democratic politics. It is worth keeping this in mind for the subsequent analyses.

World-systemic, geopolitical and international relations context

A first question regarding the uprisings in the Arab world concerns 'the sudden surge and stiff resistance and demonstrations' in societies where there was fragmentation of grievances with multiple salient cleavages and the fact that regimes concerned were supported economically, politically and militarily by important allies, such as US, EU, Russia and China (Dupont and Passy 2011). Western governments reacted according

to with a prescribed protocol to deal with upheavals in repressive regimes they were backing up. Dixon (2011: 309) describes it like this:

With the US at the helm, high-level government officials urge ‘restraint on both sides’. When the revolts appear to be not so easily thwarted, they then call for reform. Tensions escalate and international media attention grows, the call for reform turns to an acknowledgement of the need for a new government.

As any Arab democracy in an unknown quantity (the concern being especially with popular vote going to extreme Islamist parties and the link to war on terror), Western governments are reluctant to risk security interests (Springborg 2011: 6). In the European Union policy sphere there is a struggle between being a relevant actor in the MENA region and being a simple spectator, due to the trained relationship between particular country and common interests, sub-regionalism and bilateralism vs. inter-regionalism and so on (Schumacher 2011: 108). Perthes argues for the importance of the political signal sent through these uprisings for Europe’s democratic market-economy model in relation to China and also points out that EU policies ‘betrayed the professed European values of freedom, democracy and the rule of law rather than exporting them’ (2011: 82).

However, when Western governments eventually accepted this new reality, this is where the appropriation of Arab revolutions begins by the Euro-Atlantic axis (Africa 2011, quoted in Dixon, 2011). Examples of such discourse is Obama’s address to Egyptians attributing the success of the revolution to their ‘ingenuity and entrepreneurial spirit’, while at the same time a more neo-conservative discourse even credits George W. Bush claiming that it was his policy which helped the regions’ democratic movements to flourish (Dixon, 2011: 311). A US assistance package with expertise to help involves:

(1) Microsoft will work with civil society groups to improve information and communications capacity; (2) the US Overseas Private Investment Corporation (OPIC) will support private equity firms and US–Arab business partnerships; (3) the administration is asking Congress to establish a Tunisian–American enterprise fund; and (4) business leaders and young entrepreneurs will connect through the US–North Africa Partnership for Economic Opportunity (Kaufman 2011 quoted in Dixon, 2011: 311).

Further, both Egypt and Tunisia were considered as examples of the neo-liberal reform agenda, and there is a direct link of the revolutions occurring against regimes, which were following that agenda (Armbrust 2011, cited in Dixon, 2011: 314). In the 1990s, the IMF led a bulk of structural adjustment programmes (Mackell, 25 May 2011). It is obviously myopic to think that the uprisings occurred just against corrupted elites: ‘Corruption is more than the personal wealth “stolen”, but rather is those in power and with connections enriching themselves through legalised processes of privatisation’ (ibid.).

It is tempting to think of the commonalities of the countries involved and treat the uprisings as a single movement, due to the diffusion and the domino effect of revolts against strong states by weak civil societies. It is worth entertaining this

argumentation in this section, to then be able to identify how the differences impacted the diversity of revolutionary outcomes. There are various examples of such analysis. Way (2011) for example compares the Arab uprisings to the revolutions and regime transitions after the collapse of communism in Eastern Europe. The conclusion drawn by Way in this comparison is that more autocrats will hang on in 2011, while where authoritarian collapse occurs they will be less likely to democratize than their European counterparts were: ‘authoritarian retrenchment in Bahrain, massive repression in Syria, and instability in Libya and Yemen—illustrate the paradoxical influence of diffusion in the absence of other structural changes’ (Way, 2011:17). Byman (2011) analyzing what the revolutions mean for the Israeli state, quotes an Israeli official as saying: ‘When some people in the West see what’s happening in Egypt, they see Europe 1989. We see it as Tehran 1979’. And it is not just Israelis, who have played the democratic card against their neighbors, who think that, it is also a view held by feminist movements and women political participation activists in the region. Women have been excluded from major decision-making bodies since the fall of Mubarak, and Isobel Coleman warns: ‘Arab women might soon be channeling their Iranian sisters, who have complained that Iran’s Islamic Revolution has brought them little but poverty and polygamy’ (Coleman, 20 December 2011). It is well known also that electoral authoritarianism regimes establish multiparty elections, to institute the principle of popular consent, while they keep subverting it in political life (Schedler, 2006).

Another factor beyond the obvious commonalities in the Arab countries where revolts were experienced beyond political repression, social media, youth unemployment and the domino effect (the opening in the political opportunity structure) is the matter of domestic food prices. Harrigan (24 May 2012) argues that the timing can be explained by the rising food crisis, and food security in the Arab world. This is also supported by Way (2011) in that high unemployment and rise of food prices fed mass-level discontent. And yet Way argues that in Tunisia and Egypt the countries experienced growth and their were robust enough to pay the police and soldiers. It is the nonmaterial values and ties, which will make these regimes robust. This shared ethnicity or ideology in a context of deep ethnic or ideological cleavage was not there to boost the legitimacy of the regimes (ibid, p. 20) and this is particularly interesting in terms of the globalization of values (more below).

In the next section, the media context of the Arab uprisings is discussed, in order to situate the discussion on the extent of the role of social media activism within the digital development and e-governance environment specific to each. Social media activism is looked at here in relation to the history of digital activism and resistance: ‘digital’ resistance within wider networks of discontent and protest against a neo-liberal capitalist order in a time of a global financial crisis; the effect of ICTs on mobilization structures, organizational forms, participation, recruitment, tactics and goals of protesters; changes in framing processes; the impact of the political opportunity structure on resistances; and hacktivism, cyberattacks in support of the protesters or crackdown over internet dissent by the authorities.

Digital development and social media use: Does technology guarantee revolution?

A second edition of the Arab Social Media Report released by Dubai School of

Government (<http://www.arabsocialmediareport.com>) offers empirical evidence on the importance of ICTs, and their political economy as an important factor in the Arab Spring uprisings. Facebook usage between January and April swelled in the Arab region and sometimes more than doubled, with the exception of Libya. These are some snapshots of important findings of that report to set the platform for this part of the discussion. Peak usage of Twitter and Facebook in the Arab region, the consumption of news through social media more than other outlets, the online acting as a barometer of the offline and vice versa, and efforts at censorship are the significant aspects here (Huang, 6 June 2011):

The most popular Twitter hashtags in the Arab region in the first three months of this year were “Egypt”, “Jan25”, “Libya”, “Bahrain” and “protest”. Nearly 9 in 10 Egyptians and Tunisians surveyed in March said they were using Facebook to organise protests or spread awareness about them. All but one of the protests called for on Facebook ended up coming to life on the streets.

During the protests in Egypt and Tunisia, the vast majority of 200plus people surveyed over three weeks in March said they were getting their information from social media sites (88 per cent in Egypt and 94 per cent in Tunisia). This outnumbered those who turned to nongovernment local media (63 per cent in Egypt and 86 per cent in Tunisia) and to foreign media (57 per cent in Egypt and 48 per cent in Tunisia). The flurry of tweets spiralled during the turning points of the uprisings. In Tunisia they peaked around the January 14 protest start date. In Egypt they spiked around February 11 when longtime President Hosni Mubarak stepped down. And in Bahrain they jumped in the days after the demonstrations began on February 14. The authorities’ efforts to block out information, the report said, ended up “spurring people to be more active, decisive and to find ways to be more *creative* about communicating and organising”.

Nevertheless, and rightly so in my view, other analysts of the Arab Spring do not see ICTs as a major catalyst for protest, even where multiple underlying causes are present (Stepanova, 2011: 2). Underdeveloped countries would be excluded from social media activism by default owing to underdevelopment and the lack of Internet access, such as Iraq and Afghanistan or other countries such as Myanmar and Somalia. Stepanova also found that no direct regional correlation can be traced between levels of Internet penetration and other IT indicators (such as the spread of social media networks) and proclivity for and intensity of social protest: ‘States with some of the highest levels of internet usage (such as Bahrain with 88 percent of its population online, a level higher than that of the United States) and states with some of the lowest levels of Internet exposure (like Yemen and Libya) both experienced mass protests’ (ibid.) In cases with low levels of exposure the cell phones, tweets, emails, and video clips were used to connect and transmit protests to the world. Different ICTs were used in different ways and social media did not outmatch satellite or mobile communications:

While the media utilized the term “Twitter revolutions” for the developments in the Middle East, identifiable Twitter users in Egypt and Tunisia numbered just a few thousand, and the mobilization role of micro-blogging as a driver of protests has been somewhat overemphasized, as compared to other ICTs, including cell phones, video clip messaging (such as YouTube), and satellite

television. (ibid., 3)

Khondker (676 or 66-7) also thinks that to overstate the role of the new media may not be helpful: 'Certainly, social network sites and the Internet were useful tools, but conventional media played a crucial role in presenting the uprisings to the larger global community who in turn supported the transformations. The new media, triggering mass protests'. Still, the difference that the images and films put on Facebook of two million users made to protest in Tunisia was great in contrast to protests in 2008 (then with only 28,000 Facebook users), which were not publicized and never reached a global audience. In the Tunisian case there were only 2,000 registered tweeters and only 200 were active (ibid).

Saletan (18 January 2011) does an excellent job in posing certain crucial issues in a report on the Future Tense Forum sponsored by Slate, Arizona State University, and the New America Foundation, where bloggers and activists from countries in turmoil, particularly in the Middle East, gathered to talk about how interactive media and social networks are influencing events on the ground. Here's the main points of his account summarized here and are worth exploring in further:

1. Technology doesn't guarantee revolution. Sometimes poverty impedes revolution by impeding access to technology.
2. The medium can lead to the message. Young people went online to keep up with their friends and youth culture. In doing so, they became politicized.
3. Online crowd dynamics mimic offline crowd dynamics.
4. The Internet facilitates repression, too.
5. Pressure causes adaptation, censorship creates activists who know how to circumvent control.
6. Geography matters, even offline (i.e. the use of neighbor countries systems to circumvent censorships)
7. Think small (cell phones, text messages, CDs, flash drives, Twitter—are critical to circumventing totalitarianism.)
8. Beware Animal Farm (i.e. who replaces the regimes and what type of democratization occurs).
9. Regimes can use the Internet to keep power the right way. (how the government can identify grievances online and address them).

On the first point, on technology and revolution, in terms of the stage of digital development and the impacts of use in varied political context and the issue of high or low use, Stepanova (2011: 3) argues that ICTs can have a more critical impact in countries where the regime has little or no social base. In the case where the regime has partial social support or legitimacy there are limitations on what social media can achieve. Stepanova also believes that 'for ICT networks to succeed, the younger, relatively educated generation, which represents the most active Internet-users, should make up not only the bulk of activists, but also a sizeable percentage of the population at large'. In this analysis the critical pattern with high social media use is the likelihood to have less violent protests, while where there is low or minimal social media use this corresponds with more violent escalations (ibid. 6).

On the second point of the medium influencing the message: how a young educated mass *produced* themselves to the point of organizing a revolution, while social media

brought together groups that would not collaborate in the offline world, and where there was no strong civil society, it was social media created a common thread (Howard and Hussain 2011: 41). This coming together in organized protests through internetted movements in rhizomatically organized sociopolitical networks has been historically a frequent occurrence in mass mobilizations since 1999 in Seattle with the anti-globalization movement. The use of social media and ICTs during the Arab spring was not a surprise for scholars of digital activism, hacktivism and cyberconflict. It is a well known empirically proven fact that ICTs and especially networked media have transformed organizational forms, enable the acceleration of mobilization, force transformation on framing and much faster grasp of the opening in the political opportunity structure.

It is not wise to look at the Arab uprisings in a homogenous manner, but since they were mediatized in the global public sphere as sudden, spontaneous unpredictable events, it is worth asking whether they were sudden and whether the usual 'elements usually associated with revolutionary processes (pre-existing networks, power fragmentation, cross-class coalitions, etc.)' were present. Another issue frequently brought up is how groups with such different values and contradictory ideologies, identities and strategies come together in a short period of time. Again this was the case with both with the global justice movement and especially relevant to the anti-war mobilizations in 2002-3, where diverse groups joined in protests without obvious ideological coherence or leaderships (ibid.). Again, this is not new and it is observed with the Occupy movement and other social media enabled protest movements. It is also known that 'the use of interactivity and networking on the websites contributes to micro-mobilization, and also to enhancing internal cohesion and bonding, rather than to building dialogic communication and solidarity online' (Moussa, 2011: 48). Different platforms accomplished different functions and suited for countries and societies in diverse digital infrastructures. During the anti-Mubarak protests, an Egyptian activist put it succinctly in a tweet: 'we use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world' (Global Voice Advocacy, 2010 cited in Khondker, 2011).

In certain respects, whether social media were a crucial factor or just a facilitating factor is not a question worth posing. For anyone paying half attention, it is obviously a key factor in transforming how social movements operate and it has been so over a decade now. To be posing this question again, only means that commentators will be asking it every time there is a revolution or a social media movement of any description, especially in the developing countries and its not meaningful as such for media policy or e-governance or advancing theory on the various literatures. Obviously suddenly knowing that others feel the same as you in their thousands and are willing to mobilize, having access to the information that the regime is weak and trusting the leaders of the protest to know that a potential mobilization will be successful is all bound to the use of social media to exorcise fear and uncertainty that a protest will not be met violently by the regime. This is the reason certain uprisings succeeded and others did not, and this is the reason why in Iran and China the regimes are still able to hold on to power.

Further, on the political opportunity and diffusion the type of questions to answer my employing elements of social movement and resource mobilization theory in the cyberconflict framework would be for future research the following:

Did ruling elites play a crucial role in opening up this window of opportunity? Were ruling elites divided and split into rival factions as was the case in communist East Germany? For example, Tunisia, Egypt and Libya were initiating power transition processes. Relatives of the strong men in power had been groomed for succession...Did these succession plans fissure the unity of powerholders and open up a breach for contenders? And what was the role of the army in these authoritarian countries? Did revolutionary episodes follow patterns of diffusion, and if this is the case what are the channels of this diffusion: networks and ties binding protestors across countries, traditional media such as Al Jazira, social and virtual networks such as Facebook or Twitter, or still other channels allowing for the spread of protest throughout the region? And what was diffused: action strategies, tactics to avoid repression, organizational models, symbolic action frames, or still other elements?

(Dupont and Passy, 2011).

Another factor in the success is that activists and their innovative use of technology and social media 'increased the potential political costs that the military would incur if it sided with the regime and violently attacked civil resisters. Since the whole world was watching, this type of crackdown would surely have elicited international condemnation and the potential end to diplomatic relations, trade agreements, and aid' (Nepstad, 2011: 490). Nevertheless, one problem with over-relying on the social media and ICTs as the crucial factor is ignoring crucial others, such the role of the military in influencing the outcome of a revolt. In fact, Nepstad (2011) argues that the military and its decision to remain loyal to the regime or to side with civil resisters played a critical role in shaping the outcomes of these Arab Spring uprisings. In the case of Tunisia and Egypt, the nonviolent movement won the support of the regime's military and achieved regime change. In the case of Syria, this was not so, and on top of Nepstad argues that 'if military personnel are comprised of different ethnic or religious groups that have unequal power relations to the regime, the likelihood that the military as a whole will side with the opposition movement is low', while when military defectors take up armed struggle against the state, 'the nonviolent aspect of the struggle will dissipate and the nation will likely slide into civil war (Libya and potentially Syria)'. Nonviolent disruption and discipline, meant that the military was more likely to side with the protesters, making difficult to shoot reasonable civilians with reasonable demands. Making social media absurdly the cause or the main factor in the uprisings, by terming them the 'Twitter, Facebook, WikiLeaks revolutions' misses important elements and treats them as homogenous protests bound on by the common thread of networked everyday digital technology. One of this, intersectional conflicts and afar more specific quest for rights is examined below.

Intersectional Conflicts and the Demands for Rights

In this last section, it is worth posing the question of how group identities are constructed in relation to ethnic/religious/cultural difference and also gender and class difference in intersectional conflicts occurring during the uprisings. For instance the already mentioned Gonen, one of the leaders of the Egyptian uprising, a Google executive for the MENA region left his home and swimming pool in an affluent neighbourhood in the Emirates to join the revolution. There are various class issues to be explored and in terms of who was leading the protests using social media and the digital gap/digital divide have less for example. Although this and the religious and minority factions and conflicts are worth exploring in the Arab uprisings, the focus in this limited chapter is unsurprisingly on women, pointing to the debate generated about women and social change and women's parliamentary participation (Al Otaibi, M. and Thomas, 2011: 139).

However repugnant the cases of female reporters raped in Tahrir square from UK, French and American media are obviously not the only reason to be concerned about the role of women during and after the uprisings. Examples of the military in Egypt carrying 'virginity tests' during a demonstration on March 8, International Women's Day, which 'attracted a few hundred women but was marred by angry men shoving the protesters and yelling at them to go home, saying their demands for rights are against Islam' (Coleman, 20 December 2011).

As it was mentioned earlier (Cohen-Almagor 19 November 2012), Islamic parties are proving the winners in post-revolutionary countries, as they are seen less corrupt, which means that is Islamic values with a certain view on the place of women in political life which would inform the new Arab democracies. The last decade the prejudices and discriminations are more pronounced among the younger generation of the voter sample. Al Otaibi (2008 quoted in Al Otaibi, M. and Thomas, 2011: 139) found in the case of Bahrain: 'This may be due to their being impressionable and thus easily influenced by religious extremists. It is noteworthy that an Islamic fundamentalist trend in terms of segregation and sectarianism has recently re-emerged in Bahrain'.

Ebadi has also argued strongly on this case questioning the term 'Spring': 'I do not agree with the phrase "Arab Spring." The overthrow of dictatorships is not sufficient in itself. Only when repressive governments are replaced by democracies can we consider the popular uprisings in the Middle East to be a meaningful "spring." (12 March 2012). A proliferation of Islamic parties might mean Islamic values informing Arab democracy in a way that will not necessarily improve the social and legal status of women in the Arab world. Ebadi encourages interpretations of Shariah law toward a conception of being a Muslim and enjoy equal gender rights, which can be exercised while participating in a genuine democratic political system (ibid.). She also recommends using legal tools such as the International Covenant on Civil and Political Rights, so in the case of Iran that 'the international community can play an important role in urging Iran to ratify the Convention on the Elimination of All Forms of Discrimination Against Women' while her recommendation is that 'Arab women familiarize themselves with religious discourse, so they can demonstrate that leaders who rely on religious dogma that sets women's rights back are doing so to consolidate power' (ibid.).

A lot of hope is placed on how the political changes across the Arab world in 2011

might result in radical social change of fortunes for women in politics and the role of social media as tools of liberation: 'The future prospects for women's representation in politics in Bahrain as elsewhere in the Arab world lie with such social media in the masterful hands of a younger politically-astute generation' (Al Otaibi and Thomas, 2011: 152). Nevertheless, Mohamed Ben Moussa who looked at websites used as tools of liberation in the Arab world, points out what is also true about digital activism in the rest of the world: its potential is always embedded within local and transnational power relations. The discourses and power relations are in turn always reproduced in the digital virtual environment. 'In traditional conventional religious cultures, women are perceived to be less qualified than men to run for, achieve and hold public office'... 'The reasons for women's disempowerment and male dominance are in his view three-fold: economic looting; sexual looting; and ideological looting' (ibid. 145). No matter how social media are mobilized and connect demands for rights in incredibly creative ways across the Arab world, these are residual structural factors and will remain hard to change, the fact that women 'score high as mothers and very low as political participants' (Mustapha Higazi, cited in ibid).

The short term picture is that this 'Facebook generation' has yet to create a political platform and indeed there is resistance in getting involved in institutional politics, with activists divided as to whether they should even be seeking to form or support institutionalised political parties. Springborg argues that 2011 will be more like the 1948 failed revolutions than 1989 and captures the critical issues. It is worth quoting in full here:

How the globalised Facebook generation can convince large numbers of struggling Egyptians that their economic needs and demands can be addressed more effectively through democratic institutions than through access to patronage in an authoritarian system, remains to be seen... The poster children of the Arab Spring, Tunisia and Egypt, do not seem well equipped to imitate the success of Eastern European countries following the collapse of communism. The context in which Egyptian reformers are seeking to democratise their country is not nearly as conducive as was that in say Poland, largely because the security concerns of global and regional powers are thought by them to be better served by at best a very cautious, tentative democratic transition.

(2011: 12).

More optimistically, in what is a ground-breaking account using Deleuzo-Guattarian logic to theorise the interplay of digitality, orality and cultural diversity, Alakhdar (2012) argues that the kind of connectivity of the online world does not have to reduce cultures into one singular form. Rather, the internet has the potential to promote traditional cultures as much as it promotes market culture. Reinventing spaces, these *producing* e-immigrants and e-nomads, 'take energy and flow from their real lives, expand and negotiate their cultures online then borrow from it to re-assemble their real worlds'. And elsewhere: 'Islamic cultural interaction online revitalizes the goal of global connectivity known of Islamic traditional culture' (221). And still the questions remain what happens to cultures that are not *produced* online and 'how far are traditional cultures themselves rhizomically open for development

across speed and mobility?’ (ibid.).

This perspective and these questions are critical in understanding the long-term of networked everyday media in the Arab world and their importance, not as a trendy tool which overtook the MENA region like a storm, as the mainstream media would have it, and premediating not only in manipulating populations (Grusin 2010), but also as creating spaces of peace enabling political and social transformation in these societies, initiating a creative discourse which links for example Islam to civil, human and gender equality rights discourses.

The Arab uprisings are occurring at the same time as protests and massive mobilizations against austerity measures in Southern Europe (Greece, Italy, Spain, Portugal), in which digital media and activism are recognized as key facilitating factor and have been recognized as such (but not the cause of mobilization) since 1999 with cyberactivism on Seattle, the anti-Iraq war mobilizations, and now the Occupy movement has spread around the globe in a postnational demand for reform in radical opposition to transnational corporate control of politics, economics and society. The so-called Arab Spring and accompanying media movement, is part of this story, even if the demands had a ‘patriotic’ and nationalist character (i.e. ‘We are not traitors financed by foreign governments, we want to save country from corrupt elites’ type of discourse), which mostly did not link directly to anti-capitalist movements and resistances.

In the next section, I examine digital surveillance ideology in relation to the Snowden leaks, in order to nuance the politics, traditions, 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. *These trusted global networks comprised by governments, corporations and international organizations seem to have the mandate, or plain and simple the monopoly of planning power, to represent the interests of citizens/consumers in the global networked public sphere. I argue that there is an ideology of the Centre of the political spectrum in combination with elements of centralized network surveillance complex ‘collect-it-all’ ideology, which form a quasi-totalitarian ideology at work in societies of liquid surveillance and control, by examining specific empirical examples directly drawn from media reports of the Snowden revelations. This study was prepared for a special issue of the Journal New Formations (the final journal published version was later co-authored with Martin Gak. I only include here my first original version, as this was prepared for this book).*

3.4 The Snowden Affair

‘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 Director of the Government Communications Headquarters (GCHQ), UK (Moore, 11 October 2014).

While public concern is continuously rising over surveillance and control (Associated Press-NORC Center for Public Affairs Research, 2013), governments and tech elites blame each other for the loss of trust by the public in relation to their handling of privacy and surveillance of network communications. The NSA programs were put in

place for seven years without any public debate of any kind. The Obama administration justified the agency's programs by claiming they have been crucial to 'successes' in counter-terrorism. The debate is happening for the first time since 9/11 and it is a debate on what affects rights/liberties and freedoms in the digital age, and which subsequently has become a crusade in defense of democracy and constitutions in place to protect people from unreasonable searches and seizures unless there a warrant. This was the frame offered by The Guardian, which led the media reporting of the Snowden leaks, starting with the Laura Poitras/Glenn Greenwald famous video interview with Snowden in Hong Kong. In the trade off between privacy and security, governments argue for the need for secrecy to protect the public against terrorist and criminal networks, while civil society organizations advocate transparency and open access-enabled deliberation and oversight of the processes involved. Meanwhile, tech elites pronounce exasperation with their own relationship to governments and project their own need to protect their customers' privacy, in order to guarantee their own income flows and their reputation as socially responsible corporate actors.

Within this disastrous *ménage à trois* of "trusted" global networks, which have the mandate, or plain and simple the planning power, to represent a bastardized citizen/consumer, it is still the individual that has to solve their information communication problems in relation to privacy and surveillance. It is the individual that has to buy their digital equipment, access and literacy in form of consumption, education and training. And, it is the individual who has to acquire skills and software to protect their privacy in digital homes built by tech elites and surveilled by governments (for security) and corporations (for profit). This paradoxical conundrum places the individual citizen/consumer in the impossible situation of 'hack or be hacked', which inspires the rationale for this analysis.

If the individual is controlled in their digital pursuits by monopolized and centralized surveillance, they will always be controlled, unless their purpose of communication is always declared in a specific manner. And yet, the global middle classes mostly believe that digital communication matters only affect personal or professional enterprise and they do not interfere with basic values of life. Nevertheless, Wacquant points to the 'desolidarizing' impacts of 'synoptic' surveillance (where the many observe the few) and 'lateral' surveillance (where people and neighbours watch each other) (Wacquant, 2008 cited in McCahill and Finn, 2014).

Against this background, I am inclined to follow Hayek's argument on economic control and totalitarianism. Only in this case, I argue that it is digital control and *the assumption that it does not affect freedom*, which mirrors his argument about economic control. To demonstrate this point, I shall resort to crude sensational measures, by replacing his *economic* (freedom) with *digital* (freedom) and in all other instances:

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.

(Hayek, 2007: 127)

Further, it is the unchecked power of “digital planners”, the tech corporate and deep state digital order that is really the crux of the matter in the discussion of societies of control. The recent Snowden leaks and Assange’s WikiLeaks provide significant evidence in hundreds of thousands of documents, that there is what resembles a *U.S. led transnational authority comprised by global trusted networks* presently directing surveillance of digital networks almost in their entirety, and that it does involve the collaboration, albeit protestant, of transnational corporate tech elites. The power over information and communication this authority can master, due to monopolized surveillance is nothing less than *control over both digital consumption and production, and this at a global level*. (Shirky, 2011; Fuchs, 2011; Castells, 2012; Harvey 2012; Lovink, 2012). Currently, the global citizenry is at the mercy of these digital planners.

Nevertheless, I would argue, what is of interest is not just the power and resistance to these digital planners, but *the specific type of ideology* used to justify both the power and the source of this power over information and communication via surveillance, as well as the relentless governmental crackdown on movements in favor of transparency and advocacy of new alternatives. The reason I think this is an urgent discussion to be had is that academic debates over surveillance are restricted to worthy, but often isolated disciplinary areas, which do not nuance specifically the ideology of digital surveillance. For instance, McCahill and Finn (2014) examined surveillance in settings as diverse as migrants, protesters, school children, individuals under probation and pointed to *surveillance capital*: Subjects utilizing everyday tacit knowledge developed through their engagement in power relations to challenge this power, which provides subjects with enhanced agency in local contexts and settings. These authors argue that targeted individuals and groups in surveillant assemblages:

...have the police knock on their door after they have been seen ‘out and about’ on camera in areas where crimes have been reported that fit the surveillance profile; they are followed by security guards who ask to see their money before granting them permission to enter the shopping mall; they have their emails read by the police and telephone calls intercepted by the authorities; they are regularly pulled out of the queue at the airport and questioned by the authorities; and they have their performance monitored by the management as they work ‘on camera’ when patrolling the shopping mall. (ibid, p.9)

There is nothing new about that. Surveillance might prove empowering by this use of surveillance capital, whereby ‘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”. (ibid. 80) This is consistent with Foucauldian notions of resistance against the microphysics of power in the everyday (McNay, 1994).

Although McCahill and Finn provide via Bourdieu (2005) a new theoretical frame termed surveillance capital, there is demand to understand technosocial agency in broader theoretical and philosophical discussions. New materialist accounts drawing from recent theories of affect and embodiment, posthuman-influenced materialisms, accelerationism, postmodern critical theory, and critiques of network theory, explain individual human agency as a nexus of overlapping and often competing subjectivities within the context of technologically distributed agency (Karatzogianni and Scandorf, 2014). This is a significant philosophical and theoretical development, which cannot be left out from discussions of surveillance and privacy in digital networks. Indeed, Berardi, in his doctoral defense recently spoke of ‘neuro-totalitarianism’ as an explanatory frame of a new species in the societies of control (Lovink, 24 October 2014).

I introduce the term ‘quasi-totalitarianism’ to explain how technosocial transformations of agency should enhance a civil type of association inspired by radical democratic politics to counter enterprise association dedicated to profit making and securitization in the digital public sphere. I then proceed to support this frame with specific empirical examples from the Snowden documents, reports of those documents by diverse media, and opinion expressed over the balancing act over privacy and surveillance in the digital public sphere.

Quasi-Totalitarianism of the Centre

Despite ethereal and postmodern conceptualization of digitality of utopian and dystopian creed, the old modernist demands for power, participation and democracy still hold currency, while race, gender, class and other hierarchizations are produced and reproduced in digital networks. It is therefore poignant, to identify the “older” more traditional ideologies driving the surveillance complexes in the United States, the UK and elsewhere, as well as countries where different political systems are in place, for example in China, Iran or Russia. In that sense, my argument is that as far as tech corporate and government elites are concerned, there is an indication of an emergent *quasi-totalitarianism* in relation to digital surveillance, which resembles certain elements of historical totalitarianism, however cannot be called ‘totalitarian’, as defined by leading scholars in the field of totalitarianism and the intricate matrices of debates therein. Nevertheless, I am using the term quasi-totalitarianism of the centre as a concept within a genealogical continuum to historical academic and political discussions about the totalitarian left and the totalitarian right, as well as authoritarianism and despotism (Fascism, Nazism, the Soviet regimes, semi-peripheral dictatorships in Latin America and the MENA region, post-totalitarianism and so on) (Arendt, 1951; Friedrich and Brzezinski 1956; Talmon, 1961; Rupnik, 1988; Siegel, 1998; Žižek, 2011).

Within the context of these debates, the term ‘quasi-totalitarian’ I introduce here, fits better with the surveillance ideology in contemporary times, because it explains the resemblance of the collect-it-all practices of the governments and corporate actors to historical practices of the past, without trivializing the horrific historical experiences of totalitarianism, which ranged from mass murder to totalistic control of the thoughts and actions of a country’s population under specific historical regimes.

Moreover, on another level, the quasi-totalitarianism of the centre, points to the “Centre” of the ideological spectrum. Traditionally, the centre has been occupied by liberals and social democrats of some description or another in democratic systems. Nevertheless, I would argue the ideological centre in non-democratic states is in turn the ideological centre in the specific spectrum of the political culture in country-specific contexts. The quasi-totalitarianism of the centre refers here to a second layer in relation to centralized hierarchical organizations, even if they are networked, as the sociopolitical logic remains hierarchical despite the use of network communications. The centers of digital planning and of surveillance networks are steeped in an ideology which is quasi-totalitarian in character, but obviously not the historical totalitarian left (communism) or totalitarian right (fascism) instantly recognizable as historical events, regimes, political practices, or a way of total politicization of everyday life.

This is exactly why liberals and social democrats, parliamentarians and others in the Western ideological centre find it preposterous a suggestion that ubiquitous surveillance (the digital planners’ control over global networks) is a totalitarian practice. It is because, the ideological centre is blind to this simple fact: *The ideology of the planners, whoever they happen to be is directly drawn from the ideological centre of the political system they have emerged from and which they now operate.* 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 believe 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.’ (Hopkins, 6 October 2013). I argue that there is a new form of ideology emerging: that of the *collect-it-all centre*, a hybrid of the traditional ideological centre infected by the centre in the form of centralized networks of surveillance complexes. This ideological hybrid 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.

Zóon Politikon: Edward Snowden and Human Conduct as Civil Association

In the context of intensely networked societies, it is no longer enough to mobilise constitutionalism and representative democratic politics against the control of big data and digital network infrastructures by state and corporate actors. It is obvious, that the digital network war machine is entangled within both state and corporate-controlled network environments. This type of contemporary critique (i.e. Terranova, 2003; Wark, 2004; Benkler, 2011) traces back to authors such as Deleuze and Guattari (1987), Foucault, Marx or the situationists. It is also a critique, which is widely accepted by key actors in the anti-surveillance, freedom of information, and

transparency-related movements. For a “Network *res publica*” to function without resorting to closed, fixed, surveilled and censored networks based on the reactive affect of biopolitically controlling/ed subjects and the micro-targeted commodification of desire, it is critical to understand how human conduct is affected by the network form.

To that effect, I use these modes civil versus enterprise association to differentiate human conduct in network societies by reconsidering Oakeshott’s ideas in *On Human Conduct* (1981), because I think that 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. As Terry Nardin (2001) explains: ‘The idea of civil association as association on the basis of agreed laws addresses this problem. The state as a legal order provides a procedure for adjudicating interpretive disputes, and in a state that is understood to be a civil association that procedure is concerned with legal rights and duties, not with promoting substantive goals.’

In other words, whereas the market is about economic growth, civil association is about restraints on arbitrary power. The danger as Noel O’Sullivan (2012) explains does exist, because of ‘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’ (p. 310). Despite extensive criticism from all ideological sides on Oakeshott’s political heritage, O’Sullivan also points to how radical thinkers like ‘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’ (ibid. 306). 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’ (ibid. 296).

Commensurate with this argument, I argue here that Edward Snowden in his leaks of hundreds of thousands of National Security Agency documents conducted himself specifically against enterprise association in the form of complete structural acquisition of data from private individuals and organizations both by governments, but also tech elites and international organisations, the disastrous *ménage à trois of “trusted” global networks. The affective response to Snowden’s ‘Let us put surveillance to public scrutiny’ from Anonymous -- a new vigilante formation in global politics fighting against surveillance, censorship, injustice, and resistance in favor of solidarity to movements fighting against repressive and authoritarian*

governments -- shows quite poignantly how Snowden's revelations were received by movements working against 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%. (<http://revolution-news.com/anonymous-releases-private-nsa-documents/>)

According to one of the main media organisations Snowden collaborated with, The Guardian, Snowden revealed NSA's Prism, which, according to the Snowden documents, is the biggest single contributor to its intelligence reports. It is a 'downstream' program, which means the agency collects the data from Google, Facebook, Apple, Yahoo and other US internet giants. One slide claims the agency has 'direct access' to their servers, but this has been hotly disputed by the companies, who say they only comply with lawful requests for user data (The Guardian, 1 November 2013). Snowden also leaked the existence of Tempora, a program established in 2011 by UK's GCHQ that gathers masses of phone and internet traffic by tapping into fiber-optic cables. GCHQ shares most of its information with the NSA. The documents, which are reportedly marked top-secret, come in the wake of other high-profile disclosures attributed to Snowden since he first started collaborating with the paper for articles published beginning June 6 2013. The United States government has since indicted Snowden under the Espionage Act, he requested asylum from no fewer than 20 foreign nations and ended up in Moscow, as the Putin regime, ironically obliged to provide him with asylum.

The relationship between NSA and tech giants is a paradoxical one indeed. Again according to *The Guardian*, from June to July 2010, data from Yahoo generated by far the most NSA intelligence reports, 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. Facebook, where the typical user has 190 friends, shows how three degrees of separation gets you to a network bigger than the population of Colorado. According to internal documents cited by the journalists, Microsoft 'developed a surveillance capability' that was launched "to deal" with the feds' concerns 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' **RT. (11 July 2013).**

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) (Huet, 11 July 2013). 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' (Poitras et al. 1 July 2013)

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' (Rushe 12 September 2013).

The public appearance of tension, whether this is actually real or presented as such in the public sphere, either way points to decision making outside democratic politics, because it involves back-channel negotiations between state and corporate elites, under secrecy, as the tech corporations are not allowed to divulge information about requests made by the NSA. That would be treason, which makes Meyer's quote all the more important. 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 rulings on Section 215. 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.

There are two more areas, which are pointing to quasi-totalitarianism beyond this bizarre relationship between state and corporate elites. The first is at the level of International Relations and global politics and the second involves the role of investigative journalism in holding governments accountable. Let us take those in turn.

There is a matrix whereby governments are not allowed to spy on their own populations but they can spy on another nation's as they are defined as 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. (Reuters 30 June 2013).

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' (Schow, 1 July 2013). 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' (Augstein, 16 July 2013). An explanatory analysis of why this might be the case points to a division of duties and at times extensive cooperation among the intelligence agencies in the Western world: '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' (Poitras et al., 1 July 2013).

In contrast to European reactions, Brazil's Rousseff cancelled an official meeting with Obama and at the U.N.'s General Assembly called on other countries to disconnect from U.S. Internet hegemony and develop their own sovereign Internet and governance structures, because NSA rules also impose geo-locational-based jurisdictional mandates (based upon the route of your Internet traffic or the location of the data services and databases you use). This would infringe on 'Article 19 of the Universal Declaration of Human Rights—protecting the right to freedom of opinion, expression, and the opportunity to participate in the information society—is at risk.' (Meinrath, October 2013).

Besides the lukewarm reaction to the revelations in Europe, based on the Western intelligence argument, i.e. it is accepted that governments and populations between allies will be spied upon routinely, justified by 'war on terror' requirements, another critique is truly relevant to the quasi-totalitarianism frame I am proposing. This involves the Iraq war legacy in the American deep state. 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: "At the time, more than 100 teams of US analysts were scouring Iraq for snippets of electronic data that might lead to the bomb-makers and their hidden factories. But the NSA director, Gen. Keith B. Alexander, wanted more than mere snippets. *He wanted everything: Every Iraqi text message, phone call and e-mail that could be vacuumed up by the agency's powerful computers.*" Rather than look for a single needle in the haystack, his approach was, *'Let's collect the whole haystack,'* said one former senior US intelligence official who tracked the plan's implementation. *'Collect it all, tag it, store it. . . . And whatever it is you want, you go searching for it. . . . 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'* (Greenwald, 15 July 2013).

McCoy writing about the making of the American surveillance state similarly writes about the operational mentality of Keith Alexander in the following way:

During a visit to a GCHQ facility for high-altitude intercepts at Menwith Hill in June 2008, NSA Director General Keith Alexander asked, "Why can't we collect all the signals all the time? Sounds like a good summer project for Menwith." In the process, GCHQ's Operation Tempora achieved the "biggest Internet access" of any partner in a "Five Eyes" signals-intercept coalition that, in addition to Great Britain and the U.S., includes Australia, Canada, and New Zealand. When the project went online in 2011, the GCHQ sank probes into 200 Internet cables and was soon collecting 600 million telephone messages daily, which were, in turn, made accessible to 850,000 NSA employees

(McCoy, 15 July 2013).

Houston writing at The Economist, which is not of the Popular Resistance ideological variety as is the origin of the previous quote, nevertheless again similarly writes:

What kind of message are we sending about the viability these democratic ideals—about openness, transparency, public participation, public collaboration? How hollow must American exhortations to democracy sound to foreign ears? Mr Snowden may be responsible for having exposed this hypocrisy, for having betrayed the thug *omertà* at the heart of America's domestic democracy-suppression programme, but the hypocrisy is America's. I'd very much like to know what led Mr Obama to change his mind, to conclude that America is not after all safe for democracy, though I know he's not about to tell us. The matter is settled. It has been decided, and not by us. We can't handle the truth

(Houston, 9 July 2013).

The Atlantic responded to Obama's surveillance speech with equal frustration about his justification of NSA activities, which included references to open debate and democratic process:

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."

(Friedersdorf, 12 August 2013).

The third area pointing to quasi-totalitarianism, beyond the collaboration/conflict relationship with tech companies, and the Western matrix of intelligence enable collect-it-all targeting of millions of records of data of various countries' populations is the impact of the Snowden revelations on journalism overall. It is rather obvious that smashed servers in *The Guardian's* basement is not the flagship product of a democratic state and it rather *resembles* historical totalitarian practices (in Nazi Germany it started with the burning of books and it finished with the burning of people). The detention of Greenwald's partner by the authorities was yet another melodramatic knee-jerk reaction by the UK government, which needs to appear to pull its weight in the special relationship.

The most significant support for the quasi-totalitarianism frame I developed in the first part of this section is the explanation offered by Edward Snowden himself. Snowden's flight to Hong Kong and then Russia and his subsequent asylum there to be joined by his pole-dancer awesome girlfriend does seem a storyline taken out of a James Bond movie or a Hitchcock plot behind the Iron Curtain during the Cold War. And yet, it is worth examining the target of his conduct and his professed ideological enemy. This is how his statement at Moscow's Sheremetyevo International Airport was reported:

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"

(Davidson, 16 July 2013).

To conclude, this section introduced the term 'quasi-totalitarianism' to explain digital surveillance as leaked by Edward Snowden to the global mediascape. The resemblance (quasi), but not the reality of historical totalitarianism, is based on the following elements, which the argumentation supports: a. the monopoly of digital planning on surveillance rests on back-channel secret communication between government and tech corporate elites; b. enterprise association politics ensures that the dual goal of state (security) and capital (profit) continues unabated and unaccounted for; c. at the very least there is a Western intelligence matrix of surveillance of unprecedented proportions in the form of total structural data acquisition; d. journalists, whistle-blowers and transparency movements are prosecuted in the clumsiest manner possible resembling historical totalitarian practices of the past; e. there is significant anger and frustration not just from the usual organizations fighting for digital rights and freedom of information and privacy, but also by the public about the infringement on civil liberties, against what is currently resembling (i.e. quasi) totalitarianism. Our redeveloped study of the Snowden revelations with Martin Gak also includes the cooptation of advocacy and NGOs accepting donations from government and industry in this area of work (Karatzogianni and Gak, forthcoming.)

The case studies we looked at so far show that where there is digital materialisation, the Real follows suit, so in the defense of civil association politics in the digital public sphere, the quasi-totalitarian practices of enterprise association style politics, conducted by global trusted networks (state, capital, coopted civil society) and led by the United States, has to be seriously reconsidered.