Chapter 26 — Leaktivism and its discontents

Athina Karatzogianni

Introduction

With the appearance of Anonymous and WikiLeaks from 2006 onwards, the past decade has witnessed the unstoppable acceleration and proliferation of what has been as a form of whistleblowing plugged straight in to twenty-first century, information-age global politics: what Micah White (2016) dubbed 'leaktivism' and Gabriella Coleman (2017) called 'the public interest hack (PIH)'. Between 2015 and 2017, the DNC Leaks, DCLeaks, and the Panama Leaks follow the trend set by WikiLeaks (Brevini et al. 2017) to global prominence in 2010, and Edward Snowden (2013) as significant examples of what is fast becoming the decade of 'leaktivism'. In normative terms, the 'internet' is used to obtain, leak and spread confidential documents with political ramifications, with the aim to expose corruption, wrongdoing and inequality, potentially enhancing accountability in the democratic process, through greater transparency. Coleman provides a typology and then an excellent brief genealogy of this in 'The Public Interest Hack' (2017) in the *Hacks, Leaks and Breaches* issue she co-edited with Christopher Kelty for the journal *LIMN*, exploring 'how are hacks, leaks and breaches transforming our world, creating new collectives, and changing our understanding of security and politics' (Coleman and Kelty 2017).

The purpose of this chapter is certainly in the spirit of that exploration, but in this case focusing on the politics of specific instances of leaktivism. Providing typology, overall history and in-depth empirical cases is not in the scope of the discussion here. They are sure to be analyzed and published in the extensive academic scholarship of the future. Here I want to point to central issues and themes in leaktivism, which emerged in the examination of cases

in my own scholarship (Karatzogianni 2015), in order to cut through the fog of vast amounts of knowledge generated by information from large volumes of empirical data. This approach could zoom directly into the core themes and debates they bring to the fore, or are likely to dominate on the politics of digital media, and in turn, the impact of digital media on global politics.

Transparency versus secrecy, openness versus control

Data leaks bring out new information in an accelerated hybrid media environment; however, the ethical and ideological debates, tactics and targets of leaktivism are by all accounts: not new at all. The demands, tactics and politics of whistleblowers, leaktivists, or public interest hackers are as old and modernist as politics back in the twentieth century, if not before: transparency, participation, power, democracy, equality, anti-corruption, reform, revolution, insurgency, propaganda, information warfare, espionage and so on. Nevertheless, these actors are operating in a highly hybrid media environment, which is unprecedentedly vast, voluminous, networked, global, and moreover corporatized and controlled by global trusted networks (Karatzogianni and Gak 2015). A case in point, the biggest leak so far: Panama Papers, or, as was later adopted after protests from the Panamanian government, the Mossack Fonseca Papers (released 2015), belonging to the law firm and corporate service provider Mossack Fonseca, involves 11.5 million leaked documents and 214,488 offshore entities. An activist calling themselves 'John Doe' leaked the papers to Bastian Obermayer from *Süddeutsche Zeitung* (SZ) and explained his motivation was inequality and the injustices their contents described. SZ asked the help of the International Consortium of Investigative Journalists (ICIJ), and eventually 107 media organizations from 80 countries collaborated to bring stories out starting from spring 2016. In terms of size at 2.6 terabytes, this is the biggest leak historically. It is also yet another example (with the WikiLeaks and Snowden affairs) of the transformations that journalism is undergoing in terms of

extensive use of data software tools and the transnational collaboration involved. One needs to read minimum of a hundred pages before grasping only a very basic understanding of actors, relationships, and elites in the countries involved in the truly vast amount of documentation leaked (https://panamapapers.icij.org).

Although the Mossack Fonseca is in terms of size the biggest leak in history, implicating elites around the globe, to my analysis undoubtedly the most visible and continuous impact in the arena of cyber conflict and global politics is from WikiLeaks especially starting from the 'Collateral Damage' video in the summer of 2010 (on WikiLeaks's ideological and organization conflicts and the politics of emotion see Karatzogianni 2012). We found in examining scholarship between 2010-2012 (Karatzogianni and Robinson 2014), that in international relations (IR) and related disciplines, including diplomacy studies, 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. In disciplines more closely aligned to the social such as culture, media, communication studies, and sociology, the major debate is between *openness* versus *control*: here, issues include the relationship between WikiLeaks and the hacker ethic, the constraint of overwhelming state power, the emergence of a global digital 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 and their use of ICTs. These differences emerge for a particular reason: the framing of the state–network conflict through the gaze of the state, or from an interpretive standpoint framed by the attempt to understand the social: the people's standpoint.

The two debates, transparency versus secrecy and openness versus control, tend to dominate discussions on leaktivism throughout the WikiLeaks saga and polarize transnational publics, even providing one of the first example of

affective politics and the polarization of global public opinion over both the organization, and particularly the radically opposite significations and outpour of emotion surrounding Julian Assange as hero or traitor, in mobilizations and petitions in support of his release by a wide network of actors, and even in products of popular culture such as films, books, and documentaries (Karatzogianni 2012).

The following section illustrates how these two core debates (secrecy versus transparency and openness versus closure) influence the framing of ethics and tactics, and produce unintended consequences for actors and relationships surrounding leaktivism. To illustrate my argument, I refer to DCLeaks, and WikiLeaks' DNCLeaks and CIALeaks. These specific empirical examples are chosen, because there is a consistent thematic on intelligence, secrecy and transparency, democratic accountability, propaganda and sabotage in global politics involving prominent actors in the United States and Russia, as well as proxy countries across the East-West Cold War axis.

Key leaks 2016-17

DCLeaks

DCLeaks broke out in June 2016 with leaks of military and government emails in the United States, which the American intelligence community and private security firms attributed to Russian intelligence undermining the 2016 US elections. DCLeaks' purpose as stated on their site is 'to find out and tell you the truth about US decision-making process as well as about the key elements of American political life', while they describe themselves as 'the American hacktivists who respect and appreciate freedom of speech, human rights and government of the people' (dcleaks.com).

The leaks involved three hundred emails from Republican targets and information about two hundred Democratic party targets. Portfolios included Bill and Hillary Clinton, DNC official William Rinehart, former NATO commander General Philip Breedlove and a Democratic Party-linked PR professional called Sarah Hamilton. US Gen. Philip Breedlove, who had already retired and was formerly the top military commander of the North Atlantic Treaty Organization, emails from his personal account show him complaining that the Obama administration wasn't paying enough attention to European security particularly in relation to Ukraine. Breedlove told CNN that the emails were stolen as part of a state-sponsored intelligence operation.

Self-defined on their website as 'DCLeaks is a new level project aimed to analyze and publish a large amount of emails from top-ranking officials and their influence agents all over the world' (https://twitter.com/DCleaks_?lang=en). Initially it was thought to be a right-wing political-opposition researcher outlet and not hackers/hacktivists, because of how the site and its digital structure were set up. However, in subsequent analysis what dominated global media discourse is that it was another front being used by Russian intelligence. Analysis from cybersecurity firms linked DCLeaks to both 'Guccifer 2.0' (a hacker calling himself Guccifer 2.0 and purporting to be Romanian initially took credit for the DNC hack: that claim was viewed skeptically, in part because the hacker didn't appear to speak Romanian) and Fancy Bear (a Kremlin-affiliated hacking group subsequently thought connected to the DNC Leaks). WikiLeaks founder Julian Assange said at the time that there's 'no proof whatsoever' that Moscow was involved. DCLeaks.com was registered in April 2016, and many of the documents were posted in early June. A DCLeaks administrator, who identified himself by email as Steve Wanders, didn't respond to written questions, including why much of the material focuses on Russia or Russian foreign-policy interests. Cyberintelligence firms have linked that hacking group to the GRU, Russia's military intelligence service, whose Moscow

headquarters is nicknamed the Aquarium. Three private security groups have linked the DNC incursion to that group and another Russian hacking group associated with the FSB, the country's civilian intelligence agency.

According to domain records, the dcleaks.com address was registered in mid-April via a small web hosting company in Romania. The site itself traces back to an IP address in Kuala Lumpur, Malaysia. DCLeaks corresponded with *The Smoking Gun* (*TSG*) via a Gmail account in the name of 'Steve Wanders'. Since being provided a password by 'Guccifer 2.0', *TSG* has monitored DCLeaks for further evidence that the site is being used as a cut-out for the cabal behind the DNC hacking and the 'spear phishing' directed at Clinton campaign workers (we will return to this DNC and DC problem of connection below).

The same summer of 2016, DCLeaks released 2,576 files from George Soros's Open Society Foundations, laying out strategies, plans and internal communication from the foundation's international activities. The most prominent leak from Soros' Open Society Foundations included internal files that totalled a significant 1.51GB in size with funding reports, contracts and confidential briefing memos. The foundation defines itself as working 'to build vibrant and tolerant democracies whose governments are accountable and open to the participation of all people' (https://www.opensocietyfoundations.org/about/mission-values). The information appears to date back to somewhere between the 2008 and 2009 timeframe, and has more current documentation up to 2016 as well. The leak contains internal memos, end of year reports, grants, contracts, agenda details, and biographies of all staff and board members. In the case of Soros's Open Society, hackers stole a trove of documents after accessing the foundation's internal intranet, a system called Karl, according to a person familiar with its internal investigation. On e August 2016, the DCLeaks.com Twitter account tweeted 'Check George Soros's OSF plans to counter Russian policy and traditional values,' attaching a screenshot of a $500,000 budget

request for an Open Society program designed to counter Russian influence among European democracies.

DCLeaks offered nothing about Hillary Clinton, Bernie Sanders, or Donald Trump, considering reports that Soros has donated or committed more than $25 million to boost Hillary Clinton and other Democratic candidates and causes, according to Federal Election Commission records. DCLeaks notes that Soros is 'named as the architect and sponsor of almost every revolution and coup around the world for the last 25 years.' In a Facebook post, the site reported that the hacked documents revealed Soros's plans to support opposition movements in Ukraine, Russia, Georgia, Armenia, and other countries 'where the United States desire to promote their interests' (Bastone 2017).

WikiLeaks and DNCLeaks

In July 2016, WikiLeaks released the DNCLeaks with two publications of 44,053 emails and 17,761 attachments (https://wikileaks.org/dnc-emails) covering the period between January 2015 and May 2016 from the accounts of seven key figures in the Democratic National Convention: Communications Director Luis Miranda (10,520 emails), National Finance Director Jordon Kaplan (3,799 emails), Finance Chief of Staff Scott Comer (3,095 emails), Finanace Director of Data & Strategic Initiatives Daniel Parrish (1,742 emails), Finance Director Allen Zachary (1,611 emails), Senior Advisor Andrew Wright (938 emails) and Northern California Finance Director Robert (Erik) Stowe (751 emails).

Several security vendors including CrowdStrike, ThreatConnect, and Fidelis have looked at both the Democratic Party (DNC) breach as well as the Democratic Congressional Campaign Committee (DCCC) breach, and said that the same Russian group was behind both attacks. The timing of the

DCCC and the Soros data published on DCLeaks is causing speculation about the connection of Guccifer 2.0 with DCLeaks, although it has been denied by DCLeaks and WikiLeaks. Several security groups have theorized that 'Guccifer 2.0' is a Russian invention, a hype man tasked with publicizing criminal acts that were actually committed by skilled government hacking groups. While he has described himself in emails as an 'unknown hacker with a laptop' and a foe of 'all the illuminati and rich clans which try to rule the governments', 'Guccifer 2.0' has acted more like a press flack, promising 'exclusives' and pushing journalists to do stories based on stolen documents carrying little news value. 'Guccifer 2.0' told *The Smoking Gun* that the material would be available through DCLeaks, a web site he described as a 'sub project' of WikiLeaks. Assange denied any connection with DCLeaks.

WikiLeaks and CIA leaks

In March 2017, WikiLeaks released CIA Vault7 and continued with steady releases of what they claimed it was only 1% of CIA material it had available, saying that the CIA had 'lost control' of an archive of hacking methods circulated 'among former US government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.' (see 'Year Zero', https://wikileaks.org/ciav7p1/cms/index.html).

The first part of the WikiLeaks Vault 7 series of 8,761 documents, allege how CIA's malware targets iOS and Android, Windows, OSX, and Linux routers using USB sticks, software on CDs, and turning the Samsung F8000 Smart TV into listening device by putting the TV into 'fake-off' mode. Two already stand out: 'Fine Dining', a questionnaire identifying which tools can be used for which operation, and 'Hive', a customized malware suite implants for Windows, Solaris, MikroTik used in internet routers and Linux platforms, and a Listening Post (LP)/Command and Control (C2) infrastructure to

communicate with these implants. This explosive development means that the US government is now well into leaking-like-a-paper-bag territory. The impact of the historically continuous competition between the CIA, the NSA, and FBI, and the exploitation of the internal feuds in the intelligence community in the US by the Trump administration, means that many more leaks are yet to come. The fact that US intelligence agencies accused formally Russia of intervening in the US elections to help Trump get elected (after the 2,000 emails hacked from the Clinton campaign which WikiLeaks released) and the war between Trump and the so called 'deep state', is a symptom of stark divisions and polarization in the US government and exacerbated by the political conflicts, well inside the intelligence communities.

The sacrifice of legal and ethical principles to the madness of internal intelligence and political wars is crystal clear, as well as how impossible it is to safeguard against leaks in such environment. The first problem is CIA's [Remote Devices Branch](https://wikileaks.org/ciav7p1/cms/page_20251151.html)'s [UMBRAGE group](https://wikileaks.org/ciav7p1/cms/page_2621751.html), where the CIA maintains a library of stolen malware produced in other countries. This malware can be used to disguise and misdirect attribution of where attacks have originated from in 'false flag' operations. This is feeding into theories that US intelligence services might have engineered such operation to point to Russia as the culprit of the meddling with the elections, as it falls into the hands of the Trump administration, which denies vehemently collaboration with WikiLeaks or Russia during the US elections. According to WikiLeaks: '[Tradecraft DO's and DON'Ts](https://wikileaks.org/ciav7p1/cms/page_14587109.html)' contains CIA rules on how its malware should be written to avoid fingerprints implicating the 'CIA, US government, or its witting partner companies' in 'forensic review'.

A secondary complication revolves around the commitment of the US government to the Vulnerabilities Equities Process. Tech companies lobbied and won for the disclosure of all pervasive vulnerabilities after 2010. The CIA keeping knowledge of these exploits to itself means that tech companies will not fix them and systems can be open to hacking by other governments, non state actors and cybercriminals. This puts tech companies yet again, as with the Snowden revelations, in a place of mistrust against the US government at a sensitive point in the country's history of fake news and accusations of bugs in the Trump Tower against the Obama administration. It does not matter if vulnerabilities have been fixed, as tech giants were to quick to reassure: the fact they were kept in the dark and were left exposed continuously is a significant break of any trust left in their own government. It also means that any cyberweapons used by the CIA at any point in time can be exploited by third parties everywhere and anywhere. Cyberweapons infecting machines in the wild are no longer classified.

The impact of internal intelligence wars and their exploitation by the Trump administration is a great big mess for the US and its relationships with other intelligence agencies. MI5 faced leaks that it allegedly devised 'Weeping Angel', which transforms a Samsung TV model F8000 into a listening device when it appears to be switched off and sends the recording to a CIA server. CIA also uses the US consulate in Frankfurt as a covert base for its hackers covering Europe, the Middle East and Africa and the whole world knows.

Leaktivism's discontents

Leaktivism puts intelligence agencies in an impossible position of forced transparency, which has transformed business as usual in the spy business, ever since the first WikiLeaks documents on Iraq and Afghanistan, with Snowden's death nail documenting the pervasive complete structural

metadata acquisition by the NSA. Ultimately, the US has been unable to protect its secrets since 2010, and this puts the intelligence communities and US allies in a world where secrecy is now impossible, even when devices are switched off. It places individual citizens in world where privacy is a victim of longstanding political domestic and international conflicts and intelligence predatory cyberwar tactics with no accountability or oversight, no effective action to get a grip on leaks, and where tech companies are the last to know about vulnerabilities on their systems, like the cheated husband. It is a world of hack or be hacked.

The political economy of the digital environments involved is significant here. This is a particular problem in the articulation of digital politics: the process of political disenfranchisement brought about by corporations looking to profit, governments looking to regulate information flows, and co-opted groups in civil society looking to appropriate the legitimate concerns of users for their own political and financial subsistence. The distinct features of this quasi-totalitarianism include: the monopoly of digital planning on surveillance that rests on back-channel and secret communication between government, tech corporate elites and, sometimes, NGOs; the use of civil society NGOs as mechanisms for circumventing democratic processes; 'enterprise association' politics, aimed at ensuring that the dual goal of state (security) and capital (profit) continues unabated and with little unaccountability; the unprecedented scope offered by total structural data acquisition on the part of western intelligence matrixes; the persecution and prosecution of journalists, whistle-blowers and transparency actors outside the scope of civil society groups; and the significant if insufficient contestation by members of the public concerning the infringement on civil liberties (see Karatzogianni and Gak 2015).

This *ménage à trois* of 'trusted' global networks — governments, corporations and NGOs — are holding a *de facto* mandate, and effective planning power, in

the digital field. They clothe themselves in a bastardized version of publicness, and in this guise usurp the political agency of individual members of society. In fact, these three supposedly trusted networks constitute an oligopoly that dominates the space in which governance is negotiated. They relegate the individual to a place of marginality, from where they are only able to address the threat of surveilling agents to their privacy from a position of acute precariousness. It is the individual has to pay for digital equipment, access, and their own necessary digital literacy, thereby funding the processes of purchase, connectivity and training; and it is also the individual who has to acquire the necessary skills and software to protect their privacy in the digital homes that are built by tech elites and surveilled by governments (in the name of security) and corporations (for the sake of profit). The individual citizen is put in a rather impossible situation, in which they must simultaneously procure the tools for the enforcement of the legal guarantees presumably held by the state to protect their rights, and at the same time develop tools to enforce them. In this environment — in which the state undermines privacy in the name of security, commercial interests collude with the state while offering false shelter, and civil society groups hijack the very voice of political engagement — the individual has only one choice: 'hack or be hacked'.

It is the precarious state of rights in the face of these developments that is a particularly thorny problem when individuals and groups engage in leaktivism or public interest hacks to create awareness about a particular ethical problem in the digital political economy, security, intelligence gathering or digital policing.

A case in point, Edward Snowden's leaks of hundreds of thousands of National Security Agency documents. Notwithstanding the conspiratorial tone, the response by the group Anonymous to Snowden's attempt to put surveillance under public scrutiny shows quite poignantly the reaction to the

revelations by movements instinctively opposed to quasi-totalitarian models of the digital public sphere:

> Your privacy and freedoms are slowly being taken from you, in closed door meetings, in laws buried in bills, and by people who are supposed to be protecting you ... Download these documents, share them, mirror them, don't allow them to make them disappear. Spread them wide and far. Let these people know, that we will not be silenced, that we will not be taken advantage of, and that we are not happy about this unwarranted, unnecessary, unethical spying of our private lives, for the monetary gain of the 1%.
> (https://www.facebook.com/anonymouslv/posts/521076614608161)

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

As we wrote with Martin Gak in 'Hack or be Hacked' (2015), leaktivism is a tactic resisting state and corporate actors' influence, that influence, however it can be also coopted by those same actors. NGOs are perhaps one of the most interesting cases concerning the usurpation and concealment of corporate and government interests under the cloak of civil association. The explicit argument here is that the corporate funding of NGOs has an impact on leaktivist ideological directions and impact of leaks. Certain of the leaktivism wars do not just impact governments and intelligence, but target or involved

in one way or another corporate-funded civil-society actors. Besides the leaks which set out to harm Soros, which were mentioned above, to illustrate my argumentation we can turn to eBay founder Pierre Omidyar, who eventually set up The Intercept, which published unredacted Snowden documents. Having begun his philanthropic activities in the late 1990s, by early 2014 Omidyar had given out $1 billion to all sorts of organizations and projects. In 2013 alone, his organizations gave out grants of $225 million. As well as personal donations, its funding is organized through three organizations: the Omidyar Network Fund, HopeLabs and Humanity United. Michael Gentilucci of Inside Philanthropy has argued that: 'We're dealing with an archipelago here, not a solid land mass, and the overarching entity is The Omidyar Group'. NGOs funded by Omidyar include Change.org; Center on Democracy, Development, and the Rule of Law; Global Integrity; Fundacion Ciudadano Inteligente; Global Voices; Media Development Investment Fund; The Open Data Institute; Open Government Partnership; Project on Government Oversight (POGO); Sunlight Foundation; The Transparency and Accountability Initiative; The Foundation for Ecological Security; the Endeavor Foundation; and Ashoka. Omidyar's American record includes contributions to the presidential campaign of Wesley Clark, and he is a co-investor with the CIA's venture capital firm IN-Q-TEL and Booz Allen Hamilton (an NSA subcontractor and former employer of Edward Snowden). Omidyar was the man who eventually became the guardian of the Snowden papers. In 2013, with a pledge of $250 million dollars, Omidyar had started a media network under the name First Look Media. His first three hires were Glenn Greenwald, Laura Poitras and Jeremy Scahill. In February 2014 First Look Media spun off a second media structure under the name of *The Intercept*. This online publication was devised in order to publish the unredacted Snowden documents and to 'produce fearless, adversarial journalism across a wide range of issues'.

To be explicit, the main discontent with leaktivism is that corporate-funded

leaktivist organizations of various descriptions tend to be involved in aspects of disrupting government intelligence, as well as other civil society organizations funded by either corporate or government actors.

Conclusion

In synopsis, leaktivist individuals and/or organizations present themselves as new surreptitious actors who engage in global political vigilantism, in order to mount resistance against surveillance, censorship, perceived injustice and corruption, and in solidarity with movements fighting repressive and authoritarian governments. Anonymous and Snowden serve to demarcate the space of resistance to the hidden mechanics of thoroughgoing political penetration of the social, and in so doing reveal the totalitarian mechanisms which they each claim to resist. Furthermore, leaktivism can have devastating timing and can partially influence elections, to the extent that in the public discourse leaktivism is seen as both enhancing democracy by holding governments and corporations accountable and enforcing transparency, and at the same time disrupting the democratic process, when the leaks are manipulated to influence public opinion and voting behaviour, as witnessed with the phenomenon of election-timed leaks occurring in the US, but subsequently in France and the UK during 2017. Lastly, to use a metaphor, the two faces of leaktivism — enhancing versus disrupting democracy — are historically continuous with debates observed from the very 2010 WikiLeaks start: the openness versus closure, stemming from social and communication fields, and transparency versus control debates, stemming from international relations and security fields, continue to characterize the controversies and discontents surrounding the phenomenon.

References

Brevini, B., Hintz, A. and McCurdy, P. (eds) (2013) *Beyond WikiLeaks: Implications for the future of communications, journalism and society*. New York: Palgrave Macmillan.

Bastone, W. (2017) 'Tracking The Hackers Who Hit DNC, Clinton', *The Smoking Gun,* 12 August, <http://www.thesmokinggun.com/documents/investigation/tracking-russian-hackers-638295> , accessed 11 September 2017.

Coleman, G. (2017) 'The Public Interest Hack', in G. Coleman and C. Kelty (eds) *Hacks, Leaks, and Breaches*, *Limn*, no. 8. <http://limn.it/the-public-interest-hack>, accessed 11 September 2017.

Coleman, G. and Kelty, C. (eds) (2017) *Hacks, Leaks, and Breaches*, *Limn*, no .8, <http://limn.it/issue/08>, accessed 11 September 2017.

Karatzogianni, A. (2010) 'Blame it on the Russians: Tracking the Portrayal of Russians During Cyber Conflict Incidents', *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, 4, pp. 127-150, <http://www.digitalicons.org/issue04/athina-karatzogianni>.

Karatzogianni, A. (2012) 'WikiLeaks Affects: Ideology, Conflict and the Revolutionary Virtual' in A. Karatzogianni and A. Kuntsman (eds) *Digital Cultures and the Politics of Emotion: Feelings, Affect and Technological Change*. Basingstoke: Palgrave Macmillan, pp. 52-73.

Karatzogianni, A. (2015) *Firebrand Waves of Digital Activism 1994-2014: The Rise and Spread of Hacktivism and Cyberconflict*. Basingstoke: Palgrave MacMillan.

Karatzogianni, A. and Robinson, A. (2014) 'Digital Prometheus: WikiLeaks, the State-Network Dichotomy and the Antinomies of Academic Reason', *International Journal of Communication*, 8, Feature 1-20, pp. 2704-2717, <http://ijoc.org/index.php/ijoc/issue/view/10#more4>, accessed 11 September 2017.

Karatzogianni, A. and Gak, M. (2015) 'Hack or Be Hacked: The Quasi-Totalitarianism of Global Trusted Networks', *New Formations: A Journal of Culture, Theory, Politics*, No.84/85, pp. 130-147, <http://www.lwbooks.co.uk/journals/newformations/issue/nf8485.html>.

White, M. (2016) 'The Panama Papers: leaktivism's coming of age', *The Guardian*, 5 April, <https://www.theguardian.com/news/commentisfree/2016/apr/05/panama-papers-leak-activism-leaktivism>, accessed 11 September 2017.