VOLUME 9

The International Journal of

Technology, Knowledge, and Society

WikiLeaks and the Public Sphere

Dissent and Control in Cyberworld

NATHALIE MARECHAL

COMMON GROUND

TECHANDSOC.COM

THE INTERNATIONAL JOURNAL OF TECHNOLOGY, KNOWLEDGE, AND SOCIETY
www.techandsoc.com

First published in 2013 in Champaign, Illinois, USA
by Common Ground Publishing LLC
www.commongroundpublishing.com

ISSN: 1832-3669

The International Journal of Technology, Knowledge, and Society is peer-reviewed, supported by rigorous processes of criterion-referenced article ranking and qualitative commentary, ensuring that only intellectual work of the greatest substance and highest significance is published.

WikiLeaks and the Public Sphere: Dissent and Control in Cyberworld

Nathalie Marechal, University of Southern California, USA

Abstract: This paper analyzes the competing discourses that are informing the debate about privacy and transparency on the Internet, through the lens of the WikiLeaks controversy of 2010-2011. The WikiLeaks affair is simultaneously 1) emblematic of a new world order, 2) the product of state power encountering a technologically-enabled counter-power, and 3) a focal point for the (re)negotiation of norms and values governing the control of and access to information. This public controversy concerns the rights and responsibilities of citizens and the state vis-a-vis information, with profound implications for public life, diplomacy, and international relations. Not only is it substantively about the media, it is also in the media and argued through the media. Drawing from a variety of disciplines such as communication studies, rhetoric, sociology, political science, and international relations, this paper examines public discourse in the forms of official rhetoric (coming from the U.S. government, WikiLeaks and proxies for either party), as well as the comments of media and scholarly observers, as representative of arguments that work to define and constitute these ideas as discursively sustained institutions of civic and political culture. This qualitative study relies chiefly on archival research focused on news articles published by the global newspapers that collaborated with WikiLeaks on the so-called Cablegate releases, feature-length articles from prominent newsmagazines, and other publications.

Keywords: WikiLeaks, Hacker Ethic, Hacking, Cybersecurity, Julian Assange, Bradley Manning, Chelsea Manning, Information Security, Leaks, Whistle-Blowers, Privacy, Transparency, Surveillance

Introduction

In 2010 and 2011, the WikiLeaks controversy highlighted the ongoing renegotiation of the trade-off between secrecy and the openness that is at the heart of liberal democracy. Simmering tensions about transparency and privacy in the Internet age reached a boiling point after the April 2010 release of the Collateral Murder video, depicting what appears to be unprovoked killing of Iraqi civilians by the U.S. Army. The releases of the Iraq War Logs, Afghanistan War Diary, and State Department Cables, as well as the legal travails of Julian Assange and Bradley Manning, have added fuel to the flames to create a veritable maelstrom with diplomatic, political, legal and media implications that will take years to untangle.

In this paper I argue that the WikiLeaks affair is emblematic of a renegotiating of societal norms about control of and access to information in the Internet Age – what I call cyberworld. The WikiLeaks phenomenon is simultaneously 1) emblematic of an emerging world order, 2) the product of state power encountering a technologically-enabled counter-power, and 3) a focal point for the (re)negotiation of norms and values governing the control of and access to information. The purpose of this study is to analyze the competing discourses that are informing the debate about privacy and transparency on the Internet, through the lens of the WikiLeaks controversy of 2010-2011.

Methodology

To that end, this paper examines how the concepts of information access and control are implicated in public discourse about the WikiLeaks controversy. I examine public discourse in the forms of official rhetoric (coming from the U.S. government, WikiLeaks and proxies for either side), as well as the comments of media and scholarly observers, as representative of arguments that work to define and constitute these ideas as discursively sustained institutions of civic and political culture. This qualitative study uses archival research focusing on news articles

The International Journal of Technology, Knowledge, and Society
Volume 9, 2013, techandsoc.com, ISSN: 1832-3669

published by four of the global newspapers that collaborated with WikiLeaks on the Cablegate releases (The New York Times, The Guardian, Le Monde, and El País) in 2010 and 2011. A fifth publication, Der Spiegel, also worked with WikiLeaks, but was excluded for reasons of linguistic access. I also included feature-length articles from prominent newsmagazines such as The Atlantic, The New Yorker, The Economist, and Time, as well as representative articles from right-leaning publications such as the Wall Street Journal and the Washington Times.

Literature Review

In this paper I draw from a variety of disciplines, including communication studies, rhetoric, sociology, political science, and international relations. The matter at hand is a public controversy about the rights and responsibilities of citizens and the state vis-à-vis information, with profound implications for public life, diplomacy and international relations. This controversy is substantively *about* the media, *in* the media and argued *through* the media. Therefore, in order to make sense of it one must ground one's analysis in a solid understanding of media studies.

Manuel Castells defines media as "the social space where power is decided," opposing power – "the structural capacity of a social actor to impose its will over other social actor(s)" - to counter-power – "the capacity by social actors to challenge and eventually change the power relations institutionalized in society" (Castells 2007). Despite the ideal of journalistic objectivity, "the way the mass media construe reality" is subject to the "formidable influence" of "established institutions (as compared with opposition movements)," and there is no institution more influential than the U.S. Government (Gitlin 1990). The indexing hypothesis holds that "the range of voices and viewpoints in news and editorials is 'indexed' to 'the range of views expressed in mainstream government debate about a given topic" (Bennett 1990). Indeed, Daniel Hallin's study of media coverage during the Vietnam War showed that if the Republican and Democratic parties agree on something, it is treated as truth by the media. The zone of legitimate politics consists of the issues on which the two parties disagree. Measures and viewpoints opposed by both parties are relegated to the fringes and deemed illegitimate (Hallin 1986).

Castells argues that since both power and counter-power need media space to assert themselves, in light of the tight grip that the establishment holds on mainstream media, the media of mass self-communication (what is often called social media) is the space where counter-power is created and exercised (Castells 2007). Thus, transparency mechanisms like WikiLeaks are a new battlefield where counter-power has the home advantage – at least for now.

The political philosophy behind WikiLeaks is rooted in the hacker ethic. The hacker subculture was born in the 1950s in the U.S. academic milieu, notably the Massachusetts Institute of Technology, Carnegie-Mellon and Stanford, where a small cadre of undergraduates became enthralled with tinkering with the hulking mainframe computers that were then the cutting edge (Levy 1984). As Helen Nissenbaum explains, a set of common norms emerged that included

> commitment to total and free access to computers and information, belief in the immense powers of computers to improve people's lives and create art and beauty, mistrust of central authority, a disdain for obstacles erected against free access to computing, and an insistence that hackers be evaluated by no other criteria than technical virtuosity and accomplishment (by hacking alone and not 'bogus' criteria such as degrees, age, race, or position) (Nissenbaum 2004).

The subculture developed its own mythology, imagining cyberspace as

> a new frontier where great freedoms and great opportunities lay, where brave (if sometimes bizarre) cowboys and 'homesteaders' would create a space distinct from conventional physical space, embodying ideas of liberty and plenty (Nissenbaum 2004).

Meddlesome authorities, such as university administrators, project managers, or governments, have no positive role to play in a world ruled by the hacker ethic, which "eschews centralized, restricted access to computers and information."And conversely, the hacker ethic is "inimical to the interests of established corporate and government powers, including particularly intellectual property and order"(Nissenbaum 2004).

Over the past few decades, the public conception of hacking has moved from an image of "ardent (if quirky) programmers" to "miscreants, vandals, criminals, and even terrorists" (Nissenbaum 2004). For Deborah Halbert, this is "the result of conscious movement by mainstream voices of governmental and private authority to demonize and portray hackers as abnormal, deviant bullies, who victimize the rest of ordered society," and this for two reasons. First, "to control the definition of normalcy in the new world order of computer-mediated action and transaction" (what I call cyberworld), and second, to justify "further expenditures in security, vigilance and punishment" (Halbert 1997). Similarly, Andrew Ross "portrays the changing moral status of hackers as a cultural regrouping, with hackers pitted against the corporate and government mainstream" (Ross 1991). Indeed, much as the Old West was inevitably tamed by the norms and values from back East, cyberspace has been progressively normalized into mainstream daily life:

> Local retailers, global corporations, credit card companies, traditional media corporations, governments (local, state and federal), grandmothers, preachers and lonely hearts sought their fortunes online. Pragmatic economic visions (from the likes of US vice-president Al Gore) competed with the romantic mythologies of futurists as cyberspace became increasingly domesticated, encompassing the mundane and being encompassed by it. These familiar presences, in turn, brought with them familiar practices and modes of interactions and associated norms and institutions. (Nissenbaum 2004).

Real-world concepts like property, sovereignty, indecent speech, and capitalism have combined to transform what Lawrence Lessig terms Net95 into "the enclosed, gated, regulated world of Net01" (Lessig 2006). When confronted with this hedged-in version of cyberspace, the hacker's natural inclination is to break free – but how?

Albert Hirschman suggests that people can try to change institutions in two main ways. They can *exit*, i.e. opt out or drop out, or they can *voice* their opposition and desire for change. Institutions typically respond either by ignoring the contrary behavior where possible, or by "seeking ways to make themselves less vulnerable to either form of dissidence, by devising mechanisms for defusing the power of voice and exit, focusing on ways to 'strip the members-customers of the weapons which they can yield'" (Hirschman 1990). As Paul A. Taylor points out, the issue of dissent in a media-saturated public sphere predates the Internet:

> Umberto Eco addresses head-on the problems faced by political protest in a media-dominated age, distinguishing between a strategic and a tactical approach. The former aims to fill the existing channels of communication with radically like-minded people who can seek to change their impact with their own liberating opinions and information. The latter involves more directly confrontational techniques. For Eco, the likelihood of success with the strategic approach is limited because, while it may achieve good short-term political or economic results, 'I begin to fear it produces very skimpy results for anyone hoping to restore to human beings a certain freedom in the face of the total phenomenon of Communication (Eco 1967).

The Internet has added a layer of complexity by creating new channels for counter-power to assert itself and providing a digital underground where dissenters could gather outside of the

public eye – much like early Christians secretly worshipped in catacombs and freedom fighters of all kinds hid in the woods.

Obscurity can be a double-edged sword, though, as the public's fear of the unknown can be exploited. Thus, the term "hacktivist" – aside from being a hideous neologism – serves to create a word association between political activists and hackers, further delegitimizing those who would change the status quo by drawing attention to their misunderstood methods. Taylor argues that "hacktivism seems fully conscious of the dangers of over-identification with the technological means of protest," however, which may explain why the "hacktivist" label is more frequently bestowed than claimed (Taylor 2005). The term lacks a commonly accepted definition, which further complicates things. In common parlance, the term "hacktivism" is used to refer to the use of the Internet in executing an exit or voice strategy. Taylor calls it "a refocusing upon the political nature of the end to which technological means should be put: a normative element has been put back into objectified computer code," without specifying a common agenda. Journalist Stuart Millar goes a step further, defining hacktivism as a "highly politicized underground movement using direct action in cyberspace to attack globalization and corporate domination of the Internet" (Millar 2001). Regardless of the definition chosen (broad or narrow), the WikiLeaks affair is a highly visible example of hacktivism that is already being analyzed by media scholars and commentators.

One such work, "WikiLeaks and the Age of Transparency" by Micah L. Sifry situates the WikiLeaks affair in the context of a technologically mediated trend toward increased information sharing – for better or for worse. Sifry conceives of the book as "a report from the trenches where a wide array of small-d democracy and transparency activists are hard at work using new tools and methods to open up powerful institutions and make them more accountable, and to situate WikiLeaks in that movement" (Sifry 2011). Meanwhile, for Andrew Murray, the WikiLeaks debate "is framed against a distinct but not unrelated debate currently taking place in the media outlets, political fora and coffee houses of the United Kingdom." Murray concludes that "transparency may sometimes be sacrificed in favour of competing privacy rights," and notes that

> WikiLeaks, and the media in general, view public sector bodies and private corporations as monolithic. This is of course not the case. All bodies corporate (be they private or public) are in fact organisms made up of thousands, or even tens of thousands, of decision makers; individuals who collectively form the "brain" of the organization. The problem is that individuals need space to make decisions free from scrutiny, or else they are likely to make a rushed or panicked decision (Murray 2011).

Analysis

Reactions to the WikiLeaks affair ran the gamut from calling for Julian Assange's death to praising him as a visionary martyr to the cause of information freedom. Most of the discourse, of course, is much more nuanced.

Information Wants To Be Free

As I described earlier, the hacker ethic rejects the notions of proprietary information and hierarchical decision-making. A former hacker himself under the moniker Mendax, Assange has over the years produced a series of writings that are far from comprising a coherent political philosophy, but do give insight into his thought process and logic. In 2006 (around the time WikiLeaks was founded), Assange wrote three short essays that are ostensibly on conspiracies, but his definition of conspiracy is so broad as to include most, if not all, legitimate government action, and even any non-governmental collective action that operates under typical norms of privacy and confidentiality. Urizenus Sklar (a pseudonym used by Northwestern University

philosophy professor Peter Ludlow) explains that Assange uses 'conspiracy' to mean "secrecy and exchange of information within a closed network," and points out that his theory of conspiracies owes much to Granovetter and other network theorists (Granovetter 1973; Sklar 2010).

Aaron Bady, then a graduate student, wrote the first analysis of Assange's writings to receive widespread attention. In fact, The Atlantic's Alexis Madrigal credited Bady with "changing WikiLeaks coverage," as the blog post was passed on from one wonk to another until the New York Times' breaking-news blog The Lede linked to it, exposing the piece to "many of the most influential journals and opinion leaders." Significantly, the WikiLeaks Twitter account linked to the post, calling it a "Good essay on one of the key ideas behind WikiLeaks."1 As Bady explains,

> [Assange] begins by describing a state like the US as essentially an authoritarian conspiracy, and then reasons that the practical strategy for combating that conspiracy is to degrade its ability to conspire, to hinder its ability to "think" as a conspiratorial mind. The metaphor of a computing network is mostly implicit, but utterly crucial: he seeks to oppose the power of the state by treating it like a computer and tossing sand in its diodes.
>
> […]
>
> This, Assange reasons, is a way to turn a feature into a bug. And his underlying insight is simple and, I think, compelling: while an organization structured by direct and open lines of communication will be much more vulnerable to outside penetration, the more opaque it becomes to itself (as a defense against the outside gaze), the less able it will be to "think" as a system, to communicate with itself. The more conspiratorial it becomes, in a certain sense, the less effective it will be as a conspiracy. The more closed the network is to outside intrusion, the less able it is to engage with that which is outside itself (true hacker theorizing).

Bady goes on to explain that for Assange,

> the most effective way to attack this kind of organization would be to make "leaks" a fundamental part of the conspiracy's information environment. Which is why the point is *not* that particular leaks are *specifically* effective. WikiLeaks does not leak something like the "Collateral Murder" video as a way of putting an end to that particular military tactic; that would be to target a specific leg of the hydra even as it grows two more. Instead, the idea is that increasing the porousness of the conspiracy's information system will impede its functioning, that the conspiracy will turn against *itself* in self-defense, clamping down on its own information flows in ways that will then impede its own cognitive function. You destroy the conspiracy, in other words, by making it so paranoid *of itself* that it can no longer conspire… The leak, in other words, is only the catalyst for the desired counter-overreaction; WikiLeaks wants to provoke the conspiracy into turning off its own brain in response to the threat. As it tries to plug its own holes and find the leakers, he reasons, its component elements will de-synchronize from and turn against each other, de-link from the central processing network, and come undone. Even if all the elements of the conspiracy still *exist*, in this sense, depriving

1 Madrigal, Alexis. 2010. "The Unknown Blogger Who Changed WikiLeaks Coverage." The Atlantic, December.

> themselves of a vigorous flow of information to connect them all together as a conspiracy prevents them from *acting* as a conspiracy.
>
> […]
>
> Because we all basically know that the US state — like all states — is basically doing a lot of basically shady things basically all the time, simply revealing the specific *ways* they are doing these shady things will not be, in and of itself, a necessarily good thing. In some cases, it may be a bad thing, and in many cases, the provisional good it may do will be limited in scope. The question for an ethical human being — and Assange always emphasizes his ethics — has to be the question of what exposing secrets will actually accomplish, what good it will do, what better state of affairs it will bring about. And whether you buy his argument or not, Assange has a clearly articulated vision for how Wikileaks' activities will "carry us through the mire of politically distorted language, and into a position of clarity," a strategy for how exposing secrets will ultimately impede the production of *future* secrets. The point of WikiLeaks — as Assange argues — is simply to make WikiLeaks unnecessary (Bady 2010).

Even as he portrays himself as a radical transparency activist, Assange's actions belie a fierce commitment to protecting his own privacy. Longtime colleague Daniel Domscheit-Berg portrays Assange as obsessed with transparency for everyone but himself (Domscheit-Berg and Klopp 2011). Likewise, Andrew Murray notes that while WikiLeaks' core political value appears to be that "publishing improves transparency, and this transparency creates a better society for all people," WikiLeaks itself appears exempt from sunshine's salutary effects (Murray 2011). This double standard seems prevalent among transparency radicals. Indeed, even as they argue that all organizations (government, business and civil society alike) should practice total transparency, the cyber-vigilantes like Anonymous and LulzSec who have been waging cyber-war against organizations deemed opposed to the nebulous cause of Internet freedom are themselves extremely opaque.

U.S. Government, Allies and Proxies

At the other end of the spectrum are secrecy hard-liners claiming to speak for the U.S. government. The most strident voices belonged to politicians with little expertise in or responsibility for information security. Then-presidential hopeful Sarah Palin called Assange "an anti-American operative with blood on his hands," and asked why he wasn't being "pursued with the same urgency we pursue al Qaeda and Taliban leaders." Republican Congressman Peter King "called on Washington to pursue aggressively WikiLeaks and Mr Assange for violating the Espionage Act," and Senator Joe Lieberman called the leaks "outrageous, reckless and despicable."2 Newt Gingrich, then a front-runner in the race for the 2012 Republican presidential nomination, said:

> What we should do is treat Assange as an enemy combatant. Information warfare is warfare. The National Security Agency should close down that site, keep it closed

2 Anon. 2010. "WikiLeaks: Sarah Palin demands Julian Assange hunted down like Al Qaeda terrorist." The Daily Mail, December 1, Online edition. http://www.dailymail.co.uk/news/article-1334341/WikiLeaks-Sarah-Palin-demands-Julian-Assange-hunted-like-Al-Qaeda-terrorist.html.

> down. Every time they try to reopen it under a new name, they should close it down. We should wage active information warfare against any effort to release American secrets.3

While such statements could be brushed aside as so many politically pandering soundbites, they actually seem to be representative of a broad consensus among the Washington establishment. Marc Thiessen, a former speechwriter for George W. Bush's, wrote in the Washington Post:

> Let's be clear: WikiLeaks is not a news organization; it is a criminal enterprise. Its reason for existence is to obtain classified national security information and disseminate it as widely as possible -- including to the United States' enemies. These actions are likely a violation of the Espionage Act, and they arguably constitute material support for terrorism. The Web site must be shut down and prevented from releasing more documents -- and its leadership brought to justice… Assange is a non-U.S. citizen operating outside the territory of the United States. This means the government has a wide range of options for dealing with him. It can employ not only law enforcement but also intelligence and military assets to bring Assange to justice and put his criminal syndicate out of business… With appropriate diplomatic pressure, these governments may cooperate in bringing Assange to justice. But if they refuse, the United States can arrest Assange on their territory without their knowledge or approval.4

For Thiessen, WikiLeaks is as grave a threat to national security as Al-Qaeda, warranting extra-judicial action of the sort that was used against Osama bin Laden in Pakistan. He also adds,

> taking him off the streets is not enough; we must also recover the documents he unlawfully possesses and disable the system he has built to illegally disseminate classified information. 5

As Ludlow points out, recovering stolen documents is impossible in cyberworld, particularly since Assange had taken care to give an encrypted file of the as-yet unpublished leaks to supporters around the globe and set up a "dead-man's switch" to ensure that the documents would be released should anything happen to him (Ludlow 2010). Moreover, this line of argumentation is predicated on the assumption that the leaks directly caused harm to befall informants of the U.S., and the empirical evidence is decidedly mixed.

Former Department of Homeland Security official and legal scholar Paul Rosenzweig views what he terms "the WikiLeaks Fiasco" as a cyber-war between "corporate boards reacting responsibly to an irresponsible act" and "cyber insurgents." The question of collateral damage to informants is at most an afterthought. Rosenzweig identifies the WikiLeaks disclosures as "an assault on state authority (and more particularly, that of the United States)" – and for him, this is a bad thing. Having spent his career between government service and think tanks, Rosenzweig can only react in one way to a challenge to U.S. hegemony, and that is to treat it as an act of war. Indeed, in his opinion counterinsurgency (COIN) is "the right doctrinal solution for winning in cyberspace." When all you have is a hammer, everything looks like a nail. For Rosenzweig, WikiLeaks isn't about speech, it's about power – and he believes that the hackers are trying to seize it:

---

3 Eddlem, Thomas R. 2010. "Gingrich Calls Assange an 'Enemy Combatant'." The New American, December 9. http://thenewamerican.com/usnews/foreign-policy/5454-gingrich-calls-assange-an-qenemy-combatantq.
4 Thiessen, Marc. 2010. "WikiLeaks must be stopped." The Washington Post, August 3, sec. Opinion. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080202627.html.
5 Thiessen, Marc. 2010. "WikiLeaks must be stopped." The Washington Post, August 3, sec. Opinion. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080202627.html.

> WikiLeaks-like insurgents seem to have a different aim – "independence" – from government. That independence is premised on weakening political authority over the cyber domain (Rosenzweig 2011).

However, Rosenzweig misses a crucial distinction here. Unlike kinetic insurgents, hackers don't deny the government's authority over the physical world – only over certain online activities. They are not trying to wrestle control from the state, but to limit the encroachment of government power into cyberspace.

Media: The Gray Zone

The tone in media coverage of WikiLeaks shifted in 2010 with the release of the so-called Afghanistan and Iraq war logs, which brought the group's efforts to the attention of the mainstream media. Secrecy hard-liners like Dick Cheney and reactionary "rally 'round the flag" while patriots started to vilify Assange and his organization, the elite media consensus seemed to be that WikiLeaks was providing a global public service by exposing potential war crimes, drawing favorable comparisons to the Pentagon Papers.

Moreover, data without context and analysis is not information. Information is something that "consumers can use, presented in a way they can use it," and the sheer volume of data comprising the Iraq and Afghanistan war logs precluded its public usability (Lessig 2009). Recognizing that traditional journalism skills were needed to provide this context and analysis, Assange partnered with the *Guardian* and the *New York Times* to prepare the Iraq and Afghanistan documents for publication, but even these seasoned investigative journalists struggled to make sense of the half-million records in their possession: "It's like panning for tiny grains of gold in a mountain of data," complained veteran journalist David Leigh. "How are we ever going to find if there are any stories in it?" (Leigh and Harding 2011).

The involvement of the *Guardian* and the *New York Times* undoubtedly gave the Iraq and Afghanistan leaks a level of visibility that they would not have enjoyed otherwise, but the significance of the leaks remained open to subjective interpretation, and by and large, media commentators found "evidence" to support their existing normative biases. For example, left-leaning European newspapers focused on the horrors of war recounted in minute detail by the military field reports:

> Thousands of documents released online support the idea that the allies are failing, and fuels the debate about the Pakistani secret service's duplicity in the struggle against the Taliban.6

> What do these reports, written by low-level American soldiers after routine missions? Nothing, unfortunately, that changes the image of this war. To the contrary, they confirm the daily horror of an improvised occupation, whose first victims are civilians by the hundreds of thousands, facing GIs under orders to "protect yourselves first." These reports contradict a number of official statements. For that reason alone, they deserve to be read.7

---

6 Cypel, Sylvain. 2010. "Afghanistan: les revelations sur les coulisses de la guerre embarrassent Washington." Le Monde, July 28.
7 Kauffman, Sylvie. 2010. "WikiLeaks: le dossier irakien." Le Monde, October 24.

> The Afghanistan papers, more than 90,000 secret Pentagon documents leaked by the WikiLeaks site, illustrate the failure of a war that has already lasted nine years and prove the Pakistani intelligence service's complicity with the Taliban.8

In contrast, conservative American outlets like the *Wall Street Journal* and the *Washington Times* focused their coverage on Assange's "antiwar activism" and on the threat posed by WikiLeaks to American national security:

> The 93,000 documents on six years of war in Afghanistan take the narrative to last December, when President Obama's new strategy (with 30,000 additional troops) was barely getting started. But that was not relevant for WikiLeaks' antiwar agenda. The aim clearly is to drive up antiwar numbers at a time when opinion polls give Mr. Obama's war the support of fewer than half the people."9

> Broadly speaking, there was little news in the logs. It's been long known, for example, that elements of Pakistan's spy agency, the Inter-Services Intelligence, have deep ties to the Taliban and other enemies of the U.S. But the logs include deadly details. […] WikiLeaks claims it aims to protect civilians in wartime. Instead it has endangered untold numbers of Afghans who are willing to help fight the Taliban. It says its actions can bring transparency to government, but these leaked reports may ultimately cause less information to be tracked and shared. Those of us inclined to view technology as a force for good need to recognize when it can be abused. Technology makes it possible to release lethal information in wartime indiscriminately. It doesn't excuse people who choose to do it.10

> But the WikiLeaks story is a new and troubling event. Our initial reaction was that the documents expose no big lies about the war and, judging from what we've seen so far, no small ones either. They reveal nothing that wasn't already known about Iranian and Pakistani support for the Taliban. In other words, their value in terms of the public's right to know is de minimis. But the closer we and other have looked at the documents, it's clear that the WikiLeaks dump does reveal a great deal about the military's methods, sources, tactics and protocols of communication. Such details are of little interest to the public at large, and they are unlikely to change many minds about the conduct, or wisdom, of the war. But they are of considerable interest to American's avowed enemies and strategic competitors such as Russia and China.11

A second shift in coverage followed the November 2010 "Cablegate" release, comprising thousands of classified State Department cables or memos. This release was coordinated with five leading news publications from five different countries: *The Guardian* (UK), *Der Spiegel* (Germany), *Le Monde* (France), *El País* (Spain), and *The New York Times* (USA), and the pace of news stories was coordinated in advance by the editorial teams. The coverage from late November and December 2010 is an unprecedented hybrid of reporting, editorials and first-person accounts, as the five publications were simultaneously the first to report on the content of the cables, published editorials on the cables' revelations and on their own decisions to publish

---

8 Anon. 2010. "La web WikiLeaks difunde los secretos del Pentagono sobre Afganistan." El Pais, July 27.
9 de Borchgrave, Arnaud. 2010. "Gusher of WikiLeaks: Activists hope documents will undermine war support." The Washington Times.
10 Anon. 2010. "WikiLeaks and 'War Crimes'; Julian Assange, founder of WikiLeaks.org, says he wants to protect civilians. In fact he's endangering them." The Wall Street Journal, August 1, sec. Opinion.
11 Anon. 2010. "WikiLeaks 'Bastards'; The website has endangered the lives of Afghan informants." The Wall Street Journal, July 28, sec. Opinion.

them, and provided a forum for others (including several American ambassadors) to voice their views. The papers were also reporting on the Assange rape allegations in Sweden and the proceedings against Manning in the United States. All five are considered to be "the newspaper of record" in their respective country/media market: the stakes could not have been higher.

Publications outside of the "cartel of five" focused their reporting on the leaks as media event and on developments in Assange and Manning's legal travails. For example, *The Economist* discussed the WikiLeaks affair and its repercussions in detail as part of a July 2011 special report on the news industry:

> Despite WikiLeaks' difficulties, its approach is being adopted by others. Al-Jazeera has set up a "transparency unit" with a WikiLeaks-style anonymous drop box. The Wall Street Journal launched a drop box of its own in May, but was criticized for not offering enough legal protection to leakers. "Everyone's looking at the idea," says the Guardian's Alan Rusbridger, "but if you're going to do it you have to make it really secure."12

Unlike the Afghan and Iraq releases, Cablegate lacked a single, clear moral justification for release that could fit into a soundbite. As was noted by numerous media reports, on the whole, America's diplomats came across as responsible professionals doing their job. Covering topics as disparate as Prince Andrew's adventures in Central Asia and then-Tunisian strongman Ben Ali's pet tiger, Cablegate seemed to be about openness for its own sake. But among the more salacious stories were revelations about American spying at the United Nations and countless instances of diplomatic hypocrisy by virtually every country on the planet. While spies posing as diplomats and kleptocratic strongmen surprised no one (or at least they shouldn't have), the cables provided the evidence that had been missing. These stories were of varying interest to the readers of the five central publications, and each paper focused on the stories that were most relevant to their readers. For example, *Le Monde* focused on

> articles about France, its anti-terrorist policies and its urban youth, on French-American relations, and on topics of particular concern to French diplomacy: Iran and Afghanistan, Russia and Lebanon. And on Africa: Senegal, Cote d'Ivoire, al-Qaida in Maghreb and its French hostages. 13

Likewise, *El País* emphasized stories about Spain and Latin America, and *Der Spiegel* chiefly wrote about Germany's involvement in Afghanistan.

The U.S. government's reaction to Cablegate was somewhat disjointed, simultaneously condemning the release in the strongest terms and dismissing the content of the leaks as banal, in an attempt to both avoid spurring interest in the cables (the "Barbara Streisand effect" - see for example Bernoff and Li 2008) and warn any would-be whistleblowers against leaking information themselves. As Micah Sifry put it,

> Instead of an honest discussion about what the war logs and cables tell us in toto, in the wake of their emergence we have been treated to a bizarre and contradictory set of responses. Sometimes, what WikiLeaks has done is portrayed as worse than what Al Qaeda has done. And other times, we are told that the so-called revelations are actually pretty humdrum (Sifry 2011).

---

12 Anon. 2011. "WikiLeaks and other newcomers: Julian Assange and the new wave." The Economist, July 7, sec. Special report: the news industry. http://www.economist.com/node/18904166.

13 Ourdan, Remy. 2010. "Dans les coulisses de la diplomatie americaine." Le Monde, November 30.

Indeed, the significance of the cables' contents is hotly contested. Those who believe that the content itself is fairly insignificant focus on the questions that the WikiLeaks affair raises about information sovereignty. Those who believe that the content itself is significant tend to either applaud WikiLeaks for its supposed role in fomenting the Arab Spring, or to condemn it for what it may have revealed about the sources and methods of America's diplomacy and intelligence.

Conclusion

The WikiLeaks affair did not happen by accident. The conditions for a leak from within the largest bureaucracy the world has ever seen had been gathering for years: the proliferation of digital information, the growth of the U.S. intelligence community, technological innovations that facilitated information-sharing while giving the comforting illusion of security, and increasingly blurred definitions of journalism. It was only a matter of time before a "Black Swan" event brought existing trends into relief. Like the terrorist attacks of September 11, 2001, the WikiLeaks affair caught the world by surprise, has had (and is continuing to have) a major impact on the world and the world system, and is retrospectively predictable (Taleb 2010). Thus, reactions to WikiLeaks should be interpreted as reactions to the preexisting trends. Comments like those of Sarah Palin, Newt Gingrich and Joe Lieberman are all the more sinister when conceived not as ad hominem attacks against a "peripatetic Australian," but as a visceral rejection of the emerging world order and opposition to any form of counter-power.

The evolution of norms governing information access and control is closely related to other matters of concern for our society, including copyright over creative works, asynchronous and multisynchronous communication, and the eroding boundaries between work and play in the "always on" workplace, all evidence of cyberworld's relentless encroachment on the purely physical world. And just as the "real" world brought its bourgeois norms into cyberspace, cyberworld is bringing the hacker ethic into the existing political system, and arguably has enabled the rise of laissez-faire libertarianism, characterized by rejection of government authority and enthusiasm for self-regulation.

Hacktivists like Julian Assange and Chelsea (then known as Bradley) Manning can thus be seen as cyberworld versions of frontier heroes like Zorro and Davy Crockett, both troubled misfits lashing out at what they perceive to be an unfair world using a relatively rare yet powerful weapon: hacking. As Nissenbaum remind us,

> If there is something political that ties together these descendants of early hackers, it is protest – protest against encroaching systems of total order where control is complete, and dissent is dangerous. These hackers defy the tendencies of established powers to overreach and exploit without accountability. With their specialized skills, they resist private enclosure and work to preserve open and popular access to online resources, which they consider a boon to humanity. Ornery and irreverent, they represent a degree of freedom, an escape hatch from a system that threatens to become overbearing. In societies striving to be liberal and democratic, this is a significant part of the value of hacking and an important reason to resist obfuscation of the category (Nissenbaum 2004).

Postscript

Since the completion of this project, Edward Snowden's leaks concerning the National Security Administration's surveillance activities have raised the stakes for both transparency activists and for the national security apparatus – and according to Snowden collaborator Glenn Greenwald, the biggest news is yet to come. As of October 2013, Private Manning is serving a 35-year sentence for leaking the Iraq, Afghanistan and State Department documents to WikiLeaks, Julian Assange is living as an asylee in the Ecuadorian embassy in London, and Edward Snowden

received temporary asylum in Russia. Assange and Snowden are both unable to physically reach the countries that have offered them protection, as they would have to traverse physical space under the control of one or more countries that have promised to arrest and extradite them to the United States and to Sweden, respectively. Assange further believes that Sweden is likely to surrender him to the United States. The irony of avowed civil liberties activists being protected by illiberal, largely undemocratic regimes has not been lost on their detractors or their supporters. The question remains whether this says more about their motives or about the US government.

REFERENCES

Anon. 2010. “La web WikiLeaks difunde los secretos del Pentagono sobre Afganistan.” *El Pais*, July 27.

Anon. 2010. “WikiLeaks ‘Bastards’; The website has endangered the lives of Afghan informants.” *The Wall Street Journal*, July 28, sec. Opinion.

Anon. 2010. “WikiLeaks and ‘War Crimes’; Julian Assange, founder of WikiLeaks.org, says he wants to protect civilians. In fact he’s endangering them.” *The Wall Street Journal*, August 1, sec. Opinion.

Anon. 2010. “WikiLeaks: Sarah Palin demands Julian Assange hunted down like Al Qaeda terrorist.” *The Daily Mail*, December 1, Online edition. http://www.dailymail.co.uk/news/article-1334341/WikiLeaks-Sarah-Palin-demands-Julian-Assange-hunted-like-Al-Qaeda-terrorist.html.

Anon. 2011. “WikiLeaks and other newcomers: Julian Assange and the new wave.” *The Economist*, July 7, sec. Special report: the news industry. http://www.economist.com/node/18904166.

Bady, Aaron. 2010. Julian Assange and the Computer Conspiracy; “To destroy this invisible government”. Personal blog. *zunguzungu*. November 29. http://zunguzungu.wordpress.com/2010/11/29/julian-assange-and-the-computer-conspiracy-%E2%80%9Cto-destroy-this-invisible-government%E2%80%9D/.

Bennett, W. Lance. 1990. “Toward a Theory of Press-State Relations in the United States.” *Journal of Communication* 40 (2) (June): 103-127.

Bernoff, Josh and Charlene Li (2008). *Groundswell: Winning in a World Transformed by Social Technologies*. Boston, Mass: Harvard Business School Press.

Castells, Manuel. 2007. “Communication, Power and Counter-Power.” *International Journal of Communication* 1: 238-266.

Cypel, Sylvain. 2010. “Afghanistan: les revelations sur les coulisses de la guerre embarrassent Washington.” *Le Monde*, July 28.

de Borchgrave, Arnaud. 2010. “Gusher of WikiLeaks: Activists hope documents will undermine war support.” *The Washington Times*.

Domscheit-Berg, Daniel, and Tina Klopp. 2011. *Inside WikiLeaks*. New York: Crown Publishers.

Eco, Umberto. 1967. *Travels in Hyperreality*. London: Picador. (Cited in Taylor 2005, p. 640)

Eddlem, Thomas R. 2010. “Gingrich Calls Assange an ‘Enemy Combatant’.” *The New American*, December 9. http://thenewamerican.com/usnews/foreign-policy/5454-gingrich-calls-assange-an-qenemy-combatantq.

Gitlin, Todd. 1990. *The Whole World is Watching: Mass Media in the Making and Unmaking of the New Left*. Berkeley, CA: University of California Press.

Granovetter, Mark S. "The strength of weak ties." *American Journal of Sociology* (1973).

Hallin, Daniel. 1986. *The “uncensored war”: the media and Vietnam*. New York: Oxford University Press.

Hirschman, Albert O. 1990. *Exit, voice and loyalty: responses to decline in firms, organizations and states*. Cambridge, MA: Harvard University Press.

Kauffman, Sylvie. 2010. “WikiLeaks: le dossier irakien.” *Le Monde*, October 24.

Leigh, David, and Luke Harding. 2011. *WikiLeaks: Inside Julian Assange’s War on Secrecy*. London: Guardian Books.

Lessig, Lawrence. 2006. *Code 2.0*. Cambridge, MA: Basic Books.

Lessig, Lawrence. 2009. “Against Transparency: The Perils of Openness in Government.” *The New Republic*, October 9.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. 1st ed. Sebastopol CA: O’Reilly Media.

Ludlow, Peter. 2010. "WikiLeaks and Hacktivist Culture." *The Nation*, October 4.

Madrigal, Alexis. 2010. "The Unknown Blogger Who Changed WikiLeaks Coverage." *The Atlantic*, December.

Millar, Stuart. 2001. "For Hackers, Read Political Heroes of Cyberspace!" *The Guardian*, March 8.

Murray, Andrew. 2011. "Transparency, Scrutiny and Responsiveness: Fashioning a Private Space within the Information Society." *The Political Quarterly* 82 (4): 509-514.

Nissenbaum, Helen. 2004. "Hackers and the contested ontology of cyberspace." *New Media & Society* 6 (2): 195-217.

Ourdan, Remy. 2010. "Dans les coulisses de la diplomatie americaine." *Le Monde*, November 30.

Rosenzweig, Paul. 2011. "Lessons of WikiLeaks: The U.S. Needs a Counterinsurgency Strategy for Cyberspace" (2560). The Heritage Foundation Backgrounder (May 31). http://ssrn.com/abstract=1884336.

Ross, Andrew. 1991. *Strange Weather: Culture, Science and Technology in the Age of Limits*. London: Verso/New Left Books.

Sifry, Micah L. 2011. *WikiLeaks and the Age of Transparency*. Berkeley: Counterpoint.

Sklar, Urizenus. 2010. Understanding Conspiracy: The Political Philosophy of Julian Assange. *The Huffington Post*. December 8. http://www.huffingtonpost.com/urizenus-sklar/understanding-conspiracy-_b_793463.html.

Taleb, Nassim Nicholas. 2010. *The Black Swan.* New York: Random House.

Taylor, Paul A. 2005. "From hackers to hacktivists: speed bumps on the global superhighway?" *New Media & Society* 7 (5): 625-646.

Thiessen, Marc. 2010. "WikiLeaks must be stopped." *The Washington Post*, August 3, sec. Opinion.
http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080202627.html.

ABOUT THE AUTHOR

Nathalie Marechal: Ms. Marechal is a doctoral student in Communication at the University of Southern California's Annenberg School for Communication and Journalism. Her research interests include media and international relations, media history, international and comparative media, media ethics, technology and society, and cross-cultural communication.

The International Journal of Technology, Knowledge and Society explores innovative theories and practices relating technology to society. The journal is cross-disciplinary in its scope, offering a meeting point for technologists with a concern for the social and social scientists with a concern for the technological. The focus is primarily, but not exclusively, on information and communications technologies.

Equally interested in the mechanics of social technologies and the social impact of technologies, the journal is guided by the ideals of an open society, where technology is used to address human needs and serve community interests. These concerns are grounded in the values of creativity, innovation, access, equity, and personal and community autonomy. In this space, commercial and community interests at times complement each other; at other times they appear to be at odds. The journal examines the nature of new technologies, their connection with communities, their use as tools for learning, and their place in a "knowledge society".

The perspectives presented in the journal range from big picture analyses which address global and universal concerns, to detailed case studies which speak of localized social applications of technology. The papers traverse a broad terrain, sometimes technically and other times socially oriented, sometimes theoretical and other times practical in their perspective, and sometimes reflecting dispassionate analysis whilst at other times suggesting interested strategies for action.

The journal covers the fields of informatics, computer science, history and philosophy of science, sociology of knowledge, sociology of technology, education, management and the humanities. Its contributors include research students, technology developers and trainers, and industry consultants.

The International Journal of Technology, Knowledge and Society is a peer-reviewed scholarly journal.

ISSN 1832-3669