Strategies of Circulation Restriction in Whistleblowing

The Pentagon Papers, WikiLeaks and Snowden Cases

Philip Di Salvo
Usi-Lugano (CH)

Abstract: The Pentagon Papers, WikiLeaks and Edward Snowden are among the most topical whistleblowing cases where journalists got involved to publish articles based on leaked information. On occasion of these major leaks, strategies of circulation restrictions were activated in order to stop the dissemination of the leaked material. In the Pentagon Papers case, *The New York Times* first published the material and received a restraining order to stop the publication (Diamond 1993); WikiLeaks was targeted with digital DDoS attacks aimed at putting it offline. In the case of Edward Snowden, *The Guardian* was instead forced to physically destroy hard drives where leaked documents were allegedly stored (Greenwald 2014a). This paper analyses the evolution of content circulation restriction strategies and their effectiveness in whistleblowing cases by means of the three aforementioned case studies, focusing on the material nature of the leaked documents. The analysis focuses on issues of digital materialization, content circulation and journalism, contributing to the debate on these topics in STS.

Keywords: Whistleblowing; censorship; journalism; WikiLeaks; surveillance; materiality.

Corresponding author: Philip Di Salvo, Università della Svizzera Italiana, Via G. Buffi 13, CH-6900 Lugano (Switzerland). Email: philip.di.salvo@usi.ch.

1. Introduction: Analog and Digital Whistleblowing and Content Restriction Strategies

Whistleblowing is a process of information circulation set to bypass veils of secrecy in order to inspire change by using transparency and impact on public opinion as strategies (Callahan and Dworkin 1994). The history of journalism is full of topical whistleblowers who inspired impactful scoops and publications, for instance the Watergate scandal "Deep Throat" has been widely historicized, even in pop culture, as one

of the most famous instances of whistleblowing (Schudson 1992). In more recent times, different cases of whistleblowing in digital environments have gained global attention, such as the WikiLeaks "Megaleaks" in 2010 or the NSA surveillance scandal in the summer of 2013. Whistleblowing cases at different levels, not only those involving national interests or high-ranking institutions, are among those instances where journalism can act as evidence-supported effective watchdogs (Curran 2005) and as independent monitors of power (Strömbäck 2010, 185-187). They provide a public service for accountability and act in a more adversarial way towards those in power. As a form of dissent, whistleblowing may not be welcome from organizations that suffer an information leak. This could lead organizations to respond with strategies of information circulation restrictions in order to maintain control and prevent information from getting out. Retaliation against the whistleblower within the organizations is common (Johnson 2003, 91-114), but when the press and governmental or public bodies are involved, authorities may also engage in active censorship practices to stop the exchange of information from the whistleblower to the recipients or to prevent publication and circulation of the leaked information. Frequently used tactics include evoking the need for secrecy in matters of national security, legal actions and, in most extreme cases, active censorship (Carpenter 1995, 7-10).

This paper provides a comparison of content circulation restriction strategies in the context of whistleblowing in both analog and digital conditions, dealing with external whistleblowing cases involving journalists and media as recipients of leaks. Analysis of the evolution of applied circulation limitations strategies from an offline to an online context focuses on three different case studies: the Pentagon Papers (1971), WikiLeaks (2010) and Snowden's revelations about the NSA surveillance (2013). Thus, the paper is structured as follows: section 2 focuses on information circulation restriction strategies applied during the Pentagon Papers case; section 3 deals with the different strategies deployed in the digital context of WikiLeaks; and section 4 analyzes the technological implications of the restrictions applied in the Snowden case. We will be looking at whistleblowing cases mainly from one points of view: the content circulation restriction strategies put in action to stop the leaks. Particular attention will be given to how authorities tried to stop the diffusion of information. The theoretical analysis is drawn on a discussion from media materiality, crossed with philosophy of technology and journalism studies. The notion of whistleblowing has been common in communication and journalism jargon since the early 70s, when the term came to express a particular form of dissent in bureaucratic systems (Johnson 2003) based on information circulation. Whistleblowing scholars Marcia P. Miceli and Janet P. Near (1992, 15) have described the practice as the "disclosure of illegal, immoral or illegitimate practices under the control of their employers to persons of organizations that may be able to effect action". The definition clearly poses whistleblowing as an

information exchange between an individual holding information and recipients able to possibly make this information actionable in different ways. In connection with journalism, whistleblowers represent a unique resource in terms of information gathering and sourcing. Especially when it comes to secretarial organizations or closed environments, insights coming from insiders turned whistleblowers may work as leads or inspirations for possible journalistic investigations or can provide evidence for an investigative hypothesis. In contexts where excessive secrecy is applied (Fenster 2014) or Freedom of Information (FOI) laws are absent or inadequate, whistleblowers are an indispensable resource for accessing data or information for reporting. Where legal limitations are at stage, whistleblowers aid in circumventing legal limitations in situations warranted by public interest and journalists provide a conduit to reach the public. Both in offline and online instances, whistleblowers act as the vehicles of dissent to a specific authority.

In Hirschmann's terms (1970), whistleblowing happens when individuals facing wrongdoings are asked to decide among different response strategies: Exit, Loyalty or Voice. By opting for Voice, whistleblowers decide to operate "in opposition" – breaking a bond of loyalty in favor of pressing ethical demands. Danah Boyd (2013) has defined whistleblowing as a form of civil disobedience. This is particularly the case with "external whistleblowing" (Kaptein 2011): cases where the recipient of complaints and leaks are entities based outside of the involved organizations. Among all of the major changes imposed by digitalization to the media environment, there is also the reconstruction of the environment architecture on a "distributed structure", mutated from the Internet network structure (Arvidsson and Delfanti 2013, 76-77) and the dematerialization of communication means in favour of its strong and growing digitalization. This wider phenomenon also brought to a growing availability of digitalized information. In 2007, over 300 exabytes of stored digital data existed globally (Hilbert and Lopez 2011). As a vast majority of communication exchanges moved online, content circulation restriction strategies also turned to the web (Byfield 2011; Deibert 2009). This built up a growing approach to censorship and content filtering that Rebecca MacKinnon (2012, 31-50) effectively calls "Networked Authoritarianism".

The spectrum of censorship on the Internet interests both authoritarian regimes and democratic countries. Despite some utopian and deterministic perspectives that view the Internet as an eminently libertarian and emancipatory tool, the ubiquity of digital censorship is on the rise. The Chinese case is a commonly analyzed example of Internet control and censorship (Negro 2013), but instances are visible in other countries as well. Additional instances include but are not limited to India (MacKinnon 2012, 91-94), Turkey (Akgül and Kırlıdoğ 2015) and Russia (Simon 2015, 54-62). A global perspective on the widespread control over

digital communications and publications is annually tracked in the "Enemies of The Internet" report[1] published by Reporters Without Borders (2014). According to Zubair Nabi (2014), around 60 countries in the world somehow actively censor the Internet.

2. Analog Restrictions: The Ellsberg Case and the Pentagon Papers

When it comes to content circulation restrictions in the context of whistleblowing and journalism, few cases are more representative than the publication of the Pentagon Papers[2] in 1971. The Papers, officially titled "History of United States Decision Making Process on Vietnam Policy, 1945-1967," was a "7000-page top secret study of U.S. decision making in Vietnam" (Ellsberg 2002, xi). They were released to the press by Daniel Ellsberg, a former analyst for the U.S. intelligence community turned whistleblower. The corpus of leaked classified documents outlined an insider perspective on the Vietnam War. Since the Papers were classified, the U.S. authorities intervened to prevent the publication of the material by the American Press. *The New York Times* published on June 13th 1971 and this was followed by an immediate reaction from the Nixon administration to obtain an order of prior restraint (Diamond 1993, 117-118) and they subsequently filed for an injunction on June 15th with the federal district court in New York. The injunction was granted and *The New York Times* received a temporary restraining order that completely stopped the publication of the newspaper for five days (Lewis 2012). The legal case eventually reached the Supreme Court, where the government alleged that the publication of the material by *The New York Times* was harmful to national security. However, the Supreme Court ruled that the allegations were insufficient to give the restraint order legitimacy (Rudenstine 1998, 301-320).

By underlining the power of the First Amendment, the Pentagon Papers case ended up strengthening the constitutional freedom of the press in the United States (Diamond 1993, 118; Lewis 2012) and is now considered a milestone for press freedom. Retrospectively, the U.S. government's attempt to restrict and censor information with an order of prior restraint on matters of national security was a direct attempt to legally stop the publications pursued within the borders of democracy. It was a circulation restriction strategy targeting the physical distribution of the information and the medium, namely, the 1971 print editions of newspapers featuring the material. The analog nature of the leak of the Pentagon

[1] Available here: http://12mars.rsf.org/2014-en/.

[2] The Pentagon Papers were fully declassified in 2011 and put online. They are available here: http://www.archives.gov/research/pentagon-papers/.

Papers forced Ellsberg to rely on legacy media for the publication of the revelations. At the time, legacy media was the only institution able to perform the gatekeeping function and provide the reach necessary for the information to become news (White 1950; Gans 1979).

As argued by Joel Simon (2015, 13), the legal comprehensive censorship against powerful institutions such as national newspapers implies a hierarchical approach, intrinsic of the analog media environment in which they were perpetuated. This hierarchical approach was also strengthened by the climate of excessive secrecy within the Nixon administration during the Vietnam War. This later culminated in the explosion of the Watergate scandal in 1972, which contributed to increasing the pressure over Nixon until his resignation in 1974 (Carpenter 1995, 80-81). Thus, the Pentagon Papers case falls under Christopher Woolmar's (1990) definition of censorship: the information released is controlled through distribution channels, rather than controlling the information itself. Moreover, from the perspective of the authorities, restricting the reach of the leak by blocking the publication of newspapers holding the documents was the only available strategy to restrain the information circulation.

This element is also tightly connected with the analog print nature of the Pentagon Papers corpus. The Papers originally existed only in physical form and were shared exclusively within a very small and elite community, mainly staff members granted access to the offices where the Papers were stored. The Papers were available in only fifteen original duplicates and Ellsberg had access to one of them (Gitelman 2011). The actual act of whistleblowing was also influenced by the analog nature of the print documents. Ellsberg himself explained (2002) the mechanic and painful difficulties he and his colleague Anthony Russo had to face in manually copying all the seven thousand pages of the books with a Xerox 914 machine. The physical and technological limitations of the copying and carrying of the documents influenced the number of copies that Ellsberg and Russo could create. In his memoir of the events, Ellsberg (2002, 372-375) recalls how crucial it was to have more than one single copy of the corpus, in order to avoid possible seizures. When the injunction reached *The New York Times*, it was the pressure of sharing the Papers with another 15 newsrooms willing to publish, including *The Washington Post* and the *Boston Globe*, that made injunctions useless and let the Pentagon Papers reach the public. If only one newspaper would have been in possession of a single copy of the Papers, an injunction against that particular publication would have caused a complete blackout against the leak. When other newspapers started publishing, thanks to the other copies of the Papers available, it was literally impossible to stop all the publications at the same time.

The backfire of a censorship attempt that leads to wider circulation of content has been defined as the "Streisand Effect", a notion accepted by the academic community to define censorship attempts that end up being counterproductive (Jansen and Martin 2015; Nabi 2014). The effect is

named after singer Barbra Streisand, who attempted to restrict circulation of a picture of her home from a public website, which led to a much wider viral circulation. Although this term was coined in the context of digital censorship, the Streisand Effect is also illustrated by the publication of the Pentagon Papers and the backfire of the governments censorship attempt. As noted by Jansen and Martin (2015), other instances of the Streisand Effect have appeared in non-digital times and, according to Evgeny Morozov (2011, 121), date back to Ancient Greek times. In the next section, the focus will shift to content circulation restriction strategies in a digital context, demonstrating how strategies in this context have led to a similar backfire reaction on a much larger scale.

When it comes to the Pentagon Papers case, it is possible to argue that the fully material circulation restriction strategy put in action against the first US newspapers publishing the material has been quite insufficient, as other publications picked up the source material in order to get it out and it would have been simply impossible to imagine a legal blockage against all the involved media. As discussed earlier, this was possible mainly because of the existence of several copies of the original Papers. Otherwise, with the eventual seizure of the content, the circulation of the leaked information would have been completely blocked. When it comes to the practice of whistleblowing, instead, the analog nature of the Papers was also the possible limitation to its own efficiency: to create copies of the original content was technologically complicated and very difficult to scale. In the next two sections we will dig into two digital cases, in order to analyze whether digitalization reinforced whistleblowing practices and the consequent circulation restriction strategies.

3. Digital Restrictions: The WikiLeaks Case

WikiLeaks, launched in 2006, proposed a different approach to whistleblowing, relying on the affordances of digital technologies. WikiLeaks provided on its own website an encrypted dropbox where whistleblowers could submit documents and tips in a safer and anonymous way. In the first 10 years of operation, WikiLeaks has been publishing several leaks, with a spike in terms of impact and interest in 2010. Thanks to a massive leak of digital materials, provided by Chelsea Manning, WikiLeaks had access to more than 600'000 classified files coming from the US intelligence and army archives. The publication of that information was done working closely with some major news outlets, such as *The New York Times*, *The Guardian* and *Der Spiegel*. With its own approach, WikiLeaks has become one of the most powerful voices in the field of whistleblowing in the digital era.

In the previous section, we discussed how the Pentagon Papers leak happened in an analog context where legacy media and newspapers were strong gatekeepers of news. That situation and process underwent a

complex and radical disruption with the rise of the web. As Axel Bruns puts it (2005, 13): "digital media like the World Wide Web function according to different models than print or even the electronic broadcasting media, and as a result, gates kept by news organizations can now be bypassed". The result of this switch of power facilitated by digitalization pushed the role of traditional media towards a new function of "gatewatchers," shaping a new networked relationship status between traditional media and new irregular news providers (Beckett 2012, 147-160). Although gatekeeping has changed its status and role, it is definitely still "alive and kicking" (Heinderyckx 2015); however, the power legacy media and newspapers have to shape the flow of news has diminished.

Whistleblowers in the digital age profit from having more tools and strategies than their analog counterparts. WikiLeaks, in particular, exemplifies the power of digital encryption tools in anonymizing and circulating the accomplishments of a whistleblowing act online (Bruns 2014). WikiLeaks established a new "e-tactic" for whistleblowing in the digital age. In the context of online activism, an e-tactic is defined as an opportunity to complete a given task - profiting from the web's distinct affordances, without the need for physical copresence (Earl and Kimport 2011, 7-8). WikiLeaks, thanks to its own online anonymous leak submission system, gave whistleblowers an easier and faster tool to leak information by proving the opportunity to deliver vast amount of digital content in an easier and faster way. Major cases such as the "Afghan War Logs", the "Iraq War Logs" and "Cablegate", resulted in 600,000 digital files in total being leaked by whistleblower Chelsea Manning in 2010. The material was published in cooperation with major international news outlets and illustrates how powerful the WikiLeaks e-tactic has been.

Distributed Denials of Service (DDoS) are hacking attacks that are an "increasingly common Internet phenomenon capable of silencing Internet speech, usually for a brief interval but occasionally for longer" (Zuckerman et al. 2010). They are realized by harnessing a large number of remotely controlled computers and by address an overwhelming numbers of requests to an Internet domain, until it goes offline (Zuckerman et al. 2010). WikiLeaks itself had to cope with content circulation restriction strategies, mainly digital. As Rebecca MacKinnon recalls (2012, 82-83), in 2010 when WikiLeaks started publishing the Cablegate documents, a corpus of more than 250 thousand U.S. diplomatic cables on a dedicated site, the site domain was targeted with untracked DDoS attacks that put it offline for some hours and made its content unavailable (Schonfeld 2010). Similar attacks happened again in 2012 (Kerr 2012). DDoS attacks can be used as content circulation restrictions to silence websites, as illustrated with WikiLeaks. Their use has been documented in Russia, where newspaper *Novaya Gazeta* was a censorship target (Zuckermann et al. 2010) and also in Saudi Arabia and Belarus, among other instances (Morozov 2011, 108). But DDoS attacks are ambivalent strategies and, besides being possible tools of censorship, are being increasingly used as a hacktivist

e-tactic for protests (Earl and Kimport 2011, 7-8). As anthropologist Gabriella Coleman notes (2014, 136-142), use of DDoS extends a long tradition of disruptive activism by transferring analog tactics such as sit-ins or occupations online. The hacker collective Anonymous brought DDoS to a higher level of efficiency during its operations against WikiLeaks' adversaries, when companies involved in the banking blockade against WikiLeaks saw their flagship websites targeted and put offline by DDoS attacks although without suffering any damage or data losses.

Beside DDoS, there are additional forms of digital circulation restriction strategies when it comes to whistleblowing: online filtering, for instance, is one of the most common strategies. Online filtering involves making websites unavailable to selected users or from selected locations, both at the TCP/IP (Transmission Control Protocol/Internet Protocol) and DNS (Domain Name System) level (Murdoch and Anderson 2008). The practice is a daily routine under the Chinese Great Firewall (Powers and Jablonski 2015, 168-172), in Bahrain (OpenNet Initiative 2005), Pakistan (Nabi 2014) and also in countries such as Burma, Syria, Thailand and Tunisia, among others (Deibert 2009). Filtering also plays a part when it comes to restricting access to content originating from whistleblowing acts. Regarding WikiLeaks, federal workers in the United States were unable to access the website on the Internet because of a ban imposed on the site domain on computers hosted in federal offices – including the Library of Congress.

Despite putting such strategies in place, leaked documents were nevertheless easily accessible through major news outlets that collaborated with WikiLeaks, such as *The Guardian* (MacAskill, 2010). At the same time, the U.S. authorities pressured Internet Service Providers to prevent access to WikiLeaks (Jansen and Martin 2015), with a public-private partnership in censorship (Cannon 2013). These attempts sparked the Streisand Effect, thereby causing a chain reaction with the formation of "mirror sites" for WikiLeaks. The mirror sites were replications of the contents of WikiLeaks, however they were hosted under different domains worldwide. According to journalistic reports (Warrick and Pegoraro 2010), when WikiLeaks was under attack in 2010 the number of mirror sites grew from 200 to more than 1000 in few days, making a complete restriction against WikiLeaks almost impossible.

The organizational nature of WikiLeaks is also based on the potential of its own peculiar organizational structure, such as not having a newsroom, a national affiliation or an identifiable organization chart. The technological structure of WikiLeaks followed the same pattern: spread throughout different legislative contexts with servers located in several different countries (Bruns 2014). This technological structure created very complicated circumstances to restrict access to what WikiLeaks puts online. The combination of the organizational and technical structure of WikiLeaks, the support obtained through the proliferation of mirror sites and the backlash of the DDoS attack perpetrated by Anonymous made

content restriction strategies against WikiLeaks almost useless (Cannon 2013). When DDoS attacks against WikiLeaks peaked, there was an escalation in launching mirror sites: 355 websites were available in December 2010 (Schroeder 2010). Nabi's (2014) definition of the Streisand Effect as "unintentional virality of any information, online or otherwise, as a consequence of any attempt to censor, suppress and/or conceal it" is illustrated through the backlash when authorities tried to silence WikiLeaks and mirror sites appeared in hundreds. The power of WikiLeaks stays definitely in the "networked" environment in which it operates and the rise of the Networked Society had a lasting effect on whistleblowing (Benkler 2011; McCurdy 2013).

The near impossibility of silencing WikiLeaks is also due to the technological changes to the kinds of documents and information whistleblowers are able to carry and leak to external recipients. As Gina Neff notes (2014), "the change of a medium, say from paper documents to digital documents, can have an enormous impact on how these roles play out" and this applies to all the players involved in a whistleblowing act. If we consider the Pentagon Papers and WikiLeaks as the embodiment of two different phases in the evolution of external whistleblowing, differences emerge by analyzing the kinds of documents they were able to deliver to the press. The Pentagon Papers consisted of hard copies of a classified leaked report, whereas the WikiLeaks publications took place in a highly digitalized environment where impressive quantities of classified information is routinely stored in digital archives and networks. In the time between 2001 and 2011, the U.S. federal government digitized 475 million pages of federal records (The White House 2011). Taking a closer look at these numbers, it is possible to frame them within the wider phenomenon of "datafication" (Mayer-Schönberger and Cukier 2013). This concept involves in a constantly less-physical way every aspect of the contemporary age in which information is being shared among individuals and institution, toward a massive and pervasive extension of digitalization of information in form of digital files.

In the shift from an offline to a data ecosystem, it is important to focus on the nature of documents that whistleblowers can now access and leak. In order to download the documents which were later leaked to WikiLeaks, Chelsea Manning, the whistleblower behind the major WikiLeaks' revelations, accessed a top secret network from her workstation in Iraq. This involved searching through classified digital documents on five different archives, including the New Centric Diplomacy database (Zetter 2011). U.S. diplomatic cables, such as those included in the Cablegate leak, are usually transferred in PDF form via email using a State Department classified network called ClassNet. They are later stored in PST form, the format used by Microsoft Outlook to compress and store data, in order to be searchable. Manning downloaded a massive amount of files from the SNAP computer and saved them on CD-RWs (Ambinder 2010). For instance, the 250 thousand files that comprised the Cablegate corpus

was 1.6 GB in size. It could later be delivered by Julian Assange to *The Guardian* using a USB flash device, as journalist David Leigh recalls (2010).

The details above fit perfectly in Floridi's (2010) theorization of how digitalization and "datafication" were able to completely change the concepts of *objects* and *processes*. Following this path, growing digitalization caused the loss of "physical connotation" of objects which, in digital form, can easily be considered independent from their origin. In this sense, in comparison to the original Pentagon Papers stored in the RAND offices in Washington, it is intrinsically more difficult to individuate the *original* copies of the diplomatic cables Manning was able to copy and download. Following Floridi's proposed framework (2010), digital objects are "typified in the sense that an instance of an object […] is as good as its type". In this sense, digital objects are perfectly clonable and all copies are interchangeable with one another. Consequently, to create copies is considerably easier than it used to be in the offline environment in which Daniel Ellsberg was operating. Is has been calculated that it would take approximately 41.8 hours of straight printing at a rate of 100 pages a minute to print out the entire Cablegate leak (McCurdy 2013). Chelsea Manning's leak to WikiLeaks, instead, was only one click away and despite its vastness could be downloaded, copied and shared with relatively low computing skills and agility (Zetter 2011).

When discussing the nature of digital artifacts, it is also important to consider their distributed nature (Kallinikos, Aaltonen, Marton 2010). Digital artifacts are essentially "borderless" entities that cannot be identified within clear physical borders, in contrast to physical entities such as books or paper documents. This distributed nature of digital artifacts evolves into the substantial impossibility to control the spread of leaked documents once they are extracted from archives and disseminated. This is also at the core of the likelihood of the Streisand Effect in situations where a circulation restriction strategy is applied to digital whistleblowing cases in order to prevent the spread of information. This Effect is further illustrated by WikiLeaks: despite the aforementioned attempts, WikiLeaks has never been completely silenced and is still online and operational. Moreover, since the explosion of the WikiLeaks revelations, also the scale of journalistic leaks has escalated. For instance, the Panama Papers, published in spring 2016, consisted of 2,6 TB of digital files (11,5 m documents), a size which is almost twenty-six times bigger than the original WikiLeaks Cablegate dataset (Obermaier et al. 2016). The growth in terms of size of the leaks is interesting in at least two different directions. First, it shows how affordances involved in digital storage and carrying of files can really facilitate the practice of whistleblowing, particularly when large amounts of documents are involved. Secondly, it shows also how, despite the content circulation restriction strategies analyzed in this paper and the attempts, both technological and political, to stop the spreading

of leaks, the practice of whistleblowing in the digital era seems to get more and more relevance in terms of effectiveness and scale.

4. Re-materialized Restriction: The Snowden Case

In the summer of 2013, the disclosure of a vast amount of classified information from the NSA and its own allied agencies by whistleblower Edward Snowden sparked an unprecedented debate about digital freedom and rights and the role of journalism as a fourth estate. When it comes to journalistic practices, the case represents one of the most peculiar examples of whistleblowing in the digital era. Although not realized through a whistleblowing platform such as WikiLeaks, it proved how crucial encryption and digital security tools are in securing journalists' online communication with their sources (Greenwald 2014a; Ziccardi 2015, 193-198; Schneier 2015, 143-145). The number of digital files that Edward Snowden was able to download and hand over to journalists is still unclear (Greenwald 2014b) but the revelations have had a global impact. The reach has extended far beyond the newspapers that were first given access to the leaked material (*The Guardian* in the UK and *The Washington Post* in the US), amenable to different levels of media attention and engagement (Di Salvo and Negro 2015).

Consequences for the publication of this sensitive classified material have been harsh: Edward Snowden himself has been charged with different felonies, including some under the U.S. 1917 Espionage Act. His American passport was invalided and he is currently living in Russia, where he was granted temporary asylum after having spent 4 months in the international area of the Moscow airport seeking to reach South America from Hong Kong. Journalists who worked on the analysis of the original classified material were put under police investigation in the UK (Gallagher 2015) and *The Guardian*'s David Miranda was detained at the Heathrow airport for nine hours under anti-terrorism laws while allegedly travelling with documents from the Snowden cache (McGrath Goodman 2015; Paterson 2014, 34).

As with the Pentagon Papers and WikiLeaks cases, the Snowden case also exemplifies the application of circulation restriction strategies against news outlets covering the leak in order to prevent information distribution. One day after *The Guardian* published the first article related to the PRISM NSA surveillance program, the Minister of Defence in London issued confidential D-Notices to several media outlets asking not to publish content related to the Snowden leak, in order to protect national security interests (Halliday 2013). D-Notices are only advisory, different from the injunctions against the U.S. press seen in the Pentagon Papers case, however they are nonetheless a legal form of circulation restriction.

Digital censorship has been documented on other occasions on a smaller scale. For instance, U.S. troops in the Middle East, South Asia and Afghanistan can't access *The Guardian* site, as it is blocked to prevent

access to the Snowden material and related journalistic analysis (Ackerman 2013). Concerning the Snowden disclosures, the most evident and emblematic case of content circulation restriction strategy was when UK authorities and the GCHQ, the British equivalent of the NSA, asked *The Guardian* to hand back classified digital documents obtained from Edward Snowden. The former editor-in-chief, Alan Rusbridger (2013) recalls that the formal requests followed other previous attempts to restrict the publications, including the threat of a proper prior restraint against the newspaper. In July 2013, tensions reached the top and in order to resist governmental requests, *The Guardian* decided to destroy the digital archives of Snowden leaked files in London, under the supervision and instructions of two GCHQ agents (Borger 2013). Files were stored with high-level digital security standards in encrypted and airgapped machines in a secure room in the London newsroom under constant human surveillance, as security researchers and hackers Al-Bassam and Tynan recall (2015). As indicated by national security agents, *The Guardian* staffers had to physically destroy computers and hard-drives where the documents were stored by using angle-grinders and revolving drills. A "degasseur" was also used, an appliance that destroys magnetic fields and erases data from computer drives in order to eliminate any possible trace of the leaked material (Harding 2014; McLaughlin 2015). Despite the digital nature of the material and the fully digitalized environment where files were processed and published, the circulation restriction strategy targeted the physical support where documents were eventually stored. This strategy was able to circumvent the limitations imposed by adopting digital-only circulation restriction strategies, as seen in WikiLeaks case.

The adoption of such an approach to content restriction may have different motives, including being another attempt of intimidation, as noted by scholar Chris Paterson (2014, 35). If in the Pentagon Papers case the destruction of the original print leaked document would have caused the loss of the original material, in the case of digitalized files such as those leaked by Snowden, copies of the original cache could have been created and shared much more easily. In order to avoid the consequences of a possible legal injunction, *The Guardian* proactively moved the files outside of UK legislation. This provided its New York headquarters and journalist Glenn Greenwald (based in Brazil) with access, who was also in possession of the files (Rusbridger 2013). Despite the intervention to destroy the physical supports for the digital materials, the distributed nature of the digital files (Kallinikos et al. 2010) once again played a major part in dismantling the circulation restriction strategy. Hence, *The Guardian* was able to keep publishing from its U.S. newsroom. Moreover, they also provided *ProPublica* and *The New York Times* with access to the files in order to broaden the publication spectrum of the Snowden cache with more journalists and news outlets in the United States (Beaujon 2013).

This case once again illustrates how content circulation restrictions in whistleblowing cases can actually lead to a wider extension of the reach

and yet another exemplification of the Streisand Effect in the journalism context. When it comes to restrictions themselves, instead, the Snowden case and the way authorities tried to block the work of *The Guardian* bring in another interesting aspect of circulation restrictions in the digital era. The physical destruction of the hard drives, including its own intrinsic symbolic nature, could be associated with the notion of "re-materialization", a trend that has been analyzed in different field of technology studies and consumer cultures as a trend when describing the still persistent analog characterizations of the current digital environment. In the context of this paper, it could be possible to extend this notion into the analysis of physical content circulation restriction strategies within the Snowden case seen as a way to prevent digital information to spread.

Vincent Mosco (2014) and Tung-Hui Hu (2015) have focused on cloud computing as a physical industry, contradicting the commonly accepted notion of the "cloud" as a completely ephemeral digital entity with borderless connotation. Cloud computing companies, Mosco argues, rely on extensive physical facilities and gigantic data centers in order to work, an aspect which is commonly neglected in public and journalistic discourse. On a similar note, Evgeny Morozov referred as well to the frequently neglected technological connotations of cloud storage (2013, 72-75). Conversely, Paolo Magaudda (2011; 2012) analyzed how materiality regained an important role for digital music consumption, namely with the introduction of material objects such as the iPod. The hard disk and the vinyl disc, even in times of strong digitalization, have gained a crucial role in shaping consumption practices. As Magaudda (2012) puts it, re-materialization brings together a complexity of phenomena, practices and technologies, which are once again providing digital artifacts with a strong emphasis on materiality. This happens because material objects such as the destroyed *The Guardian*'s hard disks and laptops[3], pure physical entities, are re-gaining importance in the storage of media content, even in a highly digitalized environment.

Whistleblowing has encountered fundamental changes due to digitalization and the intrinsic nature of digital artifacts that are more and more frequently leaked by whistleblowers over the Internet. As digital security researcher Bruce Schneier recalls (2015, 159-161): "technology is making secrets harder to keep, and the nature of the Internet makes secrets much harder to keep long-term. The push of a "send" button can deliver gigabytes across the Internet in a trice. A single thumb drive can hold more data every year. Both governments and organizations need to assume that their secrets are more likely to be exposed, and sooner, than ever before".

[3] In 2015, the Victoria and Albert Museum in London hosted an exhibition named "All These Things Belongs to You", where objects of public interest were included in the museum collection. Among them was one of *The Guardian*'s smashed computers (http://thecreatorsproject.vice.com/blog/smashed-snowden-laptop-slated-for-london-museum-show).

When it comes to the restriction of circulation of digital content, despite the basic impossibility to stop a digital leak, it comes as no surprise that the attention of authorities remains focused on the physical supports that contains the material. It is interesting to see how materiality arises again when a leak needs to be stopped and all of the digital methods to prevent the information from spreading have proved to be almost powerless.

5. Conclusion

This paper provided a comparison of content circulation restriction strategies in the context of whistleblowing in both analog and digital conditions. The Pentagon Papers, WikiLeaks and the Snowden cases are examples of how whistleblowing acts have caused reactions from authorities aiming to prevent leaks from reaching the public. As discussed, in the case of the 1971 Pentagon Papers, the U.S. government acted with legal prior restraints against the press in order to completely stop the publication of newspapers for some days. Content published online by WikiLeaks capitalized on the networked and digital nature of Julian Assange's website and instead was restricted through digital censorship and filtering tactics on several occasions. On the other side, during the publication of the Snowden leak, restricting the circulation of the leaked content happened in a re-materialized way, through physical destruction of the hard drives where digital documents were stored.

Despite the vast digitalization reached over the course of time in the cases analyzed, it is possible to see how content circulation restriction strategies often still rely on materiality. This demonstrates that the need for an approach focused on materiality still matters when it comes to whistleblowing. Instances of circulation restrictions strategies in the context of whistleblowing seem to confirm how specific trends of continuity between the analog and digital contexts can be identified, rather than a clear separation (Balbi and Magaudda 2014: 13-16). As discussed, re-materialization is also strictly connected with the efficiency of the restriction strategies. Both analog and digitalized cases illustrated instances of the Streisand Effect as a backfire to the censorship attempts. Further, it is possible to argue that in the Snowden case, the physical connotation of the restriction strategy put in place was meant to be a stronger level of censorship to be applied to an otherwise uncontrollable leak. Its efficiency, as discussed, remains disputable. This paper contributes to the analysis of whistleblowing in the digital era and to the related content circulation restriction strategies that could arise.

References

Ackerman, S. and Roberts, D. (2013) *US army block access to Guardian website to preserve 'network hygiene'*, in "The Guardian", June 28. Available at: http://www.theguardian.com/world/2013/jun/28/us-army-blocks-guardian-website-access (Retrieved May 16, 2016).

Akgül, M. and Kırlıdoğ, M. (2015) *Internet censorship in Turkey*, in "Internet Policy Review", 4 (2) Available at: http://policyreview.info/articles/analysis/internet-censorship-turkey (Retrieved October 15, 2015).

Al-Bassam, M. and Tynan, R. (2015) *How to Destroy a Laptop with Top Secrets*. Presentation at *Chaos Communication Camp 2015*. Available at: https://media.ccc.de/browse/conferences/camp2015/camp2015-6799-how_-to_destroy_a_laptop_with_top_secrets.html#video&t=85 (Retrieved October 15, 2015).

Ambinder, M. (2010) *WikiLeaks: One Analyst, So Many Documents. How could Bradley Manning alone have leaked so much classified material?*, in "National Journal", November 29. Available at: http://www.nationaljournal.com/white-house/wikileaks-one-analyst-so-many-documents-20101129 (Retrieved October 15, 2015).

Arvidsson, A and Delfanti, A. (2013) *Introduzione ai media digitali*, Bologna, Il Mulino.

Balbi, G. and Magaudda, P. (2014) *Storia dei media digitali. Rivoluzioni e continuità*, Roma-Bari, Laterza.

Beaujon, A. (2013) *NYT/Guardian/ProPublica collaboration: It speaks for itself, apparently*, in "Poynter.org", September 6. Available at: http://www.-poynter.org/news/mediawire/223000/nytguardianpropublica-collaboration-it-speaks-for-itself-apparently/ (Retrieved October 15, 2015).

Beckett, C. (2012) *WikiLeaks. News in the Networked Era*, Cambridge, Polity Press.

Benkler, Y. (2011) *Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, in "A. Harv. CR-CLL Rev", 46, 311.

Borger, J. (2013) *NSA files: why the Guardian in London destroyed hard drives of leaked files*, in "The Guardian", August 20. Available at: http://www.the-guardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london (Retrieved October 15, 2015).

boyd, d. (2013) *Whistleblowing is the new civil disobedience*, in "Apophenia", July 19. Available at: http://www.zephoria.org/thoughts/archives/2013/07/19/edward-snowden-whistleblower.html (Retrieved October 15, 2015).

Bruns, A. (2005) *Gatewatching. Collaborative Online News Production*, New York, Peter Lang.

Bruns, A. (2014) *WikiLeaks: The Napster of Secrets?*, in "International Journal of Communication", 8, pp. 2646-2651.

Byfield, P. (2011) *The spectrum of internet censorship*, in "Focus on International and Information Work", 42(3), pp. 107-113

Callahan, E.S. and Dworkin, T.M. (1994) *Who blows the whistle to the media, and why: Organizational chracteristics of media whistleblowers*, in "American Business Law Journal", 32 (2), pp. 151-184.

Cannon, S.C. (2013) *Terrorizing WikiLeaks: Why the Embargo Against WikiLeaks Will Fail*, in "Journal on Telecommunication & High Tech", L (11).

Carpenter, T.G. (1995) *The Captive Press. Foreign Policy Crises and the First Amendment*, Washington, DC, Cato Institute Press.

Coleman, G. (2014) *Hacker, Hoaxer, Whistleblower, Spy. The Many faces of Anonymous*, New York, Verso Books.

Curran, J. (2005) *What Democracy Requires of the Media*, in G. Overholser and K.H. Jamieson (eds.) *Institutions of American Democracy: The Press*, Oxford, Oxford University Press.

Deibert, R. J. (2009) *The geopolitics of internet control*, in A. Chadwick and P.N. Howard (eds.) *Censorship, Sovereignty, and Cyberspace. The Routledge Handbook of Internet Politics*, London, Routledge, pp. 323-336.

Di Salvo, P. and Negro, G. (2015) *Framing Edward Snowden: A comparative analysis of four newspapers in China, United Kingdom and United States*, in "Journalism", online before print July 24.

Diamond, E. (1993) *Behind The Times: Inside the New New York Times*, Chicago, University of Chicago Press.

Earl, J. and Kimport, K. (2011) *Digitally Enabled Social Change. Activism in the Internet Age*, Cambridge, Mit Press.

Ellsberg, D. (2002) *Secrets: A Memoir of Vietnam and the Pentagon Papers*, New York, Penguin.

Fenster, M. (2014) *The implausibility of Secrecy*, in "Hastings Law Journal", 65(2).

Floridi, L. (2010) *Information. A Very Short Introduction*, Oxford, Oxford University Press.

Gallagher, R. (2015) *U.K. Police Confirm Ongoing Criminal Probe of Snowden Leak Journalists*, in "The Intercept", July 24. Available at: https://theintercept.com/2015/07/24/uk-met-police-snowden-investigation-journalists/ (Retrieved October 15, 2015).

Gans, H.J. (1979) *Democracy and the News: A Study of CBS Evening News, NBC Nightfly News, Newsweek, and Time*, New York, Pantheon Books.

Gitelman, L. (2011) *Daniel Ellsberg and the Lost Idea of the Photocopy*, in S. Jülich et al. (eds.) *History of Participatory Media. Politics and Publics 1750-2000*, London, Routledge, pp. 112-124.

Greenwald, G. (2014a) *No Place to Hide. Edward Snowden, the NSA and the U.S. Surveillance State*, New York, Metropolitan Books.

Greenwald, G. (2014b) *Keith Alexander Unplugged: on Bush/Obama, 1.7 million stolen documents and other matters*, in "The Intercept", May 8. Available at: https://theintercept.com/2014/05/08/keith-alexander-unplugged-bushobama-matters/ (Retrieved October 15, 2015).

Halliday, J. (2013) *MoD serves news outlets with D notice over surveillance leaks*.

The Guardian, June 17. Available at: http://www.theguardian.com/world-/2013/jun/17/defence-d-bbc-media-censor-surveillance-security. (Retrieved October 15, 2015).

Harding, L. (2014) *Footage released of Guardian editors destroying Snowden hard drives*, in "The Guardian", January 31. Available at: http://www.theguardian.com/uk-news/2014/jan/31/footage-released-guardian-editors-snowden-hard-drives-gchq (Retrieved October 15, 2015).

Heinderyckx, F. (2015) *Gatekeeping Theory Redux*, in T.P. Vos and F. Heinderyckx (eds.) *Gatekeeping in Transition*, New York, Routledge.

Hilbert, M. and Lopez, P. (2011) *The World's Technological Capacity to Store, Communicate, and Computer Information*, in "Science", 332 (6025), pp. 60-65.

Hirschmann, A.O. (1970) *Exit, Voice and Loyalty: Reponses to Decline in Firms, Organizations, and States*, Cambridge, Harvard University Press.

Hu, T. (2015) *A Prehistory of the Cloud*, Cambridge, Mit Press.

Jansen, S. and Martin, B. (2015) *The Streisand Effect and Censorship Backfire*, in "International Journal of Communication", 9, pp. 656-671.

Johnson, R.A. (2003) *Whistlelowing. When It Works and Why*, London, Lynne Rienner Publishers.

Kallinikos, J., Aaltonen, A. and Marton, A. (2010) *A Theory of Digital Objects*, in "First Monday", 15 (6-7).

Kaptein, M. (2011) *From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing*, in "Journal of Business Ethics", 98 (3), pp. 513-530.

Kerr, D. (2012) *WikiLeaks endures a lengthy DDoS attack*, in "Cnet.com", Available: http://www.cnet.com/news/wikileaks-endures-a-lengthy-ddos-attack/ (Retrieved October 15, 2015).

Leigh, D. (2010) *How 250,000 US embassy cables were leaked*, in "The Guardian", November 28. Available at: http://www.theguardian.com/world/2010-/nov/28/how-us-embassy-cables-leaked (Retrieved October 15, 2015).

Lewis, K. (2012) *Wikifreak-out: The Legality of Prior Restraints on WikiLeaks' Publication of Government Documents*, in "Wash. UJL & Pol'y", 38, 417.

MacAskill, E. (2010) *US blocks access to WikiLeaks for federal workers*, in "The Guardian", December 3. Available at: http://www.theguardian.com/world-/2010/dec/03/wikileaks-cables-blocks-access-federal (Retrieved October 15, 2015).

MacKinnon, R. (2012) *Consent of the Networked. The Worldwide Struggle for Internet Freedom*, New York, Basic Books.

Magaudda, P. (2011) *When Materiality "Bites Back". Digital Music Consumption Practices In The Age Of Dematerialization*, in "Journal of Consumer Culture", 11 (1), pp. 15-36.

Magaudda, P. (2012) *What Happens To Materiality In Digital Virtual Consumption?,* in M. Molesworth and J. Denegri-Knott (eds.) *Digital Virtual Consumption*, London, Routledge, pp. 111-126.

Mayer-Schönberger, V. and Cukier K. (2013) *Big Data. A Revolution That Will Transform How We Live, Work and Think*, London, John Murray.

McCurdy, P. (2013) *From the Pentagon Papers to Cablegate: How the Network Society Has Changed Leaking*, in B. Brevini et al. (eds.) *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, New York, Palgrave MacMillan, pp. 123-145.

McGrath Goodman, L. (2015) *David Miranda and the Human-Rights Black Hole*, in "Newsweek", January 7. Available at: http://www.newsweek.com/2015/01-/16/edward-snowdens-helpers-296988.html. (Retrieved October 15, 2015).

McLaughlin, J. (2015) *The Way GCHQ Obliterated The Guardian's Laptops May Have Revealed More Than It Intended*, in "The Intercept", August 26, Available at: https://theintercept.com/2015/08/26/way-gchq-obliterated-guardians-laptops-revealed-intended/ (Retrieved October 15, 2015).

Miceli, M.P. and Near, J.P. (1992) *Blowing the Whistle. The Organizational and Legal Implications for Companies and Employees*, New York, Lexington Books.

Morozov, E. (2011) *The Net Delusion: The Dark Side of Internet Freedom*, New York, PublicAffairs.

Morozov, E. (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*, New York, PublicAffairs.

Mosco, V. (2014) *To the Cloud. Big Data in a Turbulent World*, London, Routledge.

Murdoch, S.J., and Anderson, R. (2008) *Tools and technology of Internet filtering*, in R.J. Deibert et al. (eds.) *Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, Mit Press, pp. 57-72.

Nabi, Z. (2014) *~~Resistance~~ censorship is futile*, in "First Monday", 19 (11). Available at: http://firstmonday.org/ojs/index.php/fm/issue/view/428 (Retrieved October 15, 2015).

Neff, G. (2014) *Learning from documents: Applying new theories of materiality to journalism*, in "Journalism", 16 (1).

Negro, G. (2013) *Chinese Internet Governance - Some Domestic and Foreign Issues*, in R. Radu et al. (eds.) *The Evolution of Global Internet Governance - Principles and Policies in the Making*, Berlin, Springer, pp. 141-156.

Obermaier, F., Obermayer, B., Wormer V. and Jaschensky W. (2016) *About the Panama Papers*, in "Panamapapers.suddeutsche.de", Available at: http://-panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/ (Retrieved April 13, 2016).

OpenNet Initiative. (2005) *Internet Filtering in Bahrain. A Country Study*. OpenNet Intiative. Available at: https://opennet.net/sites/opennet.net/files/ONI_-Bahrain_Country_Study.pdf (Retrieved October 15, 2015).

Paterson, C. (2014) *War Reporters Under Threat. The United States and Media Freedom*, New York, Pluto Press.

Powers, S.M. and Jablonski M. (2015) *The Real Cyber-War. The Political Economy of Internet Freedom*, Champaign, The University of Illinois Press.

Reporters Without Borders (2014) *Enemies of the Internet 2014: entities at the heart of censorship and surveillance*. Available at: http://12mars.rsf.org/2014-en/ (Retrieved October 15, 2015).

Rudenstine, D. (1998) *The Day the Presses Stopped: A history of the Pentagon Papers Case*, Berkeley, University of California Press.

Rusbridger, A. (2013) *David Miranda, schedule 7 and the danger that all reporters now face*, in "The Guardian", August 19. Available at: http://www-.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters (Retrieved October 15, 2015).

Schneier, B. (2015) *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*, New York, W. W. Norton & Company.

Schonfeld, E. (2010) *WikiLeaks Reports It Is Under A Denial Of Service Attack*, in "TechCrunch", November 28. Available at: http://techcrunch.com/2010/11/-28/wikileaks-ddos-attack/ (Retrieved October 15, 2015).

Schroeder, S. (2010) *WikiLeaks Now Has Hundreds of Mirrors*, in "Mashable.com", December 12. Available at: http://mashable.com/2010/12/06/wikileaks-mirrors/#bfji_U6fiaqy (Retrieved October 15, 2015).

Schudson, M. (1992) *Watergate: A Study in Mythology*, in "Columbia Journalism Review", 31 (1), p. 28.

Simon, J. (2015) *The New Censorship. Inside the Global Battle for Media Freedom*, New York, Columbia University Press.

Strömbäck, J. (2010) *Democracy and the Media: A Social Contract*, in S. Dosenrode (ed.) *Freedom of the Press: On Censorship, Self-censorship, and Press Ethics*, Baden-Baden, Nomos.

White, D. M. (1950) *The Gatekeeper: A Case Study in the Selection of News,* in D. Berkowitz (ed.) *Social Meanings of news: A Reader*, Thousand Oaks, Sage, pp. 63-71.

The White House (2011) *By the Numbers: 475 Million*. Available at: http://-www.whitehouse.gov/blog/2011/11/28/numbers-475-million (Retrieved October 15, 2015).

Warrick, J. and Pegoraro, R. (2010) *WikiLeaks' resilience shows strength of Internet-age lifelines*, in "The Washington Post", December 9. Available at: http:-//www.washingtonpost.com/wp-dyn/content/article/2010/12/08/AR2010-120807287.html (Retrieved October 15, 2015).

Woolmar, C. (1990) *Censorship*, London, Wayland Books.

Zetter, K. (2011) *Forensic Expert: Manning's Computer Had 10K Cables, Downloading Scripts*, in "Wired", December 18. Available at: http://www-.wired.com/2011/12/cables-scripts-manning/ (Retrieved October 15, 2015).

Ziccardi, G. (2015) *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, Cortina.

Zuckerman, E. (2010) *2010 Report on Distributed Denial of Service (DDoS) Attacks*, report, The Berkman Center for Internet & Society at Harvard University. Available at: https://cyber.law.harvard.edu/publications/2010/DDoS-_Independent_Media_Human_Rights. (Retrieved October 15, 2015).