National Journal of Advanced Research
ISSN: 2455-216X; Impact Factor: RJIF 5.12
Received: 16-05-2019; Accepted: 19-06-2019
www.allnationaljournal.com
Volume 5; Issue 3; July 2019; Page No. 27-38

Challenges to freedom of expression in the digital World: Lessons from Jamal Khashoggi, Saudi Journalist

Dr. S Krishnan[1], Nighat Nazir[2]
[1] Assistant Professor, Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India
[2] Research Scholar, International Islamic University, Islamabad, Pakistan

Abstract
Two developments the death of Jamal Khashoggi, a Saudi Journalist leading to the Arab Spring, and the Panama Papers releases have demonstrated individual's capacities in advancing free expression, transparency, and social change through the use of online and social media movements. However, these events have also highlighted new sets of challenges and threats that interfere with, and restrict, such media usage.
On October 2nd, 2018 Jamal Khashoggi, a well-known journalist and critic of the Saudi government, walked into the country's consulate in Istanbul, where he was murdered. It is suspected he was killed and dismembered by Saudi agents inside the consulate. The Washington Post ran what is called his final column, which lamented the lack of freedoms across the Arab world, which has resulted in mass amounts of its citizens to be uninformed or misinformed. Dreaming of an oasis for freedom of expression, he criticized governments "whose very existence relies on the control of information" that "have been given free rein to continue silencing the media at an increasing rate." Was Khashoggi's death a result of governments attempt to control the flow of information and thus was hesilenced for his criticism of the Saudi government? This recent development has demonstrated the capacities of individuals and movements in advancing free expression, transparency and social change through the use of media, whether print, online or social in response to Khashoggi's death. However, it also highlights a new set of challenges and threats that interfere with, and restrict, such media uses. Expansion in technologies like Facebook; Twitter and Instagram played a vital role for the promotion of freedom of expression on the Internet. While at the same time, the media has remained a powerful tool in making or breaking the access of information to the ordinary citizen. Media can manipulate evidence and distort information and can also use the same set of information to portray contradictory meanings and interpretations of the information. In Europe and US media corporations such as BBC and CNN are some of the most powerful tools to promulgate information and propaganda at national level and international level. This includes online news blogs, websites, magazines and live broadcast news channel and programs. One prime example was the instance of Terry Jones and Greet Wilder where media was used as a forum to express their anti-Islamic views. Acting upon the notion of freedom of speech no authority prevented them from promulgating hate speech against Islam. Blasphemous cartoon contest was the heinous act which hearting the religious sentiments on the name of freedom of
In this article, an analytical framework for understanding and investigating these contemporary restrictions to freedom of expression, based on the dimensions of information control, access to infrastructure, critical resources and applications, surveillance, and physical repression will be presented. The overview takes into account current trends such as the use of intermediaries in control regimes, and provides a global perspective that incorporates restrictions in both the East and West. The 'fighting words doctrine' in the context of freedom of expression will be thoroughly examined. How free expression advocates have contested these practices, and discuss whether their agendas confirm the issue areas highlighted above will also be outlined. The restrictions to, and the advocacy for, free online communication demonstrate some of the key struggles and contestations on freedom of expression in the current digital media environment, the strategic points of intervention by different actors (states, businesses, and various civil society groups), and the requirements for "modern freedom of expression" will all be examined.

Keywords: freedom of expression, Jamal Khashoggi, media

1. Introduction
Over the past two years, two major international developments – the Panama Papers releases and the Arab Spring – have shaken the course of politics and communication. They have demonstrated the enormous capacities of individuals and movements in advancing free expression, transparency and social change through the use of online and social media. However, they have also highlighted new sets of challenges and threats that interfere with, and restrict, such media uses.

The case of Panama Papers points us to the challenge of state secrecy but also to new forms of private censorship through legal threats (using libel and defamation laws), the denial of vital resources (web space, financial services, apps), and thereby the privatization of internet policing. The Arab Spring has demonstrated the vulnerability of internet infrastructure, the use of digitally-mediated surveillance by the state, and the naturalization of content restrictions which are increasingly implemented in both 'authoritarian states' and the 'democratic West'. Both cases, furthermore,

highlight the persistence of criminalization, physical violence, and other forms of repression as obstacles to freedom of expression, even with the insurgence of social media and other contemporary or informal media.

It is pertinent, then, to take stock of the effects that the current turmoil may have on future practices, challenges, and understandings of free expression, and particularly, to consider the implications of digital environments. In this article an analytical structure for understanding and investigating these dynamics will be proposed. The observations presented here will be based on the experiences of the Panama Papers saga and of social media use in the Arab Spring, but will incorporate other current policy developments. In particular, we will discuss the dimensions of information control, access to infrastructure, surveillance, critical resources, and physical violence, and explore how these have changed in light of recent events.

Further, how far Panama Papers and the Arab Spring have triggered civil society campaigns that contest restrictions to communication flows and seek policy change will be explored. The Icelandic Modern Media Initiative (IMMI) which has declared its mission as safeguarding "modern freedom of expression" [1] as well as current initiatives and proposals for media policy change in the Arab world and elsewhere will also be outlined. These practical experiences will provide insights on how digital restrictions are perceived by free expression advocates, and they can therefore serve to test the model proposed below.

Together, these dynamics demonstrate some of the key struggles and contestations on freedom of expression in the current digital media environment. They highlight strategic points of intervention and control by different actors (particularly states, businesses, and civil society groups), and they point us to some of the core requirements for freedom of expression in an online world [2].

2. Citizen journalism opportunities and social media revolutions

Citizen-based and self-organized media production are not new phenomena. For decades, media activists and community groups have created newsletters, alternative magazines, community radio and TV, and have applied communicative action repertoires such as posters, music, video, theatre and culture jamming [3]. Alternative and grassroots media have played a crucial role in political struggles, social movement activism and democratic change. Examples include the use of cassette tapes in earlier revolutions in the Middle East [4], and the Samizdat movement in the former Soviet bloc [5].

The Internet has allowed politically minded people to not only build on these experiences, but also to expand them significantly. The global Indymedia network [6] with its open posting mechanism, created around the turn of the Millennium, was the first platform for citizen journalism where everyone could publish their stories and make them available to a global audience, and where the content of a news site was almost entirely user-generated. While Indymedia remained largely in the realm of social and political activism, the emergence of blogging as a mass phenomenon and of commercial social networking platforms such as Facebook and Twitter transformed the production of publically-available mediated messages into an aspect of everyday life – for those with access to the necessary technology. Soon, the established media started to incorporate user-generated content into their offer (e.g., CNN's Reporter), while "the people formerly known as the audience" [7], i.e. the new generation of 'netizens', were just as happy to use the new technological opportunities to bypass the gatekeepers of the traditional media business.

Participating in the production of media messages, information and knowledge has thus become a worldwide phenomenon and has changed the ways in which understandings and interpretations about the world are created. Wikipedia has become a widely used knowledge source. Efforts to democratize communication increasingly include self-organized media production, in addition to (and often surpassing) traditional advocacy approaches [8]. As the Indymedia slogan goes: "Don't hate the media, be the media [9]."

The role of social media in processes of democratization and political change has been observed and emphasized repeatedly over the past decade, from the use of SMS for protest mobilizations in Spain and in the Philippines in the early 2000s to the use of Twitter and Facebook in Iran, Moldova and elsewhere at the end of the decade, leading to claims of 'Twitter" and 'Facebook-Revolutions', and overall to great enthusiasm about the democratic potential of information and communication technology (ICT). As "liberation technology", as Diamond notes, social media and other ICT applications enable "citizens to report news, expose wrong-doing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons the of freedom [10].

The Arab Spring, i.e. the protests and uprisings in several countries of North Africa and the Middle East in spring 2011, semed to confirm this claim and placed the liberation technology paradigm firmly on the political, academic and public agendas. Social media's impact varied per country. Social networks played an important role in the rapid and relatively peaceful disintegration of at least two regimes in Tunisia and Egypt, where the governing regimes had little or no social base. They also contributed to social and political mobilization in Syria and Bahrain, where the Syrian "hacktivist" group, SEA (Syrian Electronic Army), was established in order to target and launch cyber attacks against the political opposition and news websites. While nine out of ten Egyptians and Tunisians responded to a poll that they used Facebook to organize protests and spread awareness [11], the role of the social network wasn't central in countries like Syria and Yemen, where there is little Facebook penetration. Statistics show that during the Arab Spring the number of users of social networks, especially Facebook, rose dramatically in most Arab countries, particularly in those where political uprising took place. Libya was an exception to this statistic, because at the time they still seemed to be suffering from low Internet access and consequently had reduced traffic.

Government reactions to social media activism differed significantly from country to country. While the Tunisian government blocked only certain routes and websites through which protests were coordinated, the Egyptian government went further, first blocking Facebook and Twitter, then completely blocking access to the internet in the country for five days, beginning January 28, 2011. The Internet blackout in Egypt failed to stop the protests, and instead seemed to fuel them [12]. However, although social media played a measurable role in gathering people to protest and spreading awareness of the unfair treatment of

Arab citizens, it did not create a final solution to the unrest and was not a deciding factor in resolving the nations' conflicts.

In Tunisia, Egypt and elsewhere, social networking was used for protest mobilizations and reporting, and allowed for the creation of forums for free speech and for shared criticism of the social and political situation. It helped to mobilize a critical mass of protesters, to organize logistical details, and generated a social space for developing critical discourses where an open public sphere did not exist [13]. Social media became 'effective catalysts' [14] of change and amplifiers of social movement activism. Some participants and observers even claimed that communication platforms constituted the fundamental triggers for revolution. In the words of Egyptian activist (and Google employee) Wael Ghonim: "If you want to free a society, just give them Internet access" [15]. Others have been more cautious, pointing to a "functional differentiation [16]" in which the Internet was used extensively by individuals with technical knowledge and publishers of information, whereas the broader masses and media consumers relied more on satellite television for accessing information.

The Panama Papers are 11.5 million leaked documents that detail financial and attorney–client information for more than 214,488 offshore entities [17]. The documents, some dating back to the 1970s, were created by, and taken from, Panamanian law firm and corporate service provider Mossack Fonseca, and were leaked in 2015 by an anonymous source. The documents contain personal financial information about wealthy individuals and public officials that had previously been kept private. While offshore business entities are legal (see Offshore Magic Circle), reporters found that some of the Mossack Fonseca shell corporations were used for illegal purposes, including fraud, tax evasion, and evading international sanctions.

"John Doe", the whistleblower who leaked the documents to German journalist Bastian Obermayer [18] from the newspaper *Süddeutsche Zeitung* (SZ), remains anonymous, even to the journalists who worked on the investigation. "My life is in danger", he told them. In a May 6, 2016, statement, John Doe cited income inequality as the reason for his action, and said he leaked the documents "simply because I understood enough about their contents to realize the scale of the injustices they described". He added that he had never worked for any government or intelligence agency and expressed willingness to help prosecutors if granted immunity from prosecution. After SZ verified that the statement did in fact come from the source for the Panama Papers, the International Consortium of Investigative Journalists (ICIJ) posted the full document on its website [19]. SZ asked the ICIJ for help because of the amount of data involved. Journalists from 107 media organizations in 80 countries analyzed documents detailing the operations of the law firm [20]. After more than a year of analysis, the first news stories were published on April 3, 2016, along with 150 of the documents themselves [21]. The project represents an important milestone in the use of data journalism software tools and mobile collaboration. The documents were dubbed the Panama Papers because of the country they were leaked from; however, the Panamanian government expressed strong objections to the name over concerns that it would tarnish the government's and country's image worldwide, as did other entities in Panama and elsewhere. This led to an advertising campaign some weeks after the leak, titled "Panama, more than papers". Some media outlets covering the story have used the name "Mossack Fonseca papers"

Development agencies and foreign affairs ministries in the West and North have quickly adopted the liberation discourse and have explored ways to support ICT use for democratic change in developing and authoritarian countries. As "net activists are the new democracy fighters" [22], the Swedish, US and other governments have provided aid for online freedom of expression and the use of social media in the service of global democratic change [23]. This strong interest outside the region results, at least, from one of the key effects of social media use: the dissemination of local news to, and thus the interaction with, a global audience, leading to a virtual global public sphere. Critics have noted that international observers were often better informed about local events than local participants, yet from a comfortable distance. As Hofheinz points out (regarding the 'Twitter Revolution' in Iran in 2009): "While people in New York cafés were forwarding tweets that gave them the thrilled feeling of partaking in a revolution, Iranian conservatives tightened their grip on power using YouTube videos and other Internet evidence to identify and arrest opposition activists" [24].

Dubbed the "Twitter Revolution," the Iranian 2009 Green Movement sparked the advent of social media platforms as political organizing tools. Iranians took to the streets after the 2009 presidential election, protesting Mahmoud Ahmadinejad, and demanding his removal from office. Before elected president, Ahmadinejad served as the mayor of Tehran, where he built a violent reputation for himself, consistently violating human rights, instilling fear in Iranians throughout the country. Having just risen to popularity, Twitter became the way Iranians communicated with one another and with those outside the country. Iranians used the social media platform to post important logistical protest information, as well as posting updates to inform those outside of the country on the happenings.

Iran's civil resistance movement is unique because the government's tight control of media and the Internet has spawned a generation adept at circumventing cyber roadblocks, making the country ripe for a technology–driven protest movement. As the government has cracked down on everything from cellphone service to Facebook, Twitter has emerged as the most powerful way to disseminate photos, organize protests, and describe street scenes in the aftermath of the contested June 12 (2009) election. Iranians' reliance on the social-networking tool has elevated it from a banal way to update one's friends in 140-character bursts to an agent for historic changes in the Islamic Republic.

Similar public interest, although less favourable amongst Western governments, was raised by Panama Papers, particularly regarding its release of US diplomatic cables since 2010 in what has become known as "Cablegate". The revelations by the leaks platform, including its earlier releases of the Afghan War Diaries, the Iraq War Logs, information exposing government corruption in North Africa and the secret dealings of the financial industry, amongst many others, have sparked intense debate in the realms of international diplomacy, journalism, and broader society. As a media organization with the goal to gather and publish original source material on a variety of issues,

Panama is different from the case of social media use during the Arab Spring. But just as the latter, it highlights practices of innovative ICT use for social change and of by-passing information restrictions. The Panama Paper has managed to expand the range of publicly available information and to push media organizations to report on issues they had not covered extensively so far. It has placed the issues of secrecy and transparency on the international agenda, demonstrated the roles and capacities of technical experts in challenging major powers, and indirectly contributed, through its broader support network, to a new wave of cyber-activism that has (e.g., in the form of the Anonymous network) established new action repertoires and approaches for social movements [25].

Beyond the specific opportunities that all these cases provide for democratic citizen action and for free expression, they seem to suggest a broader trend in which the power relations between individuals and institutions are shifting in favor of the former. We may be witnessing a paradigm change in which the capacities of individuals and civil society groups occupy a more prominent role than the institutions and collective bodies that much of social science has traditionally dealt with [26]. In that sense, the Arab Spring and Panama Papers may confirm some of the dreams and predictions of cyber-libertarians and techno-utopians who have long criticized traditional institutions as outdated and praised the power of individuals in cyberspace [27].

However, while individuals have demonstrated their capacities to transform the social and political environment through the use of communication technology, their actions have been closely monitored by state and business actors, and restrictions to free information exchanges in cyberspace have emerged. Thus the cases of the Arab Spring and WikiLeaks not only tell us something about the power of applying ICT for social change, but also highlight new practices of censorship and other restrictions, and thus point us to some of the corner-stones for protecting, as well as limiting, future freedom of expression. I will turn to these in the next section.

3. Obstacles to free expression

Just as social media has been used by activists to advance political change, it has also been used by governments to control and deter such action, for example by identifying protesters (as in Tunisia, Syria and Iran [28]. Vital online resources and funding streams have been cut to weaken dissident organizations (as happened to Wikileaks) [29], and social media applications or even the Internet as such have been shut down when they became a threat to an existing political order (as in Egypt in 2011) [30]. Citizen journalists who used to celebrate the unprecedented opportunities to by-pass the traditional gatekeepers of the media industry by publishing on a plethora of new online media are now facing new sets of gatekeepers.

The enthusiasm for 'liberation technology' in the midst of the Arab Spring has increasingly given way to a more sober, and in some cases even alarmed [31], observation of the obstacles and restrictions to free online communication which are emerging rapidly. In the following paragraphs, a more systematic structure of these obstacles will be proposed and discussed. This may assist in developing criteria for free expression in digital environments, as well as policy agendas for its protection.

3.1 Information Control

The most immediate practice in controlling communication flow is to curtail access to information. Panama has highlighted this problem by making sensitive government or business information available for public access. Various state's interest in preventing its citizens from accessing information that has been collected about them or in their name has been significant, and even where new laws have been set in place to expand access to information, political pressures quickly emerged to reduce their scope and re-introduce restrictions [32].

The filtering of web content has become a particularly common practice across the globe. According to the OpenNet Initiative (ONI), 47% of the world's Internet users experience online censorship, with 31% of all Internet users living in countries that engage in 'substantial' or 'pervasive' censorship [33]. While the Chinese 'Great Firewal' and filtering practices in other authoritarian countries, including in the Middle East, have been well documented, filtering is also common in Western democracies. Typically, it is initiated with the rationale of restricting illegal or otherwise unacceptable content such as child pornography, but increasingly it is expanding to other fields [34]. For example, access to the WikiLeaks website has been blocked in US government facilities. In April 2012, the British High Court ruled that the file sharing website 'The Pirate Bay' must be blocked by UK Internet service providers (ISPs) because of alleged copyright infringements on the part of Pirate Bay [35].

As the UK example shows, intermediaries such as ISPs and search engines are increasingly enlisted by governments to control and restrict access to internet content. Intermediaries thus become 'proxy censors'" [36]. Prior to the Pirate Bay decision, agreements between the government and ISPs in the UK had already led to the automatic and mandatory filtering of all online pornography in the country [37].

Whereas filtering is typically initiated by governments, private forms of censorship have equally expanded. These include libel threats and restrictive uses of anti-defamation law, for example by companies against critical reporting on their activities and business practices, and what is termed SLAPP (Strategic Litigation Against Public Participation) [38]. In countries such as the UK, strict libel laws have become a key tool for businesses (and celebrities) to prevent investigative reporting. Although Panama became famous due to its fight against state secrets, some of its earlier scoops, such as the revelation on toxic waste dumps off the African coast by a British company, contained information that had been banned from being published for libel reasons [39].

A prominent example of the latter has been the case of the Kaupthing Bank in Iceland which was granted an injunction against the national public broadcaster RUV in August 2009, just minutes before RUV news were to report extensively on Kaupthing's secret financial dealings which had contributed to the collapse of the Icelandic economy. The injunction stopped the story from being aired, and instead RUV had to point its audience to the Panama website where detailed documents on the case had been posted (thereby making Panama instantly famous in Iceland). Even more than large media organizations, grassroots alternative and citizen media have been vulnerable to threats of legal action as they typically lack

the resources to defend themselves in court. Such threats regularly lead to self-censorship [40].

3.2 Access to Infrastructure

The role of intermediaries in current censorship regimes points us to a second level at which restrictions occur – the infrastructure level. The almost complete Internet shut-down in Egypt in February 2011, followed by similar acts elsewhere in the Arab region, has highlighted the vulnerability of the supposedly 'borderless' cyberspace. The US debate over an Internet kill-switch, and the UK proposals on temporary blockages of specific online services, such as Facebook and Twitter, in times of political turmoil, have further demonstrated the willingness of governments to intervene in online communication infrastructure [41].

The debate on net neutrality – initiated in the US and increasingly spreading to other jurisdictions – has highlighted the role of network providers as potential gatekeepers who have an interest in favoring the content and applications of some information sources and services over others, and who might block access to disfavored sites or require a special fee. This provides particular challenges for non-commercial content and small businesses, and for oppositional and dissident news sources, but it may affect all media organizations as network providers may favour particular business partners [42].

More crudely, governments are increasingly considering physical restrictions of online access for certain users. So-called 'three strikes' rules are now widely discussed, and have been implemented in countries like France. They restrict people's access to the Internet in cases where they have been found to repeatedly violate, for example, intellectual property law by downloading copyrighted content [8]. In the US, content owners and Internet service providers (ISPs) have agreed to the Copyright Alert System, a 'six-strike' plan that includes sending educational alerts and potentially hijacking browsers and slowing or temporarily blocking the Internet service of users accused of copyright infringement. The mechanism by-passes governmental and judicial oversight, and therefore puts both the definition of, and the punishment for, copyright infringement in the hands of content owners and ISPs [43].

While new sets of restrictions appear online, the more traditional questions of who has, and who is denied, access to broadcast infrastructure and the radio-frequency spectrum are not necessarily resolved. Frequency allocation in response to political favours remains a widespread phenomenon and auctioning off frequencies to the highest bidder is common practice, with questionable democratic implications [44]. Community broadcasting, i.e. participatory and non-profit radio and TV that is self-managed by a civil society association or a citizen group, remains outlawed in many countries, while in others it has to compete for frequencies with commercial broadcasters or is severely limited due to discrimination regarding its reach and funding [45]. The transition from analogue to digital broadcasting provides new challenges: while the US digital radio system IBOC discriminates in favor of incumbent license-holders, the European system DAB focuses on standardized national coverage and introduces a new set of private sector gatekeepers – the multiplex operators – that may be able to make decisions on who is carried on the multiplex and who is excluded [46].

3.3 Critical resources and applications

Online publications and services typically require a broader set of resources, such as funding, and an infrastructure that allows them to generate, access and use those resources. Actors that are able to block access to such infrastructure and thus to cut off critical resources constitute important gatekeepers. Their role became particularly apparent in December 2010 when Amazon, Paypal and others closed the services they had previously provided for WikiLeaks and Panama Papers, depriving the leaks platform of its domain name and of access to necessary funds in the middle of a major release that required both [47]. This 'denial of service', as Benkler has put it, propelled the providers of critical services into the spotlight of the debate on WikiLeaks and on freedom of expression. It helped clarify and perhaps revise our understanding of so-called 'cloud' services which – despite the beautiful picture of a floating data cloud that is accessible always and everywhere – exert significant power in allowing and disallowing access to information and services, and control the gates that enable Internet users to participate in increasingly cloud-based communication exchanges [48]. Further, the actions by Amazon, Paypal, and other large e-companies demonstrated the vulnerability of these services to political interventions, as they coincided with pressure from members of the US political elite, both inside and outside government [49].

The relative success of the 'denial of service' strategy in the Panama case has certainly had an influence on the repertoires of control applied by state actors [50]. For example, the proposed 'Stop Online Piracy Act' SOPA which was discussed in the US in early 2012 included the blocking of access from critical resources as means of punishment. According to the proposed (but eventually unsuccessful) legislation, the main counter-measure against a website that facilitates piracy would have been to cut it off from funding and other private sector services. Again, this approach demonstrated the increasing trend for internet intermediaries to be used to police the network and exert punishment, and thus the privatization of internet policing [51].

App stores have come to occupy positions of similar influence that have allowed them to censor apps based on, for example, political disagreements or pressures. Again, WikiLeaks provides a key example, as Apple removed the WikiLeaks app in late 2010, following the Cablegate releases. Beyond such specific gatekeeping functions, the increasing role of apps and similar services for accessing online information has been criticized as they limit what users can do online and therefore may transform the traditionally open cyberspace into a set of "sterile appliances tethered into a network of control" [52].

3.4 Surveillance

State reactions to the Arab Spring have highlighted the increasing governmental practices of social media surveillance to generate information on protesters and dissidents. In Tunisia and Iran, authorities have used Facebook to scrape user data [53]. Syrian opposition supporters were targeted using Trojans – programs that covertly install spying software onto infected computers – and phishing attacks which steal YouTube and Facebook login credentials. In one case, the malware was included in software that would purportedly offer Skype encryption and thereby allow anonymous communication. When installed,

it allowed the attacker to capture webcam activity, record key strokes and steal passwords [54]. The region has thus become a laboratory for developing and testing surveillance concepts. Many of the necessary technical tools and services have been provided by technology companies in the West, as projects such as WikiLeaks' Spyfiles and Bugged Planet have shown [55].

The Panama case, too, has problematized the widespread public use of social networking and its increasing integration into surveillance regimes. In their quest to contain the Panama phenomenon and learn more about its supporters, US authorities turned to social media companies. Twitter was forced to hand over the account data of known Panama activists and their followers, and one can only speculate which other online services received the same requests and complied quietly [56]. Google publishes the numbers of requests by state authorities for the disclosure of its user data in its 'Transparency Report', and it reports that it received 5,950 such requests by the US government in the first six months of 2011 alone (i.e., 1000 a month or 33 a day), a number which is up 70% from 2010. Google has complied with 93% of the requests [57, 58].

Our two cases demonstrate a trend towards the dramatic expansion of digitally-mediated surveillance and data retention. With the ubiquity of electronic communication, the "capacity of the state to gather and process information about its citizens and about the resources and activities within its space is growing by orders of magnitude" [59]. These opportunities are increasingly exploited, and new legal frameworks allowing for broad and systematic surveillance have been implemented in some countries, and are being discussed in others. Current examples include the European Data Retention Directive, the proposed 'lawful access' legislation in Canada, and the proposed Cyber Intelligence Sharing and Protection Act (CISPA) in the US [60]. CISPA, if adopted, would allow government and businesses to monitor private communication, share users' private information, and effectively suspend any privacy considerations in the name of a vaguely defined notion of 'cybersecurity' [61]. New surveillance policy currently discussed in the UK would require ISPs to install eavesdropping hardware that allows governmental agencies to monitor all communication on social media, Skype calls and email communication as well as logging every site visited by Internet users. Says privacy expert Gus Hosein: "The government is proposing to force companies to collect information [...] on everyone's communications, all of the time. No democratic country has pursued a similar policy to date – the UK will find itself aligned with China and Iran if this proposal goes ahead" [62].

The Data Retention Directive, CISPA and others apply and expand the trend of enlisting private intermediaries in control regimes. They facilitate, legalize and enforce the collection of personal Internet data by private Internet companies as well as the sharing of that information with the government. CISPA, moreover, would allow for a broad range of 'counter-measures' that may include to "block online entities such as Panama or Wikileakes sites accused of copyright infringement" [63].

3.5 Physical repression

Finally, a much cruder yet persistent threat to free online expression encompasses criminalization, physical violence, imprisonment, and other forms of direct physical repression. The imprisonment of bloggers in the Arab world has repeatedly demonstrated these non-digital and non-mediated restrictions to freedom of expression [64]. In post-Mubarak Egypt, thousands of dissidents continue to be tried in military courts, among them numerous bloggers and social media users, who have made critical comments of the military, governing authorities, and religion, have been punished with prison sentences [65].

Panama Case has reminded us that practices of repression are not limited to certain regions and 'non -democratic' states. Alleged whistleblower Bradley Manning has spent (at the time of writing this article) two years in solitary confinement, without a trial and under circumstances which the United Nations special rapporteur on torture has called cruel, inhuman and degrading [66]. The attempts to charge Julian Assange, and the calls for his assassination by leading US politicians, provide further examples.

Globally, Internet activists who provide communications infrastructure for social movements or publish oppositional content have been subject to police operations such as house raids or have been incriminated through the use of anti-terrorism legislation. Servers and other technical infrastructure have been seized, often with questionable justifications [67]. In a recent example, in April 2012, US Federal authorities removed a server that was operated by the European Counter Network (ECN), the oldest independent ISP in Europe, from a colocation facility shared by the alternative non-profit Internet organizations Rise up Networks and May First/People Link in New York City [68].

3.6 Cross-cutting Issues

Value systems differ across the globe, thus so do the backgrounds and reasons for these various types of interventions regarding free online expression. In some societies questions of decency, religion, specific historical circumstances, or the respect of eminent personalities require caution, and in some instances, compromises to unrestricted freedom of expression. The most widespread reason, though, remains the protection of social and political stability, and thus the maintenance of an established social order. In the words of Kuwait's Information Minister, laws to regulate the use of social networking sites such as Twitter are needed in order to "safeguard the cohesiveness of the population and society" [69].

When that order, or 'cohesiveness', is threatened by protests and activism, restrictions to free communication are put in place, and dissident behaviour may lead to draconian punishment. Events during both the Arab Spring and the Panama saga have highlighted these dynamics, both in terms of the extent of interventions into communication processes and the severity of punishment. As examples from different regions of the world, the East and the West, they also demonstrate that restrictions are not limited to authoritarian states. In fact, governmental debates and proposals in the wake of the London riots in the UK in August 2011 mirrored some of the responses by Arab governments during the Arab Spring. Protesters were identified by the authorities through their use of social media, proposals included the temporary shut-down of social networking during protest situations, and merely communicating about the riots on social media led to severe punishment, including multi-year prison sentences [70].

If the maintenance of stability is a key reason for governmental interventions, intellectual property protection

is a close second. The expansion of intellectual property law has, in itself, provided challenges to publishers and disseminators of information as it restricts access to information. In what has been termed the 'second enclosure', we are witnessing a trend towards the commodification of knowledge and its removal from the public domain [71]. And as we have seen in the previous sections, intellectual property violations have been the rationale for wide-reaching interventions into the uses of both content and infrastructure. Legal initiatives such as SOPA and the international anti-counterfeiting treaty ACTA are to provide a discursive and regulatory framework for such interventions [72].

As the types and the scale of interventions at both the content and infrastructure level differ significantly across countries, internet users experience different applications and content in different jurisdictions. As Bambauer notes: "There is no longer one Internet. Technological censorship by countries worldwide means that how the Net appears depends upon where you access it [73]."

4. Policy initiatives in response to communication restrictions

Free online communication has typically been advanced and enabled by technical development and expertise, and so a prime strategy to deal with the restrictions outlined in the previous section has been to by-pass them at the technical level. Internet activists in Arab countries have applied anonymizing tools such as TOR, have experimented with strategies for secure online communication and have, at times, been supported by research centers, civil society groups and various companies elsewhere [74]. Panama and other content and infrastructure providers have used sophisticated server networks to avoid being cut off from internet infrastructure, particularly by placing their servers in countries with beneficial laws that prevent or reduce the risk of censorship and surveillance. Panama Papers supporters, for example, those connected with the Anonymous network, have responded with technical direct action, such as distributed denial of service (DDoS) attacks, on the restriction of access by Paypal, Amazon and others on WikiLeaks' resources, and to the online restrictions put in place by governments in the Middle East [75].

While these technical strategies make up an important part of civil society responses to the challenges presented here, we can also observe a different approach that focuses on policy, rather than technology, and aims at changing the legal environment. Such initiatives can tell us something about how the restrictions described in the previous section are perceived by free expression advocates, and they can therefore serve as test cases for the model proposed above.

4.1 The icelandic modern media initiative (IMMI)

The Icelandic Modern Media Initiative (IMMI) provides an interesting example for a national policy advocacy initiative that addresses some of the challenges and restrictions, and offers a specific focus [76]. IMMI emerged in the context of the financial collapse of the Icelandic economy in late 2008. This initiative was set up to change the development model of the country which had, until then, thrived as a safe haven for banks and financial services. Instead of the secrecy and the suppression of information that accompanied the old model and that had become disastrous for Iceland's economy, society and democracy, IMMI has aimed at transforming Iceland into a transparency haven and a favourable environment for media and investigative journalism. Local social and media activists, supported by international civil society organizations, have created a bundle of legal and regulatory proposals to "protect and strengthen modern freedom of expression". WikiLeaks was instrumental in starting the initiative: WikiLeaks activists raised the idea of a possible transparency haven, provided knowledge on relevant laws in other countries, and developed some of the thematic corner-stones together with local and international experts.

Not surprisingly, IMMI's understanding of "modern freedom of expression" thus focuses on the area of information control [77]. At its core is the concern to prevent the suppression of content by both public and private actors. IMMI has initiated the development of a new Freedom of Information Act to enhance access for journalists and the public to government-held information and to end the previous culture of secrecy. It has proposed measures to limit libel tourism, prior restraint, and strategic law suits that serve to block the flow of legitimate information – "legal harassment" of media and publishers, as IMMI puts it [78]. The group also initiated a new law on source protection, making it illegal for media organizations to expose the identity of sources for articles, books, etc., if the source or the author request anonymity. IMMI has developed policy proposals on whistleblower protection and intermediary protection, additionally the policy responds to the privatization of media policy, as well as to concerns regarding repression and critical resources. Further, it has expanded its agenda to include infrastructure issues, particularly net neutrality, and IMMI activists have engaged with debates on the European Data Retention Directive and, more broadly, surveillance [79]. IMMI, a policy initiative aimed at changing the legal environment thus responds to most of the areas mentioned in the previous section that technological solutions aim to target.

If implemented, the full IMMI package would provide a legal environment which protects national and international publishers from content restrictions, as well as other potential restrictions. All information originating from (or routed through) Iceland would be governed by the new set of laws and would therefore be very difficult to suppress [80]. In a new media environment, this does not necessarily require the physical relocation of publishing houses to Iceland but merely the posting of content on webservers hosted in the country. Blogs, websites, and all kinds of online publications would thereby fall under Icelandic jurisdiction and would be safe(r) from censorship [81]. IMMI's understanding of freedom of expression is not limited to traditional journalism, but it includes non-professional citizen journalists, publishers of blogs, and civil society groups in the remit of information producers, thereby expanding classic notions of journalism to encompass these aforementioned sources.

4.2 Advocacy on Infrastructure, Surveillance, Intellectual Property

While IMMI has put an emphasis on questioning the practice of information control, other campaigns and initiatives have targeted other issue areas. Here I will just point to a few examples. On the theme of access to infrastructure, a prominent dynamic has been the struggle on net neutrality in North America. Groups such as Free Press

(US) and Open Media (Canada) have campaigned for the protection of net neutrality, against powerful and well-resourced adversaries, such as network operators and telcos [82].

Campaigns for the legalization of community broadcasting have targeted key infrastructure issues, too. In Latin America, civil society-based policy initiatives have helped to transform a largely hostile policy environment into global showcases for advanced community media laws. In Argentina, the 'Coalition for Democratic Broadcasting', formed in 2004, developed guidelines for a new national media law, and the government charged a coalition member, university professor and community media expert to draft it. After numerous open hearings and the inclusion of further civil society comments, a demonstration of 20,000 people brought the final text to Parliament where it was adopted in 2009, making it a true "law of the people" [83]. It not only legalizes community and non-profit media, but also reserves one third of the radio frequency spectrum for them. According to the World Association of Community Broadcasters (AMARC), the law has "transformed Argentina into one of the best references of regulatory frameworks to curtail media concentration and promote and guarantee diversity and pluralism" [84]. Similar policy developments have taken place in other countries of Latin America and around the globe, including the countries with the largest populations in South Asia (India) and Africa (Nigeria), and, most recently, the US [85].

Mass protests have arisen against the Data Retention Directive that the European Union has developed in an attempt to addressed the problem of data gathering and surveillance. Mobilized by internet activists, privacy advocates and civil liberties groups, numerous campaigns and initiatives have emerged across Europe in an attempt to change the new policy. These groups have benefitted from strong national campaigns, such as the German AK Vorrat, which has inspired activists in other countries, and from international NGOs, such as European Digital Rights (EDRI), which has raised awareness across the region [86]. Demonstrations and protests have brought to the streets tens of thousands of people since 2007, including over 50,000 people in Berlin alone in September 2009 and 2010. Constitutional complaints have challenged data retention law in several countries – for example, over 30,000 people signed a legal challenge before the German Constitutional Court, making it the largest constitutional complaint in German history [87]. The European Commission (EC) told EDRi that it "will continue monitoring legislative developments at the national level" regarding the existence of data retention laws in EU Member States. The EC provided this non-committal response to the letter were sent on 2 July 2015, asking the Commission to investigate illegal data retention laws in the European Union. EDRi's analysis sent to the European Commission concluded that the existing laws in at least six countries appear to be in contravention to the Charter of Fundamental Rights. The Commission, as guardian of the treaties, is legally required to do the necessary further research and ensure that Member States bring their practices into line with EU law, making use of the infringement procedures if necessary. If the Commission continues only "monitoring", with millions of EU citizens being subject to illegal data retention laws one year after the CJEU ruling, this will not be enough [88].

In the field of intellectual property, the negotiations on the anti-counterfeiting trade agreement ACTA have drawn criticism from civil society groups (such as the French La Quadrature du Net). As ratification and implementation of the agreement became imminent in early 2012, protests erupted and have stalled its ratification [89]. Campaigns against the SOPA bill in the US were successful in stopping its adoption too [90].

4.3 An arab media policy spring?

Following the dramatic political transformations in several countries of North Africa, discussions have been initiated regarding how to revise media laws and policy in a region due to their record of severe censorship and media control. In Tunisia, where the wave of uprisings started, the debate has progressed the farthest. Yet what has emerged as post-revolutionary media policy is an uncertain and incoherent combination of new freedoms and old restrictions. A new Tunisian press law was quickly drafted by a sub-committee of the High Commission for the Realization of the Objectives of the Revolution and Democratic Transition and was unveiled in March 2011 [91]. This law limits the extent of government control and expands freedom of expression. The new decree related to the Code of Press, Printing and Publication, was developed and included important additions establishing a real freedom of press and a professional journalism. The most important additions, with regard to the strengthening of the rule of law in particular, are the exclusion of the intervention of the Ministry of Interior in the affairs of press and publication, and giving this competence over to the judiciary at all stages. The new text defines a journalist narrowly in order to attempt to purify the profession from mercenaries and those who lack professionalism, who were widely used by the previous regime. It stipulated the objective to form a Committee to assign a professional journalist card. It also recognized the right of journalists to access the news (Article 9 of Code of Press, Printing and Publication), protects journalists in doing their job (Articles 10, 11, 12 and 13), and protects the confidentiality of sources (Article 13). It considered as attacks on the confidentiality of the sources, all acts of investigation, research, inspection, and interception of correspondence or communication carried out by the public authority towards a journalist. Decree No. 115 also punishes whoever attacks a journalist during the performance of his functions, with the penalty of attack on a quasi-public official (Article 14). Articles 33 to 38 address pluralism in media. In order to support this pluralism, Chapter 34 prevents the processes that led to the possession or control, directly or indirectly, of the collective political news groups, and bans owning or controlling circulation representing more than 30% of the total circulation for a particular medium. On the other hand, this decree narrowed the field of press offenses and confined them to a limited number of cases, introducing a significant commutation to the penalties and cancelling most of the penalties resulting in deprivation of freedom. The decree related to the freedom of audio-visual communication is characterized by the same trend. However, it retains broad registration requirements for publications (which include 'publications' that are recorded on CDs and in other digital form), as well as a wide range of criminal content restrictions, such as broad interpretations of defamation which leads to a possibility of disproportionately harsh punishment. The draft was criticized as overly restrictive and not yet in compliance with international

standards [92]. Similarly, the new government has retained elements of the old internet censorship regime. The *Agence Tunisienne d'Internet* (ATI) has repeatedly been ordered by courts to continue to implement censorship orders, for example to block certain activists' Facebook accounts. On May 27, 2011, Internet users received a blow to Internet freedom as a Tunisian court ordered the blocking of all pornographic sites in response to a petition from three local lawyers who argued the "negative psychological, physiological, social and educational effects" of pornographic websites. Though the ATI attempted to have the order blocked, the decision was upheld and the *Agence Tunisienne d'Internet* (ATI) or Tunisian Internet Agency, agreed in June to comply by initiating the block, while continuing to appeal the court order. Free expression activist Slim Amamou resigned just a few months after having been appointed to the interim government [93]. He created a lot of buzz as the youngest cabinet minister in the post-revolution transitional Tunisian government that promised to reform the country after decades of corrupt dictatorial rule. He's worried the regime that replaced that cabinet, after the ouster of president Zine El Abdine Ben Ali, is heading down a dangerous path of stricter controls on the media, and score settling with rivals to maintain control.

International NGOs have teamed up with local organizations to advance policy change, and have provided elaborate contributions to the drafting of new laws. For example, the Electronic Frontier Foundation (EFF) is supporting ATI in "developing new Internet policy that departs from the old regime of pervasive Internet controls, censorship and surveillance" [94], and Article 19 has developed proposals for enshrining freedom of expression in the new Egyptian constitution [95]. Existing international declarations provide further guidelines and policy suggestions, for example the UNESCO Declaration of Sana'a on 'Promoting Independent and Pluralistic Arab Media', which discusses a broad range of freedom of expression issues and their specific characteristics in the region [96], and the Marrakech Declaration on 'The Role and Place of the Media in the Information Society in Africa and the Arab Region', which applies those issues to digital communication [97]. Issues of governmental censorship and physical repression are high on the agenda, but questions of intermediary protection, for example, appear in documents such as the Marrakesh Declaration and draw connections to advocacy priorities in Iceland and elsewhere.

5. Conclusion: evaluating digital freedoms

"I thought that t*here was no way to put the genie back in the bottle, but now it seems in certain areas the genie has been put back in the bottle"* [98] It means that the principles of openness and universal access that underpinned the creation of the internet three decades ago are under greater threat than ever [99]. There were "very powerful forces that have lined up against the open internet on all sides and around the world. The threat to the freedom of the internet comes from a combination of governments increasingly trying to control access and communication by their citizens, the entertainment industry's attempts to crack down on piracy, and the rise of "restrictive" walled gardens such as Facebook and Apple, which tightly control what software can be released on their platforms [100].

Since its creation, the internet has served as a platform for free and open communication exchange, and it has been used by civil society, activists, and citizen journalists to provide information, mobilize, and by-pass traditional restrictions to communication during political instability. The experiences of Panama Papers and the Arab Spring provide a plethora of innovative uses and applications, but they also demonstrate how quickly new restrictions have emerged, and in which areas, and by what means, governmental and business actors have been trying to tame cyberspace. In this article, we have highlighted the areas of information control, access to infrastructure, critical resources and applications, surveillance, and physical repression, and we have pointed to dynamics such as the increasing use of intermediaries and the role of intellectual property protection in control regimes. Neither Panama Papers nor the Arab Spring have initiated or triggered this process, but they provide a lens through which we can get a clearer view on emerging sets of restrictions to online free speech, and thus on the struggles and contestations on freedom of expression in the current digital media environment.

Civil society-based policy initiatives have addressed the aforementioned dimensions, with some focus on specific areas such as surveillance or infrastructure, and others developing broader agendas for 'modern freedom of expression'. Despite particular national and regional foci, they broadly confirm the issue areas proposed above. Both WikiLeaks and the Arab Spring have played central roles, not only in demonstrating key restrictions, but also in triggering advocacy efforts that oppose limitations on free expression.

The areas that were highlighted here may help us to identify relevant components for monitoring the enclosure of digital freedoms. They reflect several concerns that are already considered in evaluation efforts. For example, the citizen media network Global Voices monitors repression against bloggers worldwide [101], and the think tank Freedom House assesses ICT freedom in its 'Freedom of the Net' reports by looking at obstacles to infrastructure access, limits on content, and violations of user rights [102]. The perspective provided in this article argues for a broad approach that includes all these aspects; pays particular attention to current trends such as the role of intermediaries and the wide-spread phenomenon of private censorship through the use of libel and anti-defamation law; and considers a range of media platforms that are used for citizen-based free expression, including (digital) radio. The cases of Panama Papers and the Arab Spring, finally, provide us with an understanding of the challenges to digitally-mediated expression that moves beyond a distinction into authoritarian and democratic states and thus a reductionist view, pointing instead to a variety of restrictions which are applied, in different forms and intensities, across the globe.

6. References

1. IMMI. IMMI Status Report online, 2012, <http://www.immi.is>.
2. Research for this article is based on document analysis, investigations of social media sources, and in-depth interviews with members of policy initiatives. It partly draws from research conducted within the international collaborative project 'Mapping Global Media Policy' (which I developed together with Marc Raboy and Claudia Padovani, see http://www. globalmediapolicy. net), and from collaborative work with Stefania Milan.

3. Kate Coyer, Tony Dowmunt, Alan Fountain. The Alternative Media Handbook, (London: Routledge, 2007) (https://www.routledge.com/The-Alternative-Media-Handbook-1st-Edition/Coyer-Dowmunt-Fountain-Curran/p/book/9780415359658); John Downing, Encyclopedia of Social Movement Media, (London: Sage, 2010) (http://web.b.ebscohost.com.uml.idm.oclc.org/ehost/ebookviewer/ebook/bmxlYmtfXzQ2NzE5MV9fQU41?sid=130aa89f-0645-4c86-8a18-4ad0652da7df@sessionmgr102&vid=0&format=EB&rid=1).
4. Annabelle Sreberny, Mohammadi, Ali Mohammadi, Small Media. Big Revolution: Communication, Culture, and the Iranian Revolution, (Minneapolis: University of Minnesota Press, 1994.
5. John Downing, Radical Media. Rebellious Communication and Social Movements, (London: Sage). Samizdat ("self-publishing") was a form of dissident activity across the Eastern Bloc in which individuals reproduced censored and underground publications by hand and passed the documents from reader to reader. This grassroots practice to evade official Soviet censorship was fraught with danger, as harsh punishments were meted out to people caught possessing or copying censored materials. Samizdat originated from the dissident movement of the Russian intelligentsia, and most samizdat directed itself to a readership of Russian elites, 2001.
6. IMC, Independent Media Centre, online: <http:// www.indymedia.org>.
7. Jay Rosen. The People Formerly Known as the Audience, 2006, online (blog): PressThink <http://archive.pressthink.org/2006/06/27/ppl_frmr.html>.
8. Robert A. Hackett & William K. Carroll, The Struggle to Democratizre Public Communication, (London: Routledge, 2006 online: < https://ebookcentral.proquest.com/lib/umanitoba/reader.action?docID=268695>.
9. IMC, Independent Media Centre, online: <http://www.indymedia.org>.
10. Larry Diamond, "Liberation Technology. 2010; 21:3 Journal of Democracy, 69-83 at 70 (https://muse-jhu-edu.uml.idm.oclc.org/article/385959).
11. Huang, Carol, "Facebook and Twitter key to Arab Spring uprisings: report". thenational.ae, 6th June, 2011.
12. Cohen, Noam, "Egyptians Were Unplugged, and Uncowed", New York Times, 20th February, 2011
13. Gladwell, Malcolm, "Small Change. Why the revolution will not be tweeted", New Yorker, 4th October, 2010.
14. Khamis, supra note 11 at #.
15. Ibid at #.
16. Ben Wagner, "'I Have Understood You': The Co-Evolution of Expression and Control on the Internet, television and Mobile Phones during the Jasmine Revolution in Tunisia" 5 International Journal of Communications at # (https://ijoc.org/index.php/ijoc/article/viewFile/1174/606&embedded=true).
17. Schmidt, Michael S. Myers, Steven Lee. Panama Law Firm's Leaked Files Detail Offshore Accounts Tied to World Leaders". The New York Times, 2016.
18. Clark, Nicola, "How a Cryptic Message, 'Interested in Data?,' Led to the Panama Papers". The New York Times, 2016.
19. Document Cloud 150 Results Source: Internal documents from Mossack Fonseca (Panama). DocumentCloud. Investigative Reporters and Editors, Inc. Archived from the original on, 2017.
20. Garside, Juliette, Watt, Holly; Pegg, David. The Panama Papers: how the world's rich and famous hide their money offshore. The Guardian, 3rd 2016-2017.
21. Document Cloud 150 Results Source: Internal documents from Mossack Fonseca (Panama)". DocumentCloud. Investigative Reporters and Editors, Inc. Archived from the original on, 2017.
22. Christian Christensen. Discourses of Technology and Liberations: State Aid to Net Activists in an Era of 'Twitter Revolutions. 2011; 14:3. Communication Review 233-253 at 234 (https: //www.tandfonline.com/doi/abs/10.1080/10714421.2011.597263).
23. Ibid.
24. Albrecht Hofheinz. The Arab Spring: Nextopia? Beyond Revolution 2.0. 2011; 5:1 International Journal of Communication (https://ijoc.org/index.php/ijoc/article/view/1186); Evgeny Morozov, The Net Delusion: The Dark Side of Internet Freedom (New York: Public Affairs, 2011.
25. Bendetta Brevini, Arne Hintz, Patrick McCurdy. Beyond WikiLeaks: Implications for the Future of Communications Palgrave MacMillan, 2013.
26. Olafur Ragnar Grimsson. Keynote (European Consortium for Political Research delivered at Harpa, Reykjavik Concerta Hall, 2011.
27. John Perry Barlow. A declaration of the independence of cyberspace, 1996, online: < https://www.eff.org/cyberspace-independence>.
28. John Browning G. Democracy Unplugged: Social Media, Regime Change and Governmental Response in the Arab Spring, Michigan State International Law Review. 2013; 21:1.
29. Ibid.
30. Ibid.
31. See, for example, the series on the Battle for the internet in the Guardian in 2012 (http://www.guardian.co.uk/technology/series/battle-for-the-internet).
32. For example, in South Africa, where a progressive freedom of information law has been in place since the 1990s, a 'Protection of Information' bill was passed in 2011 which grants the government broad powers to classify documents for reasons ranging from national security to protection of state possessions; M. Le Pelley, "das Jahrzehnt der informationsfreiheit in Afrika?" (FES Perspektive, December 2011) online: < http://library.fes.de/pdf-files/iez/08818-20120110.pdf>.
33. See, for example; OpenNet Initiative, "Global Internet filtering in 2012 at a glance, 2012, online <http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance>.
34. Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain. Access Denied: The Practice and Policy of Global Internet Filtering, (Cambridge: MIT Press, 2008.
35. BBC. The Pirate Bay must be blocked by UK ISPs, court rules. BBC News Technology, 2012. http://www.bbc.com/news/technology-17894176

36. Kreimer SF. Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link. University of Pennsylvania Law Review. 2006; 155:11.
37. Internet users are still allowed to contact their ISPs and request that pornography sites are enabled for their Internet connection. Christina Angelopoulos, Filtering the Internet for Copyrighted Content in Europe, IRIS, Legal Observations of the European Audiovisual Observatory, 2009.
38. Landry N. SLAPP: Bâillonnement et répression judiciaire du discours politique. Québec: Écosociété, 2012.
39. David Leigh. How the UK oil company Trafigura tried to cover up African pollution disaster, The Guardian, 16th September, 2009.
40. Hintz A, Milan S. At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy. International Journal of Media & Cultural Politics. 2009; 5(1):23-38.
41. Arne Hintz. Challenging the Digital Gatekeepers: International Policy Initiatives for Free Expression, Journal of Information Policy. 2012; 2:128-150.
42. Balkin JM. The Future of Free Expression in a Digital Age. Pepperdine Law Review. 2009; 36(2):427-444.
43. Flaim SM. Op-ed: Imminent "six strikes" Copyright Alert System needs antitrust scrutiny. ars technica, 2012, http://arstechnica.com/tech-policy/news/2012/03/op-ed-imminent-six-strikes-copyright-alert-system-needs-antitrust-scrutiny.ars
44. Waisbord S. The pragmatic politics of media reform: Media movements and coalition-building in Latin America. Global Media and Communication. 2010; 6(2):133-153.
45. Coyer K. Community Radio Licensing and Policy: An Overview. Global Media and Communication 2(1), 129-134.; Coyer, K., & Hintz, A. 2010. Developing the 'third sector': Community media policies in Europe. In B. Klimkiewicz (ed.) Media Freedom and Pluralism: Media Policy Challenges in the Enlarged Europe. Budapest: CEU Press.; Hintz, A. 2011. From Media Niche to Policy Spotlight: Mapping Community Media Policy in Latin America. Canadian Journal of Communication. 2006; 36(1):147-159.
46. Hallett L, Hintz A. Digital Broadcasting – Challenges and Opportunities for European Community Radio Broadcasters. Telematics and Informatics. 2010; 27(2):151-161.
47. Benkler Y. A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate. Working draft, 2011, http://www.benkler.org/Benkler_Wikileaks_current.pdf.
48. Ibid.
49. Ibid.
50. Mary Footer E. The Panama Papers, Corporate Transnationalism and the Public International Order, European Society of International Law. Vol. 6, Issue 1, 2017.
51. Arne Hintz. Outsourcing Surveillance – Privatising policy: Communications Regulations by Commercial Intermediaries, Birkbeck Law Review. 2014; 2:2.
52. Zittrain J. The Future of the Internet – And How to Stop It. New Haven: Yale University Press at 3, 2008.
53. Chris Atton, The Routledge Companion to Alternate and Community Media, Routledge, 2015.
54. Villeneuve N. Fake Skype Encryption Software Cloaks DarkComet Trojan. Trend Micro Malware Blog, 2012. http://blog.trendmicro.com/fake-skype-encryption-software-cloaks-darkcomet-trojan/
55. Arne Hintz. Outsourcing Surveillance – Privatising policy: Communications Regulations by Commercial Intermediaries, Birkbeck Law Review. 2014; 2:2.
56. Activists Urge Panama to Leave Lima Group, Support Venezuela, Telesur.net, 2019.
57. Dennis Fisher. Google Report shows it complied with 93% of the US Law Enforcement Data Requests, Threat Post, 2011.
58. http://www.spyfiles.org, http://www.buggedplanet.info http://www.google.com/transparencyreport/governmentrequests/US/?p=2011-06
All these proposed and actual surveillance regulations have led to protests by technologists, activists and civil liberties groups. In the case of CISPA, even White House spokeswoman Caitlin Hayden said the "legislation that would sacrifice the privacy of our citizens in the name of security (quoted in Lee 2012.
59. Braman S. Change of State. Information, Policy, and Power. Cambridge: MIT Press, 2006.
60. Karen McVeigh, Dominic Rushe. House passes Cispa cybersecurity bill despite warnings from the White House, The Guardian, 2013.
61. Berners-Lee T. Analysis: "Cybersecurity bill endangers privacy rights. Ars technica, 2012, http://arstechnica.com/tech-policy/news/2012/04/analysis-cybersecurity-bill-endangers-privacy-rights.ars
62. APC. The big snoop: The UK's temptation to become a big brother and what it means for the rest of us. 20 2012b-2012, http://www.apc.org/en/news/big-snoop-uk039s-temptation-become-big-brother-and
63. Rodriguez K. The Impending Cybersecurity Power Grab – It's not just for the United States. Deeplinks, 2012. https://www.eff.org/deeplinks/2012/04/impending-cybersecurity-power-grab-its-not-just-united-states.
64. Farid, Shirazi. Social Media and the social movements in the Middle East and North Africa: A Critical Discourse Analysis, Information Technology and People. 2013; 26:1.
65. York J. In Review: Internet Freedom in the Wake of the Arab Spring. Deeplinks. 2011b-2011. https://www.eff.org/deeplinks/2011/12/2011-review-internet-freedom-wake-arab-spring
66. Mendez JE. Report of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Addendum: Observations on communications transmitted to Governments and replies received. Report to the United Nations General Assembly, 2012. A/HRC/19/61/Add.4.
67. Hintz, supra note 51.
68. APC. APC statement: Internet rights organisations strongly denounce attack on anonymous online speech by US government, 2012a-2012, http://www.apc.org/en/news/apc-statement-progressive-internet-rights-organisa
69. Galperin E. Kuwait Prepares to Crack Down on Social Media. Deeplinks, 2012, https://www.eff.org/deeplinks/2012/05/kuwait-prepares-crack-down-social-media
70. The Guardian. Facebook riot calls earn men four-year

jail terms amid sentencing outcry, 2011, http://www.guardian.co.uk/uk/2011/aug/16/facebook-riot-calls-men-jailed
71. Boyle J. The Public Domain: Enclosing the Commons of the Mind. New Haven: Yale University Press, 2008.
72. Luciano Floridi. The Anti-Counterfeiting trade agreement: The ethical analysis of a failure and its lessons, Ethics and Information Technology. 2015; 17:2.
73. Bambauer DE. Cybersieves. Duke Law Journal. 2009; 59(3):377-446.
74. For example. Facebook has helped activists in Tunisia using their website anonymously, and research centers such as The Citizen Lab at University of Toronto have developed programs such as Psiphon which are used for secure communication.
See the anecdote mentioned above on RUV's failed reporting on financial corruption.
75. Jared Wright, Digital Contention. Anonymous and the Freedom of Information Movement, University of Houston, 2012.
76. For all quotes from the IMMI proposal, see http://immi.is/Icelandic_Modern_Media_Initiative
77. Ibid
78. Ibid
79. Ibid
80. Jessica Beyer, "The Emergence of a Freedom of Information Movement: Anonymous, Wikileaks, the Pirate Party and Iceland", Journal of Computer-Mediated Communication, 2013.
81. Bollier D. A New Global Landmark for Free Speech. 2010. http://www.bollier.org/new-global-landmark-free-speech.
82. Blevins JL, Shade LR. International Perspectives on Network Neutrality: Exploring the Politics of Internet Traffic Management and Policy Implications for Canada and the U.S. Global Media Journal – Canadian Edition. 2010; 3(1):1-8.
83. Loreti D. Research interview by Arne Hintz. Montreal, 2011.
84. AMARC. AMARC Deplores Suspension of New Communications Law in Argentina. AMARC Link. 2010; 13:1. http://www.amarc.org/amarclink/ amarc_ link_AVRIL_2010_EN_final.pdf
85. Ibid.
86. See http://www.vorratsdatenspeicherung.de and http://www.edri.org
87. Diego Naranjo. European Commission will monitor existing EU data retention laws, Protecting Digital Freedom, 2015.
88. Ibid.
89. Luciano Floridi. The Anti-Counterfeiting trade agreement: The ethical analysis of a failure and its lessons, Ethics and Information Technology. 2015; 17:2.
90. Ibid.
91. High Commission for the Realization of the Objectives of the Revolution and Democratic Transition. Draft Press Law.
92. Centre for Law and Democracy. Tunisia – Comments on the Draft Decrees Making up the Press Law, April 2011 http://www.law-democracy.org/wp-content/uploads/2010/07/11.04.Tunisia.Prs_.pdf
93. Jillian York, "EFF Supports Tunisian Internet Agency in Protecting Free Expression Online", Electronic Frontier Foundation, 30th August, 2011.
94. York J. EFF Supports Tunisian Internet Agency in Protecting Free Expression Online. Deeplinks. 2011a-2011. http://www.eff.org/deeplinks/2011/08/eff-supports- tunisian-internet-agency-protecting
95. Article19. Egypt: Protecting Freedom of Expression and Freedom of Information in the New Constitution. Policy Brief, 2012, http://www.article19.org/ data/files/ medialibrary/3092/12-05-09-LA-egypt.pdf
96. UNESCO. Declaration of Sana'a on Promoting Independent and Pluralistic Arab Media. Adopted in Sana'a, Yemen, 1996.
97. Marrakesh Declaration. Final Declaration of the Conference The Role and Place of the Media in the Information Society in Africa and the Arab Region, organized by the Kingdom of Morocco and Orbicom, the International Network of UNESCO Chairs in Communications, 2004.
98. Katz I. Web freedom faces greatest threat ever, warns Google's Sergey Brin. The Guardian, 2012. http://www.guardian.co.uk/technology/2012/apr/15/web-freedom-threat-google-brin
99. Ibid.
100. Ibid.
101. http://threatened.globalvoicesonline.org/
102. ttp://www.freedomhouse.org/report-types/freedom-ne