Challenges to Freedom of Expression in the Digital World: Lessons from WikiLeaks and the Arab Spring

Arne HINTZ
Research Fellow, McGill University, Canada
arne.hintz@mcgill.ca

Abstract: Two recent developments – the WikiLeaks releases and the Arab Spring – have demonstrated the 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. In this article I will present 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. The model takes into account current trends such as the use of intermediaries in control regimes, and provides a global perspective that incorporates restrictions in both East and West. Further, I will outline how free expression advocates and civil society campaigns, such as the Icelandic Modern Media Initiative (IMMI), have contested these practices, and discuss whether their agendas confirm the issue areas highlighted above. 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 civil society), and the requirements for “modern freedom of expression”.

Keywords: Freedom of Expression, WikiLeaks, Arab Spring
84 Arne HINTZ Challenges to Freedom of Expression in the Digital World….

***

Les défis de la liberté d’expression dans le monde numérique : lessons de WikiLeaks et le Printemps Arabe

Résumé : Deux développements récents – les communiqués de WikiLeaks et le Printemps Arabe – ont démontré les capacités des individus et des mouvements de faire avancer la liberté d'expression, la transparence et le changement social grâce à l'utilisation des médias en ligne et sociaux. Cependant, ils ont également mis en évidence de nouveaux défis et menaces qui interfèrent avec et restreignent les utilisations des médias. Dans cet article, j’ai élaboré un cadre analytique pour rendre compréhensible et analyser ces restrictions contemporaines de la liberté d'expression, sur la base des dimensions suivantes : contrôle de l'information, accès aux infrastructures, aux ressources et applications critiques, surveillance et répression physique. Le modèle prend en compte les tendances actuelles telle que le recours à des intermédiaires dans les régimes de contrôle et fournit une perspective globale qui intègre les restrictions à la fois à l'Est et à l'Ouest. De plus, j’ai mis en exergue la manière dont les défenseurs de la libre expression et des campagnes de la société civile, telle que l'initiative islandaise des médias modernes (IMMI), ont contesté ces pratiques de contrôle. Les restrictions à la communication et le plaidoyer en faveur de la communication libre démontrent les luttes et contestations clés sur la liberté d'expression dans l'environnement médiatique numérique actuel, les points stratégiques d'intervention de différents acteurs (Etats, entreprises et société civile), et les exigences relatives à la « liberté d'expression moderne ».

Mots-clés : liberté d’expression, WikiLeaks, Printemps Arabe

***

1. Introduction

Over the past two years, two major international developments – the WikiLeaks 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 WikiLeaks 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 (webspace, 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.

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 I will propose an analytical structure for understanding and investigating these dynamics. The observations presented here will be based on the experiences of the WikiLeaks saga and of social media use in the Arab Spring, but will incorporate other current policy developments. In particular, I 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, I will explore in how far WikiLeaks and the Arab Spring have triggered civil society campaigns that contest restrictions to communication flows and seek policy change. I will outline the Icelandic Modern Media Initiative (IMMI) which has declared its mission as safeguarding “modern freedom of expression” (http://www.immi.is), as well as current initiatives and proposals for media policy change in the Arab world and elsewhere. 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), and they point us to some of the core requirements for freedom of expression in an online world.\(^1\)

2. Citizen Journalism Opportunities and Social Media Revolutions

Citizen-based and self-organized media production is not a new phenomenon. 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 (e.g., Coye\/Downmunt/Fountain 2007; Downing 2010). 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 (Sreberny-Mohammadi/Mohammadi 1994), and the Samizdat

\(^1\) 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.
movement in the former Soviet bloc (Downing, 2001).

The Internet has allowed interested people to build on these experiences, but also to expand them significantly. The global Indymedia network (http://www.indymedia.org) 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 iReporter), while “the people formerly known as the audience” (Rosen, 2006), 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 (Hackett/Carroll, 2006). As the Indymedia slogan goes: “Don’t hate the media, be the media!”

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 (2010) notes, social media and other ICT applications enable “citizens to report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom” (ibid. 70).

The Arab Spring, i.e. the protests and uprisings in several countries of North Africa and the Middle East in spring 2011, seemed to confirm this claim and placed the liberation technology paradigm firmly on the political, academic and public agendas. 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 mobilizing a critical mass of protesters, organizing logistical details, and generating a social space
for developing critical discourses where an open public sphere did not exist (Khamis/Vaughn 2011). Social media became “effective catalysts” (ibid: 1) 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” (ibid: 1). Others have been more cautious, pointing to a “functional differentiation” (Wagner 2011) in which the Internet was used extensively by individuals with technical knowledge and publishers of information, whereas the broader masses of citizens and media consumers relied more on satellite television for accessing information.

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” (Gunilla Carlsson, Swedish Minister for International Development Cooperation, quoted in Christensen 2011: 234), 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 (e.g., Christensen 2011, Kaplan 2012). This strong interest outside the region results, not 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” (Hofheinz, 2011; Morozov, 2011).

Similar public interest, although less favourable amongst Western governments, was raised by WikiLeaks, particularly 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

---

2 Earlier investigations of the role of alternative media in authoritarian environments and for political change have highlighted the importance of creating a public sphere where there is none (e.g., in Iran in the late 1970s, see Sreberny-Mohammadi/Mohammadi 1994) and of sharing criticism amongst dissidents and thereby breaking through social isolation (as in the Soviet Union, see Downing 2001).

3 Several books have appeared which tell the story leading up to the release, provide detailed accounts of what followed, and discuss the potential and actual effects. See, e.g., Mitchell 2011.
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, WikiLeaks 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. WikiLeaks 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 (Brevini/Hintz/McCurdy 2013).

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 favour 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 (Grimsson 2011). In that sense, the Arab Spring and WikiLeaks 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 (Barlow 1996).

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 have been used by activists to advance political change, they
have been used by governments to control and deter such action, for example by
identifying protesters (as in Tunisia, Syria and Iran). Vital online resources and
funding streams have been cut to weaken dissident organizations (as happened to
Wikileaks), 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). 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, observation of the obstacles and restrictions to free online communication which are emerging rapidly. In the following paragraphs, I will propose and discuss a more systematic structure of these obstacles. This may help us to develop 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 flows is to curtail access to information. WikiLeaks has highlighted this problem by making information public that either governments or businesses have wished to conceal. The state's interest in preventing its citizens from accessing information that is 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.

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. While the Chinese ‘Great Firewall’ and filtering practices in other authoritarian countries, including in the Middle East, have been well documented (e.g., Deibert et al 2008), 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. 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 (BBC 2012).

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” (Kreimer 2006: 13). 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.

---

4 See, for example, the series on the “Battle for the internet” in the Guardian in April 2012 (http://www.guardian.co.uk/technology/series/battle-for-the-internet).
5 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 (Le Pelley 2011).
6 See, for example http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance
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) (Landry 2012). In countries such as the UK, strict libel laws have become a key tool for businesses (and celebrities) to prevent investigative reporting. Although WikiLeaks 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, concerned information that had been banned from being published for libel reasons.

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 WikiLeaks website where detailed documents on the case had been posted (thereby making WikiLeaks 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 (Hintz/Milan 2009).

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.

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 favouring the content and applications of some information sources and services over others, and who might block access to disfavoured sites or require a special fee. This provides particular challenges for

---

7 Internet users are still allowed to contact their ISPs and request that pornography sites are enabled for their Internet connection.
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 (Balkin 2009).

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 (Flaim 2012).

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 (see, e.g., Waisbord 2010). 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 (Coyer 2006; Coyer/Hintz 2010; Hintz 2011). The transition from analogue to digital broadcasting provides new challenges: While the US digital radio system IBOC discriminates in favour 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 (Hallett/Hintz 2010).

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

8 See http://www.laquadrature.net. In 2006, as part of a chapter entitled ‘How governments rule the net’, Goldsmith and Wu noted: ‘There may soon come a time when abusing your privileges as a member of the Internet could lead to expulsion from the club’ (Goldsmith/Wu 2006: 79). It appears this time has come.
particularly apparent in December 2010 when Amazon, Paypal and others closed the services they had previously provided for WikiLeaks, depriving the leaks platform of its domain name and of access to necessary funds in the middle of a major release that required both. This 'denial of service', as Benkler (2011) 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. Further, the actions by Amazon, Paypal etc. 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 (Benkler 2011).

The relative success of the 'denial of service' strategy in the WikiLeaks case has certainly had an influence on the repertoires of control applied by state actors. 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.

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” (Zittrain 2008: 3).

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 disidents. In Tunisia and Iran, authorities have used Facebook to scrape user data. Syrian opposition supporters were targeted using Trojans – programs that covertly install spying software onto the infected computer – 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 (Villeneuve 2012). The
The WikiLeaks case, too, has problematized the widespread public use of social networking and its increasing integration into surveillance regimes. In their quest to contain the WikiLeaks 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 WikiLeaks activists and their followers, and one can only speculate which other online services received the same requests and complied quietly. 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.10

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” (Braman 2006: 314). 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. 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' (Lee 2012).11 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” (quoted in APC 2012b).
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 Wikileaks or sites accused of copyright infringement” (Rodriguez 2012).

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. In post-Mubarak Egypt, thousands of dissidents continue to be tried in military courts, among them numerous bloggers and social media users, and critical comments of the military, other authorities, and religion have been punished with prison sentences (York 2011).

WikiLeaks 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 (Mendez 2012). 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 (Hintz/Milan 2009). 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 Riseup Networks and May First/People Link in New York City (APC 2012a).

3.6. Cross-cutting Issues

Value systems differ across the globe, and so the backgrounds and reasons for these various types of interventions into free online expression differ, too. 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” (quoted in Galperin 2012).

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 WikiLeaks 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 (The Guardian 2011).

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’ (Boyle 2008), we are witnessing a trend towards the commodification of knowledge and its removal from the public domain. 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.

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 (2009: 481) notes: “There is no longer one Internet. Technological censorship by countries worldwide means that how the Net appears depends upon where you access it.”

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 companies
elsewhere. WikiLeaks 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. WikiLeaks supporters, for example those connected with the Anonymous network, have responded with technical direct action, such as distributed denial of service (DDoS) attacks, to the access restrictions by Paypal, Amazon and others on WikiLeaks' resources, and to the online restrictions put in place by governments in the Middle East.

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. IMMI emerged in the context of the financial collapse of the Icelandic economy in late 2008. The initiative was set up to change no less than 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 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. At its core is the concern to prevent the suppression of content by both public and private actors. IMMI has initiated the

---

12 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.

13 See the anecdote mentioned above on RUV's failed reporting on financial corruption.

14 For all quotes from the IMMI proposal, see http://immi.is/Icelandic_Modern_Media_Initiative
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 legitimate information – “legal harassment” of media and publishers, as IMMI puts it. 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, and it thus 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 (IMMI 2012). IMMI thus responds to most of the areas mentioned in the previous section.

If implemented, the full IMMI package would provide a legal environment which protects national and international publishers from content (and other) 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. 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 web servers 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 (Bollier 2010). 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.

4.2. Advocacy on Infrastructure, Surveillance, Intellectual Property

While IMMI has put an emphasis on questions 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 (Blevins/Shade 2010).

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” (Loreti 2011). It not only legalizes community and non-profit media, but reserves for it one third of the radio frequency spectrum. 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” (AMARC 2010: 10). 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.

Mass protests against the Data Retention Directive in the European Union have 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 to change the new policy. They have benefitted from strong national campaigns, such as the German AK Vorrat, which have inspired activists in other countries, and from international NGOs, such as European Digital Rights (EDRI), which have raised awareness across the region. 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.

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. Campaigns against the SOPA bill in the US were successful in stopping its adoption too.

4.3. An Arab Media Policy Spring?

Following the dramatic political transformations in several countries of North Africa, discussions have begun on how to revise media laws and policy in a region with a 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

---

15 See http://www.vorratsdatenspeicherung.de and http://www.edri.org
16 Amongst them Poland and Germany where an estimated 100,000 people took to the streets in February 2012.
sub-committee of the High Commission for the Realization of the Objectives of the Revolution and Democratic Transition, and was unveiled in March 2011 (High Commission 2011). It limits the extent of government control and expands freedom of expression. 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 lead to disproportionate punishment. The draft was criticized as overly restrictive and not yet in compliance with international standards (Centre for Law and Democracy 2011). 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. Free expression activist Slim Amamou resigned just a few months after having been appointed to the interim government.

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” (York 2011a), and Article 19 has developed proposals for enshrining freedom of expression in the new Egyptian constitution (Article 19 2012). 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 (UNESCO 1996), 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 (Marrakech Declaration 2004). 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 there 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” (Google’s Sergey Brin, quoted in Katz 2012).

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. The experiences of WikiLeaks 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, I have highlighted the areas of information control, access to infrastructure, critical resources and applications, surveillance, and physical repression, and I have pointed to dynamics such as the increasing use of intermediaries and the role of intellectual property protection in control regimes. Neither WikiLeaks 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 focusing 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 to 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,¹⁷ 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.¹⁸ 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 WikiLeaks 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.

¹⁷ http://threatened.globalvoicesonline.org/
¹⁸ http://www.freedomhouse.org/report-types/freedom-net
Références


Marrakesh Declaration (2004). *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. 24 November 2004.*


