GLOBAL INFORMATION SOCIETY WATCH 2011

INTERNET RIGHTS AND DEMOCRATISATION

Focus on freedom of expression and association online

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Introduction

Jillian C. York
Electronic Frontier Foundation
eff.org

Early visionaries imagined the internet as a borderless world where the rule of law and the norms of the so-called physical world did not apply. Free expression and free association were envisioned as entitlements, a feature of cyberspace rather than rights to be asserted.

These early conceptions quickly gave way to the realisation that, just as the internet was embraced by people, so would it be controlled: by corporations, by policy makers, by governments, the latter of which began asserting control over the internet early on, enacting borders to cyberspace and preventing the free flow of information, not unlike the physical borders that prevent free movement between nations.

For more than a decade, academics and activists have dissected and debated the various challenges to a free and open net. But the use of digital tools in the uprisings in the Middle East and North Africa, as well as the subsequent restrictions placed on them by governments, have inspired new public discourse on the subject, bringing to light the importance of and highlighting new challenges to internet freedom.

In Tunisia and in Egypt, the ability to organise and share information online proved vital to many in organising the revolutions that eventually led to the downfall of both countries' regimes. There, and in Syria, Viet Nam, Iran, the Occupied Palestinian Territories, and beyond, the videos and images disseminated from protests have demonstrated precisely why online freedom must be a policy imperative.

The Charter of Human Rights and Principles for the Internet,[1] developed by the Internet Rights and Principles Coalition, defines online freedom of expression to include the freedom to protest, freedom from censorship, the right to information, the freedom of the media, and the freedom *from* hate speech. Framed by Article 19 of the Universal Declaration of Human Rights (UDHR), the Charter recognises certain legal restrictions placed on such rights (such as the necessity to keep public order). Similarly, the Charter also frames the freedom of assembly or association online within the space of the UDHR, including in its definition the right to "form, join, meet or visit the website or network of an assembly, group, or association for any reason" and noting that "access to assemblies and associations using ICTs [information and communications technologies] must not be blocked or filtered." The two aforementioned definitions comprehensively address online rights as defined within the framework of the UDHR.

But while the freedoms of expression and association are guaranteed by Articles 19 and 20 of the UDHR, and by the individual constitutions of many of the world's nation-states, their application online has proved troublesome for even the most democratic of governments.

The internet is unique, both structurally and practically. A medium unlike any other, it enables individuals to cross borders in an instant, to seek and share information rapidly and at little cost. But just as it provides a unique means of communication, so too does it present unique challenges for regulators who, so far, have relied upon outmoded legislation to regulate the digital space.

For example, defamation laws in Turkey have led to an environment where any individual or organisation can all too easily petition a judge to block an allegedly defamatory website, thereby silencing what may very well be legitimate criticism. Similarly, in Tunisia, not long after the country's decade-long censorship of the internet ended, a group of judges successfully petitioned the court to order the Tunisian Internet Agency to block access to a large swath of pornographic websites in the interest of "morality".

The desire to restrict access to "adult content" exemplifies the challenges of enforcing existing age restrictions on online content. Where a magazine can be restricted for sale to minors or hidden in opaque packaging, and a television programme or film can come with age-appropriate warnings, online content is not so easily restricted. Instead, the most oft-used method of restriction, technical filtering, cannot differentiate between the adult and child user and therefore blocks access to content from all. In any scenario, filtering tends to be overbroad and expensive, but is also fallible, and

[1] internetrightsandprinciples.org/node/367

in most cases easily circumvented by commercially available tools.

Blocking websites is not the only means of restricting access: in Iran and in Syria, for example, authorities have slowed bandwidth to a crawl, limiting the ability of users to upload or download content such as videos or images. Several countries, including South Korea, have attempted to control access to certain content, or to track users by requiring government identification to use certain websites or to enter cybercafés. Government-enabled or sponsored attacks on infrastructure or individual websites have become increasingly common. And more recently, governments aware of the internet's organising potential have taken to implementing "just-in-time" blocking – limiting access to sites during specific periods of election or protest, or worse, arresting bloggers and social media users or shutting down the internet entirely as has occurred in Egypt, Libya and Syria.

These various forms of restriction leverage the ability of governments to censor and discredit unwanted speech, while fears of "cyberwar" make it easy for governments to justify political repression, blocking access to opposition content or arresting bloggers under terrorism legislation. A genuine need for digital security has pushed governments to develop strategies to identify and track down actual criminals; these methods are in turn used to crack down on political dissidents and others. Similarly, efforts to enforce copyright have led to chilling effects, such as in the United States (US) where, in an effort to crack down on copyright infringement, the intellectual property wing of the Immigrations and Customs Enforcement seized dozens of domain names under the guise of "consumer protection". Similarly, proposals such as France's HADOPI – which would terminate the internet access of subscribers accused three times of (illegal) file sharing – silence speech while doing little to solve the problem they are intended to combat.

Lawmakers have also found ways to restrict access to certain content from users *outside* of their countries using what is known as geolocational IP blocking. This tactic has a variety of uses, from media content hosts like Netflix and Hulu blocking users outside of the US in compliance with copyright schemes, to US companies blocking access to users in sanctioned countries like Syria and Iran.

Free expression online is challenged not only by governments, but also by private entities. Though censorship is, by definition, the suppression of *public* communications, the right to free expression is increasingly challenged by intermediaries, whether by their own volition or at the behest of governments. States have on numerous occasions relied upon intermediaries to undertake censorship on their behalf, such as in the case of South Korea, where the Korea Communications Standard Commission – a semi-private initiative – has been developed to regulate online content, or in the United Kingdom (UK), where the Internet Watch Foundation, an opaque non-governmental agency, determines a blacklist of child sexual abuse websites, which is in turn used by internet service providers (ISPs) and governmental regulators (as was the case with Australia's proposed filtering scheme). Currently, several Australian ISPs have agreed to voluntarily filter illegal content in lieu of filtering legislation, raising questions about the role of ISPs in moderating content. These issues are at the core of the debate around network neutrality, a policy framework which has yet to be widely adopted.

Companies that operate in foreign countries can impose or be complicit in limits to free expression. Companies are obliged to abide by the rules of their host country, which, in countries where restrictions to online content are the norm, results in aiding that country's censorship. Between 2006 and 2010, Google censored its search results at the behest of the Chinese government, while Microsoft continues to do so. And several companies – including US companies Cisco and SmartFilter, and Canadian company Netsweeper – allow their filtering software to be used by foreign governments.

These concerns also extend to platforms that host user-generated content. Across the Arab world and beyond, the use of social platforms to organise and disseminate information has garnered praise for sites like Facebook and Twitter. But while these platforms offer seemingly open spaces for discourse, the policies and practices of these privately owned platforms often result in content restrictions stricter than those applied by government censors, presenting a very real threat to free expression. Take, for example, the case of Wael Ghonim, the Egyptian Google executive who created the "We Are All Khaled Said" Facebook page, a core site for organising the protests. Several months prior to the uprising, the page was taken down, a result of Facebook policies that require users to utilise a real name on the service, and was only reinstated when another, identified, user stepped in to take Ghonim's place. Similarly, Facebook recently removed a page calling for a third intifada in Palestine, following public objections and numerous user reports. Other platforms have acted similarly, removing content when it violates their proprietary terms of use.

While filtering and other means of restriction affect the ability to access *content*, access to the physical and technical infrastructure required to connect to the internet can also be used by governments as a means of restricting the free flow of information and limiting individuals' ability to associate and organise. While in many cases, low internet penetration is a sign of economic or infrastructural challenges, it can also be an intentional strategy by governments attempting to restrict citizens from accessing information or developing civil society. Though this strategy is best exemplified by Cuba and North Korea – where the majority of citizens are barred entirely from accessing the internet – dozens of countries with the capability to do so have slowed or stifled the infrastructural development necessary to expand access.

These various forms of control have led to what scholars have referred to as the "Balkanisation" of the internet, whereby national boundaries are applied to the internet through these various means of control. In 2010, the OpenNet Initiative estimated that more than half a billion (or about 32%) of the world's internet users experience some form of national-level content restriction online. That number is undoubtedly increasing: in recent months, various governments across the globe have taken new steps to restrict access to content. Egypt, which had blocked websites minimally and only sporadically, took an enormous step backward when it shut down the internet for a week during the protests. Libya, which prior to 2011 filtered only selectively, has barred access for most of its population since February. Iran has recently announced plans to withdraw from the global internet, creating essentially an intranet inside the country. And even in states where access remains low – such as in Ethiopia, where internet penetration hovers around 0.5% – governments fearing the democratising power of the internet are preemptively putting additional restrictions in place. As of 2011, more than 45 states have placed restrictions on online content.

When a country restricts the free flow of information online, it impacts not only the citizens of that country, but reduces the value of the internet for all of its users and stakeholders. Just as China's extensive filtering of online content prevents Chinese users from reaching the BBC, the BBC is prevented from doing business in China; and just as Chinese users cannot access Facebook, Facebook users from across the world cannot interact with the Chinese populace.

The challenges to an open internet are decidedly complex. And with the fragmentation of the internet aided not only by authoritarian regimes, but also democratically elected governments, ISPs, user-generated content platforms, and other corporate entities, the solutions to creating an open internet are equally, if not more, complex than the problems.

Censorship does not exist in a vacuum; for every step closer to freedom, there is another step back, as governments learn from one another and implement new "solutions" for limiting free expression.

At the top level lies the simplest yet most difficult solution: convincing governments of the value of a free internet. The ideals of an open internet are often in direct conflict with the interests of policy makers, whether in debating network neutrality in the US or in the current proposal to erect a China-style firewall in Iran.

Solutions to the latter problem abound, but often act as mere bandages, offering a fallible solution to a vast and ever-developing problem. The US and other governments have poured money into circumvention technology, which can be effective in getting around internet censorship, but simply furthers the cat-and-mouse game between governments and tool developers, the former blocking the latter as the developers attempt to keep up. Mesh networking has, of late, also become a strong contender for solving the dual problems of censorship and access, with several nascent projects receiving attention – and funding – from government entities.

Trade restrictions have been proposed to curb internet censorship; notably, in 2010, Google proposed the idea of stricter trade governance as a means to prevent or lessen restrictions placed by governments on internet access. At the same time, the Global Network Initiative, a multi-stakeholder organisation comprised of academics, activists, corporations and NGOs, is working with companies to guide them toward better policies around privacy and free expression online.

But while attainment of these ideals may at times seem nearly impossible, the costs of *not* fighting for them are too great. It is therefore imperative that we – the users, the citizens – continue to push for better choices at the hands of governments and corporations, and keep fighting for the equally necessary freedoms of expression and association in this most unique of spaces. ■

GLOBAL INFORMATION SOCIETY WATCH 2011

In the year of the Arab uprisings **GLOBAL INFORMATION SOCIETY WATCH 2011** investigates how governments and internet and mobile phone companies are trying to restrict freedom online – and how citizens are responding to this using the very same technologies.

Everyone is familiar with the stories of Egypt and Tunisia. **GISWATCH** authors tell these and other lesser-known stories from more than 60 countries. Stories about:

PRISON CONDITIONS IN ARGENTINA Prisoners are using the internet to protest living conditions and demand respect for their rights.

TORTURE IN INDONESIA The torture of two West Papuan farmers was recorded on a mobile phone and leaked to the internet. The video spread to well-known human rights sites sparking public outrage and a formal investigation by the authorities.

THE TSUNAMI IN JAPAN Citizens used social media to share actionable information during the devastating tsunami, and in the aftermath online discussions contradicted misleading reports coming from state authorities.

GISWATCH also includes thematic reports and an introduction from Frank La Rue, UN special rapporteur.

GISWATCH 2011 is the fifth in a series of yearly reports that critically cover the state of the information society from the perspectives of civil society organisations across the world.

GISWATCH is a joint initiative of the Association for Progressive Communications (APC) and the Humanist Institute for Cooperation with Developing Countries (Hivos).

GLOBAL INFORMATION SOCIETY WATCH
2011 Report
www.GISWatch.org

ISBN 978-92-95096-13-4

20 APC

Hivos