A legal approach: Freedom of expression and InformationCommunication Technology (ICT)

1. Introduction
The Arab Spring and the echo it created throughout the world in 2011 raised a debate on freedom of expression and the role that new Information Communication Technology (ICT)1 can play in order to enhance democratization. Through social media, grass-root journalism, civil society and engaged individuals, current views for change were disseminated and people mobilized to act against authoritarian ruling. In some countries the mode of method raised voices and was powerful, in other constraints was made to hinder communication through open information orders, and what had started as grass-root movements were dismantled.

This presentation covers Sida’s ambition to cover current world trends with an attempt to strategically update its knowledge and understanding regarding freedom of expression and the role that new communication technology has had on the enhancement of democracy.2 The flow of information has become instantaneous, inexpensive, it transcends boundaries and empowers people and enhances globalisation. The overarching aim of the assessment is to analyze the external environments in order for Sida to enhance its own internal capabilities.

The analysis is divided into three parts: The first part focuses on the internet and the right to freedom of opinion and expressions. It continues with a brief analysis of why in certain conditions and only provided by law restricting freedom of expression is acceptable and goes on with the right to privacy and other remaining issues in need to be discussed. The second part is regional and looks into how the Internet has been perceived in three regions of the world. Primarily, this section deals with issues relating to the People’s Republic of China (PRC), but also with some insights from the Middle East and North Africa (MENA) region, sub Saharan Africa and Latin America. The third and final part looks into what

1 Information and communications technology (ICT), is often used as an extended synonym for information technology (IT), but is a more specific term that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information as an extended synonym for information technology (IT). Sida’s definition: Electronic means of capturing, processing, storing and disseminating information, see Näringslivssamverkan och ICT, INTEM presentation 130206

2 To better understand what we are dealing with; there are more than 6 billion mobile phones, 4.5 billion (75%) are found in developing countries, and there are more than 2 billion internet users in the world community today. Overall internet users statistics in the world distribution by world regions, Asia 44,8 %, Europe, 21,3 %, North America 11,4 % Lat Am/Carr 10,4% Africa 70% Middle East 3.7% Oceania/Australhia 1.0%, see http://www.internetworldstats.com/stats.htm
the international donor community does in the area on the Internet and freedom of expression and finally focus is being put on Sweden to see what is being done in the area of Information and Communication Technologies for Development (ICT4D). The last section also contains some concluding remarks and some final points of reflection.

1.1 Characterizing the topic
Freedom of expression and ICT creates room for innovation, opposition and awareness; facilitates transparency and is an effective tool to combat corruption and functions as a means to expose human rights violations. Primarily it creates a ground for communication between people, empowers them and opens up for an exchange of ideas and views that gives ground for enhanced decision making and promotes the overall progress of society as a whole. Many countries in the world community, lacking democracy and rule of law, try to find ways to limit freedom of speech and censure established channels that disseminate and enhance communication. However, the spread of new communication technologies has resulted in that a greater public can be reached and makes it more difficult for governments to control and quell citizens’ opinions.

3 B. Tamanaha, On the Rule of Law: History, Politics, Theory, CUP, 2004, p. 3. These states can be seen to have rule by law but not rule of law. The distinction that is being made is that under rule by law, the law can serve as a mere tool for a government to suppress people in a legalistic fashion. While, under the rule of law, the law is preeminent and can serve as a check against the abuse of power.
Common methods of Internet access in homes include dial-up, landline broadband (over coaxial cable, fibre optic or copper wires), Wi-Fi, satellite and 3G/4G technology cell phones. Public places to use the Internet include libraries and Internet cafes, where computers with Internet connections are available. An Internet blackout or outage can be caused by local signalling interruptions. Less-developed countries are more vulnerable due to a small number of high-capacity links. A new term, “netizen” is introduced in order to describe an individual who regularly uses, and communicates through the Internet. Also the term “social media” is being used to refer to the interaction of people in which they create, share, exchange and comment contents among themselves in virtual communities or networks. Social media technologies have developed into different forms including magazines, Internet forums, web blogs, social blogs, microblogging, wikis, social networks, podcasts, photographs or pictures, video, rating and social bookmaking.

Cyber warfare and cyber-attacks refer to politically motivated hacking to conduct sabotage and espionage. Furthermore, the term “digital divide” is used to describe the gap between people with effective access to digital and information technologies, in particular the Internet, and those with very limited or no access at all. In contrast to 71.6 Internet users per 100 inhabitants in developed States, there are only 21.1 Internet users per 100 inhabitants in developing States. This disparity is more evident in the African region, with only 9.6 users per 100 inhabitants.

In addition, digital divides also exist along wealth, gender, geographical and social lines within States. Indeed, with wealth being one of the significant factors in determining who can access information communication technologies, Internet access is likely to be concentrated among socioeconomic elites, particularly in countries where Internet penetration is low. In addition, people in rural areas are often confronted with obstacles to Internet access, such as lack of technological availability, slower Internet connection, and/or higher costs. Furthermore, even where Internet connection is available, disadvantaged groups, such as persons with disabilities and persons belonging to minority groups, often face barriers to accessing the Internet in a way that is meaningful, relevant and useful to them in their daily lives.

1.2 The internet and the right to freedom of opinion and expression

In the last decades very few, if any, developments in information technologies have had such a revolutionary impact as the creation of the Internet has had on the freedom of opinion and expression. Unlike any other medium that communicates one way (newspapers, television and radio) the Internet represents a new way seen as being an interactive medium. The innovation lies in that intermedi-
ary platforms are created that facilitate participatory information sharing and where individuals play an active role in creating an aggregated content. Individuals are not only recipients of information, but also active producers of information. These platforms have a particular value in countries where there is no independent media and where information is controlled by the government. The true innovation with Internet development lies in that information is being shared and that individuals can be part in expressing their right to freedom of expression and opinion. Today approximately more than 2 billion Internet users, more than 34% of the world population, has access to the Internet. Furthermore traditional media producers can greatly expand their audience with relatively low costs. This is being done in a speedy and inexpensive way and where information ultimately transcends national boundaries and adds a new dimension to Globalization.

In some States, Internet access has been recognized as a right. For example, the parliament of Estonia passed legislation in 2000 declaring Internet access a basic human right. The constitutional council of France effectively declared Internet access a fundamental right in 2009, and the constitutional court of Costa Rica reached a similar decision in 2010. Going a step further, Finland passed a decree in 2009 stating that every Internet connection needs to have a speed of at least one Megabit per second (broadband level). Overall, Internet speeds worldwide continue to be faster, led by Asia-Pacific countries South Korea, Japan and Hong Kong, while China remains the source of the largest amount of observed attack traffic. According to a survey by the British Broadcasting Corporation in March 2010, 79% of those interviewed in 26 countries believe that Internet access is a fundamental human right. Furthermore, the Netherlands is the first European country to adopt net neutrality legislation, and the second country in the world, after Chile.

1.3 Safeguarding freedom of expression by normative means

Within the timespan of sixty some years, progress has been made in terms of securing respect for the right of freedom of expression. This has mainly been achieved through the establishment of the United Nations and the human rights seed that was set in the UN Charter 1945. It has led to a human rights development that no one at the time could foresee. The pathway of securing these rights has gone through a number of international and regional human rights instruments. The normative structure that safeguards these rights is found in the 1948 Universal Declaration of Human Rights (UDHR), article 19, and in the 1966 International Covenant on Civil and Political Rights (ICCPR), article 19. Also found in the European Convention on Human Rights (ECHR), article 11, The American Convention on Human Rights, article 13; The African Charter of

---


13 Network neutrality (or open inter-working) means that you are in control of where you go and what you do online. Companies that provide Internet services should treat all lawful Internet content in a neutral manner. It is the founding principle of the Internet and what allows the Internet to be the largest and most diverse platform for expression in recent history, see http://www.internetsociety.org/net_neutrality?gclid=CNT5noyghRgCFQQR2cAnd310UAv

14 The UN Charter preamble makes clear “to establish conditions under which justice and respect for the obligations arising from treaties and other sources of international law can be maintained”.

15 The right of freedom of expression is guaranteed not by one single instrument, but by a number of global and regional human rights instruments, as well as under customary international law.
Human and Peoples’ Rights, art. 9 (Elaborated by a specific declaration agreed in 2002); and the Arab Charter on Human Rights\textsuperscript{16} art. 32.

It should also be underlined that human rights treaties are different than other international treaties because they do not stipulate the mutual rights and obligations of the state parties, but rather, the state party’s international obligation to protect the basic human rights and freedoms of persons within its jurisdiction.\textsuperscript{17} So in the case of freedom of expression everyone has the right to include seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.\textsuperscript{18} Reference being made to the “other media” implies that the founders of the Covenant had in mind to include any other technological developments that could accommodate individuals to express their right to freedom of expression. So the normative structures provided today not only in the CCPR, but in all instruments discussed above, are still applicable to new international communication technologies.

1.4 Restricting freedom of expression

It is acknowledged, that some forms of freedom of expression can harm the rights of others. There is a difference between freedom of opinion and freedom of expression in that the former is seen as an absolute right from where no interference is permitted from society.\textsuperscript{19} Freedom of expressions on the other hand, is not absolute, and can in some cases be legitimately restricted under international human rights law, primarily in order to safeguard the rights of others. However, any limitation that a state is planning on the freedom of expression is a very sensitive matter. This is why international human rights law allows restrictions,\textsuperscript{20} only if they comply with the provisions found in article 19(3) of the Covenant, described as a three-part test:

1. Restrictions shall only be such as are provided by law and are necessary:
2. They shall be made for the respect or reputation of others; or,
3. For the protection of national security of public order, or public health or morals.

Any restriction must also conform to the strict test of necessity and proportionality.\textsuperscript{21} Furthermore the Human Rights Committee (HRCee) has taken the view that any legitimate restriction must be in accordance with the requirements warranted in a democratic society.\textsuperscript{22} There is abundant practice where information has been restricted in exceptional cases. For instance information including child pornography (protecting the rights of children),\textsuperscript{23} hate speech (to protect the rights of affected communities),\textsuperscript{24} defamation (to protect the rights and the reputation of others against unwarranted attacks), direct and public incitement to commit gen-

\textsuperscript{17} M. Shaw, International Law (CUP, 2008) p. 75
\textsuperscript{18} Art 19(3) CCPR.
\textsuperscript{19} M. Nowak, supra note 1, p. 441.
\textsuperscript{20} See art. 4 CCPR, Permissible Derogations in Time of Emergency.
\textsuperscript{21} See CCPR/C/GC/34, paras 21-23.
\textsuperscript{23} Dissemination of child pornography is forbidden under the Optional Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, art. 3, para. 1, 16(c).
ocide (to protect the rights of others), and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life).

However, many states try to restrict, censure, and manipulate information disseminated via the Internet. States may do this without introducing any legal basis or without meeting the criteria under international human rights law. Or if legislation exists, laws may be badly drafted, ambiguous, without any explanation why restrictions are being introduced or in a manner that is evidently unnecessary or simply not foreseeable. Arbitrary use of criminal law to sanction legitimate expectation constitutes one of the gravest forms of restriction to the right, as it does not only create a “intimidating effect”, but also leads to other human rights violations, such as arbitrary detention and torture and other forms of cruel, inhuman and degrading treatment or punishment. Equally important is that freedom of opinion and expression correlates with the right to privacy. The rights of privacy has traditionally developed in such a way that peoples engagement in debates on any subject, controversial or not, has been under the assumption that it can be done anonymously. The Internet gives individuals the possibility to access information and at the same time be engaged in a public debate without having to reveal their real identities. This is often being done through the use of pseudonyms on message boards. At the same time the Internet has developed in such a way that new instruments and mechanisms through which both States and private actors can monitor and collect information about individuals’ communication and activities on the Internet. Such practices can constitute violations of Web users’ rights to privacy, and, underpin people’s confidence and security on the Internet, and may at the same time hamper the free flow of information and ideas online. States have used popular Web sites, such as Facebook, to identify and track human rights dissidents, opposition members and in some cases too, States have registered usernames and passwords to access private communication of Facebook users. TOR (originally short for The Onion Router) is a software system intended to enable online anonymity. The network helps users defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.

Using Tor makes it more difficult to trace Internet activity, including “visits to the Web sites, online posts, instant messages and other communication forms” back to the user.

---

25 See art. 3 (c) of the Convention on the Prevention and Punishment of the Crime of Genocide.
26 See art. 20, para. 2, of the ICCPR.
27 See article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. The ICCPR provides that no one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. It also provides that everyone has the right to the protection of the law against such interference or attacks. Although “correspondence” primarily means written letters, the term today has a broader meaning and covers all forms of communication over distance, including electronically transmitted information.
28 https://www.torproject.org/
PART II – Country and regional approach

2.1 China - freedom of speech and the Internet

When revolts began to spread through the Middle East and North Africa in 2011, and grass root attempts to mobilize protest started circulating on the Internet, the Chinese Government strengthened its grip on electronic communication and appeared more determined than ever before to control cell phone communication, electronic messages, e-mail and access to the Internet in order to avoid any attempts to manifest any anti-government sentiment in China.

The problem with the Internet in China lies in the restricted view the government has on human rights, particularly civil and political rights. Chapter Two of the 1982 Chinese Constitution is entitled Fundamental Rights and Duties of Citizens. This chapter of the Constitution cannot be said to be compatible with international human rights standards but chapter two has a catalogue of rights where freedom of speech is guaranteed.30 The term “human rights” was first introduced into the 1982 Constitution through the 2004 Constitutional Revision.31 The term was with difficulties used before the Constitutional Revision and was ironically only officially used after the June 4 Tiananmen Square Massacre in 1989.32 However, after the State Council issued its white paper, Human Rights in China, in 1991, the term is more often used by government officials and by the Chinese media.33

As expressed in the newly adopted National Human Rights Action Plan (2012-2015), it is made clear that: “China … still has a long way to go before it attains the lofty goal of full employment of human rights”.34

Furthermore, the first released White Paper on the Internet in China, reemphasizes that the “Chinese citizens fully enjoy freedom of speech on the Internet” and that the “government is determined to unswervingly safeguard the freedom of speech on the Internet … in accordance to the law”. On the other hand the White Paper makes clear that “China advocates the rational use of technology to curb dissemination of illegal information online”. The White Paper makes also clear that the Internet sovereignty of China should be respected and protected and that Chinese and foreign citizens, legal persons and other organisations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and consciously protect Internet security.35

30 See Articles 33-50 of the 1982 Constitution. It is adequate to make a reference to Confucius (551-479 f.Kr) who did not recommend blind obedience to the ruler (the state). When Zilu asks him “how to serve a prince”, Confucius replies: “Tell him the truth even if it offends him”, Analects 14.22.
31 See Article 33 of the 1982 Constitution that declares, that “[t]he State respects and protects human rights”
34 National Human Rights Action Plan (2012-2015), China Daily, June 12, 2012, this is the second Human Rights Action Plan in China, the first was only valid for a year 2009-2010.
2.2 Means of censoring the Web

Today China has in place one of the most sophisticated and extensive system for controlling information on the Internet and has adopted extensive filtering systems, popularly known as the “Great Fire Wall” that is controlled by the Government. The purpose is to block access to websites that contain “sensitive” terms such as i.e. “democracy” and “human rights”.\(^{36}\) On the other hand China has one of the most dynamic Web users community in the world, which makes the country the fastest growing Internet community in the world,\(^ {37}\) and possibly also the most difficult one to control. There is an estimated 597 million people active on social media in China today and the country’s top 10 sites actually have 3.2 billion individual accounts. The volume of social sharing went up by 60% in 2012 alone.\(^ {38}\) However, the apparatus of China’s Internet repression is considered more extensive and more advanced and resourceful than in any other country in the world. China also has about 50,000 police officers that not only block websites but also monitor internet access of individuals.\(^ {39}\) In addition to its massive firewall and intrusive software the Chinese government employs thousands of paid commentators who act as regular Web users to counter criticism of the government. The commentators are known as the “50-Cent Party” (wǎngluò pínglùn yuán) as they

\(^{36}\) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16 May 2011. But also issues relating to the Dalai Lama, the 1989 crackdown on Tiananmen Square protesters, Falun Gong, dissidents and other human rights related Internet sites are being blocked. Also words like “freedom” and “death penalty” are being blocked by the government. However the United Nations Website on human rights is accessible for Web users without any visible restrictions in China.


\(^{38}\) http://www.techinasia.com/2013-china-top-10-social-sites-infographic/

\(^{39}\) http://www.hjalmarsonfoundation.se/2012/03/china-40-000-police-officers-monitor-the-internet/, also in TEMA När IT Används som Vapen, 130124.
are said to be paid 50 cents for every post that steers a discussion away from anti-party content or that advances the Communist Party line. China-based Web sites cannot link to overseas news Web sites or distribute news from overseas media without separate approval from the State Council Information Agency. Only “licensed print publishers” have the authority to deliver news online. Non-licensed Web sites that wish to broadcast news may only publish information already released publicly by other news media. Furthermore, content providers are responsible for ensuring the legality of any information disseminated through their services and give government officials full access to any kind of sensitive information they wish from providers of internet services. The Governments strive to promote general and hassle-free Internet accessibility where citizens’ freedom of speech is guaranteed online appears to be everything else than hassle-free.

2.3 MENA – freedom of speech and the Internet

Tunisia, Egypt, Syria and Libya

The Jasmine Revolution that begun in Tunisia in December 2010 sent shock waves across the MENA region and began a process, which has since become known as the “Arab Spring”. The Tunisian government was in most cases the first country in the region to begin using communications surveillance, censorship and control technology. The censorship that started with simple filtering lists of websites culminated in a targeting of specific individuals, whereby personal user accounts and public websites were hacked. Notably most of the repressive technology systems were developed with support from European and American companies.

As a desperate last attempt before Ben Ali fled the country in January 2011, it was agreed to remove all censorship and institute a free press and within hours this decision was implemented and cites that were not accessible before for Tunisians were suddenly open. However much of the infrastructure of censorship and surveillance is still in place in Tunisia. The killing of Tunisian opposition politician Shokri Belaid in February 6, 2013 - the first political assassination in Tunisia since the Arab Spring uprising in 2011 have sparked angry protests across Tunisia and will most likely have repercussions on Tunisia’s peaceful revolution. Now it remains to be seen to what extent the new political space in Tunisia may enable more fundamental changes.

Seeing the change that had been possible in Tunisia led to widespread protests across the region, with Egypt as one of the first countries where mass public demonstrations took place. Unlike Tunisia however, Internet censorship in Egypt was far less restrictive than was the case in Tunisia. When restrictions of freedom of

---

40 See http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party
42 Ibid., Article 11 and 14.
43 See R. Peerenboom, ‘Assessing Human Rights in China: Why the Double ‘Standards’, 38 Cornell Int’l L.J. 71 2005. Pp. 104-107. People have been sentenced between two-six years for inciting subversion for publishing on the Internet in cases where they have been advocating the overthrow of the CCP or the government and criticizing the Three Represents among other issues that have been dealt with by courts.
44 The following presentation only follows the events in some of the countries in the MENA-region.
46 What should also become evident is that the infrastructure of Internet censorship began long before the Arab Spring in Tunisia and was an integral part of Internet communications in Tunisia. Indeed the entire Tunisian Internet was constructed to allow interference and the harming of human rights. Internet architecture was centralised and the role of the private sector was severely limited in order to ensure that the regime had maximum control over Internet communications.
47 http://www.bbc.co.uk/news/world-africa-21366235
expression took place on the Egyptian Internet, these were not a product of Internet filtering, but rather of more general surveillance. Both bloggers and journalists alike, who were identified as overstepping what the Egyptian establishment perceived as ‘red lines’, were arrested and detained, often for indefinite periods of time without trial. Instead of building an Egyptian censorship infrastructure, the state has focused on a broad surveillance network across communications mediums. This was done in close co-operation with an American technology developer and a local technology integrator, who built Internet surveillance systems in Egypt and exported them across the MENA region. Telecommunications technology was equally subject to extensive surveillance, but it was only during widespread public protests in Egypt that the restriction of communications in Egypt received worldwide public attention. The Egyptian attempt to control various forms of communications came to a critical turn during widespread public protests in early 2011. Known today is that Egypt ‘switched off’ the Internet for several days in January 2011. Not only was the Internet turned off and propaganda SMS were forcibly sent out by the regime before turning off the entire mobile phone network in Cairo. These steps were taken by local mobile telecommunications operators under direct threats of force by the Egyptian military directed at local staff. While these local operators did consult with their corporate headquarters in Europe, they saw little alternative but to do the bidding of the military. At the same time mobile phone operators have come under considerable pressure for their complicity in supporting the regime in its actions. Particularly considering the legitimate concerns of civil society and human rights advocates, there seems to be some space to develop initiatives, which promote human rights in this context. The strong linkage of many telecommunications operators in the MENA region to Europe is as evident in Egypt as it is in Tunisia.49

Another country inspired by the Arab Spring in Tunisia is Syria, although hopes of a similar success of non-violent protests have been crushed increasing accusations of war crimes and reports of the terrible violence, with more than 60,000 Syrians killed overall (January 2013 UN estimates). The total number of registered refugees and individuals awaiting registration is 792,118. This includes 6,338 Syrian refugees registered in North Africa. 50 In this regard it is impossible to discuss the communications environment in Syria outside of this context. Communications media have historically been severely restricted in Syria, with censorship and surveillance rife. However in contrast to the similarly restrictive regimes in the region, the Syrian Internet architecture is far less developed than in countries such as Tunisia. This means that slow and under-developed Internet architecture is further limited and slowed down by additional layers of censorship and control. Additionally telecommunications and Internet surveillance have been used to target specific activists and bloggers who are considered particularly dangerous. These are then detained or imprisoned as part of a wider regime strategy to limit political expression and intimidate human rights defenders and political activists. The extent to which the Syrian government was surveilling its citizens became apparent when the global hacker community discovered that many of the North American Internet surveillance devices on the Syrian Internet were entirely insufficiently protected. This led to an astonishing amount of data being published from North American Internet surveillance devices within Syria, which demonstrates the extent to which the regime was studying the actions of its citizens. However, the Syrian government embarked on an even

more ambitious project to increase the level of surveillance in Syria. The system was custom built by a consortium of European companies from Italy, France, Germany and also included North American technology. Together their more advanced system would have allowed for an additional “crackdown on protests” and an even greater violation of Syrian citizens human rights. From a corporate social responsibility (CSR) perspective, the companies engaged in the consortium were building this system during extensive public protests and widespread violence in Syria.\footnote{CSR and due diligence, see The UN Guiding Principles on Business and Human Rights – Foundation and Implementation (Raluca Mares ed), Martinus Nijhoff Publishers, 2012.} It seems hard to believe that none of these corporations had any knowledge of the on-going political situation, or that they were unaware how the system they were building in Damascus would be used. The public outcry that followed the publication of investigative reporting about the complicity of European companies in supporting the Syrian regime eventually led the consortium to pull out of Syria in November 2011. At the beginning of December, the Council of the European Union passed additional sanctions, to specifically restrict “equipment and software intended for use in the monitoring of the Internet and telephone communications”\footnote{http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=75431}.  

Another country to witness widespread public protests following the Arab Spring in Tunisia is Libya. However like Syria, non-violent protests were quickly marred by bloodshed and the resulting conflict led to tens of thousands of deaths in Libya. In response to Muammar el-Qaddafi’s continued assaults on civilians in Libya, the United Nations Security Council adopted a unanimous and historic resolution.\footnote{UNSCR 1973 (2011) 26 February 2011 The resolution formed the legal basis for military intervention in the Libyan civil war, demanding “an immediate ceasefire” and authorizing the international community to establish a no-fly zone and to use all means necessary short of foreign occupation to protect civilians.} Despite a highly questionable human rights record, Internet access in Libya seems to have been relatively unrestricted until 2011. This does not mean however that it was not extensively surveilled, with surveillance technology from North America built into the network. However it is only after the revolution that a broader picture of what Internet surveillance took place is being published. The Libyan Internet surveillance systems involved technology from companies not only in North America, but also from Europe, with one French company providing surveillance technology. What is notable in Libya is that European companies were openly selling technologies to the regime that went far beyond even highly invasive lawful interception technologies.\footnote{http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=75431 Information describing technologies used in Libya described this as the shift “from Lawful to Massive Interception”. Exporting these systems has drawn widespread criticism from human rights groups and has recently become the subject of a court case in France, which accuses a French company of “complicity in acts of torture in Libya”.} Following the Egyptian example, Libya also decided to ‘turn off’ the Internet in the country during extensive public unrest in 2011. However rather than completely blocking all forms of Internet communications, the country allowed traffic to certain government sites to pass while blocking access to others. This more nuanced approach can be seen as another stage in the development of such repressive techniques as part of a wider learning process between authoritarian regimes in the region.

2.4 Freedom of expression and Internet in Sub-Saharan Africa

Many sub-Saharan African governments view the Internet as a key tool for development and are developing ICT policies accordingly, though the region still lags behind the rest of the world in both number and percentage of Internet users. Sub-Saharan Africa has a history of media abuses and restrictions on freedom of...
the press, and the region would seem a likely setting for equally restrictive Internet policies. African Internet users account for less than 5 percent of the world’s online population, and many countries’ Internet penetration rates\(^5\) are less than 1 percent. This is likely to change in the near future, particularly with the growth of the mobile Internet and the rapid increase of mobile phone use in the region.\(^6\)

Likewise, many sub-Saharan African governments, recognizing the potential of ICT to encourage development, have made serious efforts to expand Internet access in their countries.\(^7\) Though most governments agree that greater use of ICT is beneficial for their citizens, sub-Saharan African countries vary vastly in the scope and availability of Internet services.

Even though many sub-Saharan African constitution’s guarantee freedom of expression and of the press, many governments use laws against defamation and

\(^5\) Countries with the highest penetration rate: Iceland 97.8%, Norway 97.2%, Sweden 92.9%, Falkland Islands 92.4%, Luxembourg 91.4%, Greenland 90.2, Australia 89.8%, Netherlands 89.5, Denmark 89.0, Finland 88.6, see Top 50 countries with the highest internet penetration rate, http://www.internetworldstats.com/top25.htm

\(^6\) See supra note 2.

\(^7\) In April 2009, the government of Zimbabwe announced a plan to establish Internet cafés at post offices in rural areas. Rwanda’s 2006-2010 ICT plan, which covers education, governance, infrastructure, legislation and human capacity development, is aimed at helping the country “leapfrog” into the digital-era global economy.” Uganda’s 2009/2010 government budget includes support for expanding current ICT infrastructure, linking most of the country’s major towns through 1500 km of optical fiber and providing for connectivity to ease the transition to the East African Submarine Cable System (EASSy), scheduled to be completed in June 2010.
laws protecting national security to curtail these freedoms. However, many countries in the region have recently developed or are currently developing legislation addressing cybercrime and online security.58

The events of September 11, 2001 have also led governments around the world to develop new anti-terrorism legislation; sub-Saharan Africa is no exception. These laws often grant governments expansive surveillance privileges and reduce citizens’ right to privacy. Kenya’s 2003 Suppression of Terrorism Bill prohibited “collect[ing],” “mak[ing]” or “transmit[ting]” information that was deemed to be helpful to terrorist organizations, including online information. The bill prompted such an outrage among Kenyan citizens, many of whom worried about how the government’s planned to define what constituted “helpful” information, that the Kenyan parliament eventually rejected it. However, anti-terrorism bills in countries ranging from South Africa to Tanzania have increased governments’ ability to conduct surveillance for loosely defined national security purposes.59

2.5 Internet filtering in sub-Saharan Africa

In most of sub-Saharan Africa, the technical approach to Internet filtering has not changed much since the late 1990s.60 Sporadic IP blocking of sites, rather than more sophisticated Uniform Resource Locator (URL) blocking, is the norm, and most filtering targets political content.61 However, many countries in the region also practice more indirect forms of censorship such as arresting or threatening bloggers, online journalists, and other Internet users. This type of indirect censorship can be difficult to measure, and its effects may reach deep into sub-Saharan African online communities, causing Internet users to self-censor or avoid attempting to access sensitive content out of fear of government retribution.

Attempts have been made to test the presence of technical Internet filtering in four sub-Saharan African countries in 2008-2009: Ethiopia, Nigeria, Uganda, and Zimbabwe.62 Despite government attempts in all four countries to control information, only Ethiopia was found to be filtering the Internet. Ethiopia’s filtering regime targets independent media, blogs, and political reform and human rights sites, though the filtering is inconsistent: many prominent sites that are critical of the Ethiopian government remain accessible, while some blocked sites seem harmless. All blogs hosted at blogspot.com and nazret.com, a site the aggregates Ethiopian content, are blocked. The sites of opposition political parties, minority ethnic groups, independent news organizations and Ethiopia-specific human rights organizations appeared to be a priority for blocking, though many international sites containing comparable information (such as CNN, Voice of America, Human Rights Watch and Amnesty International) were not blocked.

In March 2009, Ethiopia unblocked a number of Web sites supporting political reform, including the Committee to Protect Journalists, in what may have been a reaction to the February 2009 release of a United States Department of State report on human rights in the country.

Testing in other countries revealed no evidence of filtering. However, it was found that six ISPs in Nigeria all appeared to be allowing unrestricted access to the Internet.63 These results concur with testing conducted near the 2007 elections, during which ONI concluded that no filtering took place. In Zimbabwe, despite severe press restrictions and pervasive surveillance of online communic-
tions, ONI found that the government has not yet implemented an Internet filtering regime. In Uganda, ONI testing revealed no evidence of filtering. However, though the government does not actively filter the Internet, it temporarily blocked the site of an independent radio station during the 2006 presidential elections, blocking access to over 600 unrelated sites in the process. Similar incidents were however reported during the 2011 elections.64

2.6 South Africa Freedom of expression and the Internet

Freedoms of expression and of the press are protected in the constitution and generally respected in practice, and South Africa has vibrant journalists and press freedom advocacy organizations. However, several apartheid-era laws and a 2004 Law on Antiterrorism permit authorities to restrict reporting on the security forces, prisons, and mental institutions. Moreover, recent legislation could further restrict the scope of permissible reporting in South Africa. In 2009, the controversial Film and Publications Amendment Act was signed into law to protect against child pornography and hate speech. The legislation – which requires any publisher not recognized by the press ombudsman to submit a wide range of potentially “pornographic” or “violence-inciting” materials to a government board for approval – was widely criticized by press freedom advocates as a means of pre-publication censorship. In November 2011, the Constitutional Court accepted a multiparty legal challenge to the law.65

The constitution protects the right of access to information, and the Promotion of Access to Information. However, recent years have seen a stark increase in the use of court interdictions and gag orders66 by both governmental and non state actors. Since 2005, the Mail & Guardian has received at least three gag orders to stop reporting on corruption scandals. In addition, the ANC is considering legislation to establish a statutory media tribunal, replacing the self-regulating Press Council and Press Ombudsman with a state-run body empowered to hear complaints against the press, hand out stiff punishments for violating privacy and for defamation, and force the media to issue retractions and apologies. In July 2011, determined to respond to the ANC’s proposal, the South African National Editors’ Forum (SANEF) and Print Media South Africa (PMSA) established an independent body of individuals, the Press Freedom Commission (PFC), with a mandate to identify the most efficient and effective regulatory system for the print media in South Africa by spring 2012.67 Journalists are occasionally harassed and threatened by both government officials and non-state actors over the content of their reporting.

The Internet is expanding in South Africa, which is one of the most technologically-resourced countries on the African continent. Internet access is unrestricted, although state monitoring of telecommunications systems is authorized. By the end of 2011, 21% of the South African population had access to the internet. Access is expanding rapidly and more people have the option to access the internet from their mobile phones than from computers. However, the majority of the population is unable to benefit from internet access due to high costs and the fact that most content is in English, an obstacle for those who speak one of the 10 other

---

64 Ibid.
66 A gag order (also known as a gagging order or suppression order) is an order, sometimes a legal order by a court or government, other times a private order by an employer or other institution, restricting information or comment from being made public, or in some cases, passed onto a third party, for the purpose of “hiding” or “covering up” or “white-washing” compromising, questionable, deceptive practices, fraud, or other illegal activities with the help of the legal process itself, or to protect the privacy of victims or minors.
official languages. However, there is now content in some local languages, especially on social-networking platforms.68

2.7 Latin America – freedom of speech and the Internet

Chile, Venezuela, Mexico Colombia and Brazil

What can be said here is that most countries in Latin America recognize the value of the Internet as an integral part of modern life.69 For example, numerous groups in Chile have recommended legislation to make access to the Internet a right, alongside access to clean water and shelter. On the other hand, in December 2010, the Venezuelan Congress approved a bill to regulate access to content and the use of the Internet in the country.70 Under this law, access to websites that distribute messages or information that “may be contrary to national security” or that seek to “discredit legitimately constituted authorities” may also be restricted. Moreover, the law reform provides that “the Government will create an interconnection or access point to the network of Internet Service Providers in Venezuela for the purpose of handling the traffic originating in and sent to Venezuela, in order to achieve a more efficient use of the networks of the country, given the strategic nature of the sector.”

Access Providers would be required, since then, to establish mechanisms capable of restricting the dissemination of messages, access to portals and disclosure of information related to the actions subject to the regulations. Such a devise would clear the way for network filtering, to the detriment of freedom of information on line.71 As “the project contains serious deficiencies as regards legislative practice as it allows officials who have the responsibility of enforcing this legal instrument to act arbitrarily and discretorily, which constitutes per se a violation of the human right of freedom of expression and leads to a selective and interested enforcement”.72

In Mexico, the Party of the Democratic Revolution73 has submitted a bill that intends to monitor and regulate the use of social networks in the country. According to the bill, the mere exchange of information that helps others violate the law would be considered a crime. The bill was defended because it created an online police force to monitor and hamper the way drug cartels were using the net. Mexican Internet users had a critical reaction to the proposal: many asserted that the law would serve as a mere excuse for the government to increase surveillance; the term Big Brother was used to refer to the position the police has sought to take.

Similarly, in April 2011, the Ministry of Justice of Colombia brought a bill before Congress that intends to regulate the Internet and its content. The bill allows ISPs to remove or block access to content preventively, in the event someone claims that such content violates copyrights. Civil society has expressed its dissatisfaction with the law, calling it the Hadopi Law, after the French law, which provides a 3-strike procedure to suspend the Internet connection for violation of copyrights.74

68 South Africa: Internet users 30 June 2012: 8,500,000, Penetration rates:17.4%, internet Africa, 3.1%, Facebook, 6,269,00, see http://www.internetworldstats.com/stats1.htm
69 Population ,579,092,570, % pop. Of world 9.0%, Internet users 31-Dec-11 230,928,238, penetration % pop 39.9%, user % world 10.1%, Facebook 31-Dec-11, 145,147,740, seehttp://www.internetworldstats.com/stats1.htm
70 The bill was proposed to amend the Law on Social Responsibility in Radio and Television which already restricts content broadcast by radio and television stations, and attempts to restrict, among other issues, the dissemination of messages that “may constitute media manipulations aimed at creating social unrest or disturbing public order.”
72 Diagnosed by the NGO Espacio Público.
73 Partido de la Revolución Democrática.
In Brazil, all access to YouTube has already been blocked under a court decision issued within the framework of a process in which a very famous top model was involved. The model had been exposed in the portal through an amateur video that captured images of her and her boyfriend at the beach, which were considered to be inappropriate for minors. This event started a discussion about why and how to regulate the Internet and protect the rights of access of citizens.

Most Latin American countries have ratified the American Convention on Human Rights, which lays down rules on censorship. Similarly, the Tunis Agenda also recognizes these rights within the Information Society, and provide freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. The same provision affirms that: “measures undertaken to ensure Internet stability and security, to fight cyber-crime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.”

However, despite the fact that freedom of expression depends on the free flow of information, there is a tendency for national and regional laws to intervene in the end-to-end architecture of the Internet, prevent the free flow of information and thus undermine the rights of every citizen to freedom of expression and privacy. It is necessary to closely follow this alleged tendency towards increasing censorship of online information, as several Latin American governments, and governments around the world, have proposed legal texts that impose criminalization of legitimate expressions; liability of intermediaries; and disconnection of users on the pretext of violations to copyright or transmission of illegal information (such as pornography, drug trafficking, cyber-attacks, etc.), or that simply establish arbitrary mechanisms to filter, block and remove content from the net and fail to provide an adequate protection of the rights to privacy and protection of personal data. All these provisions are rather reprehensible, as they not only jeopardize the fundamental rights to privacy and freedom of expression of citizens, but also pose a threat to some of the key elements of the network architecture, such as neutrality and openness.

Meanwhile, while developed countries have already established a legal framework for the Internet, the movement in Latin America is still recent. As the Internet in nature knows no bounds, establishing regulations influences the freedom of access and customs of countries; therefore, it is important that developing countries also define standards to be evaluated and discussed globally.

---

75 Art. 13, see supra.
77 See article 42
PART III – International Donors – freedom of expression and the Internet

3.1 Millennium Development Goals (MDGs)
At the international level, Target 8f of the Millennium Development Goals calls upon States, “in consultation with the private sector, [to] make available the benefits of new technologies, especially information and communications.” The necessity of achieving this target was reiterated in the 2003 Plan of Action adopted at the Geneva World Summit on the Information Society, which outlines specific goals and targets to “build an inclusive Information Society; to put the potential of knowledge and [information communication technologies] (ICTs) at the service of development; to promote the use of information and knowledge for the achievement of internationally agreed development goals”. To implement this plan of action, in 2005, the International Telecommunication Union launched the “Connect the World” project. Another initiative to spread the availability of ICTs in developing countries is the “One Laptop Per Child” project that has been supported by the United Nations Development Programme. This project distributes affordable laptops that are specifically customized for the learning environment of children. Since 2006, 2.4 million laptops have been distributed to children and teachers worldwide. In Uruguay, the project has reached 480,000 children, amounting to almost all children enrolled in primary school. States in Africa lag behind, but in Rwanda, over 56,000 laptops have been distributed, with plans for the figure to reach 100,000 by June 2011.

UNESCO recognizes that the Internet holds enormous potential for development. It provides an unprecedented volume of resources for information and knowledge and opens up new opportunities for expression and participation. They assume their responsibility of promoting freedom of expression on Internet and have integrated it to its regular program. The principle of freedom of expression must apply not only to traditional media but also to the Internet and all types of emerging media platforms which will definitely contribute to development, democracy and dialogue.

With growing access to information in cyberspace, there is a raise of limit of access and information in cyberspace, done by a variety of actors which have diverse goals and values. In addition to Internet’s trans-border feature, there are so many factors shaping the level of free expression on Internet, and there exist various policy approaches which have implication on freedom of expression. The real challenge is to fully exploit the potential of new media while not compromising civil liberties, including the right to freedom of expression, to education and also to privacy. Furthermore UNESCO seeks to trigger discussion on a wide

range of issues related to Internet freedom at global, regional and national levels. They also take the responsibility to explore the changing legal and regulatory framework of Internet and provide member states with policy recommendations aiming to foster a conducive environment to freedom of expression on the net. In order to reach out they have organized a series of workshops in past WSIS Forum and Internet Governance Forum meetings since 2006 to trigger debates on freedom of expression and privacy protection. UNESCO published a pioneering standard-setting report on Internet freedom titled “Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet”.82

3.2 What is ICT4D?
Information and Communication Technologies for Development (ICT4D) refers to the use of Information and Communication Technologies (ICTs) in the fields of socioeconomic development, international development and human rights. The purpose with this new development is that more and better information and communication technologies further the development of a society.

Aside from its reliance on technology, ICT4D also requires an understanding of community development, poverty, agriculture, healthcare, and basic education. ICT4D is aimed at bridging the digital divide and aid economic development by fostering equitable access to modern communications technologies. It is a powerful tool for economic and social development.83

83 Other terms can also be used for “ICT4D” or “ICT4Dev” (“ICT for development”) like ICTD (“ICT and development”, which is used in a broader sense) and development informatics.
ICT4D can mean as dealing with disadvantaged populations anywhere in the world, but it is more seen with applications in developing countries. It concerns with directly applying information technology approaches to poverty reduction. ICTs can be applied directly, wherein its use directly benefits the disadvantaged population, or indirectly, wherein it can assist aid organisations or non-governmental organizations or governments or businesses to improve socio-economic conditions.

3.3 Swedish development assistance – freedom of expression and the internet

Even though the Arab revolution can be seen as a new event that sparked ICT4D, Sweden has since the mid-1990s been working with freedom of expression and ICT related issues. Questions relating to ICT4D are highly prioritized for the Swedish government. Swedish Foreign Minister Carl Bildt and US Secretary of State Hilary Clinton have been instrumental in the establishment of a UN resolution upholding the principle of freedom of expression and information. The resolution was endorsed by the United Nations Human Rights Council in 2012. The resolution affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice. This is a high priority issue and is reflected in the government bill 2013.

Sweden adopted strategy for special initiatives for democratisation and freedom of expression, 2012–2014, governs Sida’s implementation of special initiatives for democratisation and freedom of expression in development cooperation. The strategy aims to strengthen agents of change, primarily individuals and civil society actors promoting democratisation and freedom of expression. Through the strategy, the Government complements and strengthens its other work for democratic development and human rights. Activities consist of both planned long-term activities and urgent measures to assist agents of change promoting democratisation and freedom of expression.

Information and communication technologies (ICT) as tools for democratisation and freedom of expression are becoming more important. Initiatives in this area are to be enhanced in the strategy’s implementation compared with the previous period’s strategy. Funds amounting to SEK 215 million were at Sida’s disposal in 2012 for the implementation of the strategy. The volume for future years will be determined in connection with decisions on Sida’s letter of appropriation for each year.

The overall idea is to enhance agents of change to obtain exchange and disseminate information in order for them to be able to express their views. These agents are to be given the opportunity to work for pluralism and freedom of opinion, to pave the way for democratic, transparent decision-making and enhance legislation in this area that limit freedom of association, freedom of religion, free-

87 http://www.regeringen.se/content/1/cb/19/66/62/502be5cc.pdf
88 See Sida’s Portfolio within Democracy and Human Rights 2011.
90 See also Per-Einar Töftner’s memo see supra note 78, that explains in which Sida strategies and policies ICT4D signals are included. It is concluded that ICT is included in all strategies and with particular focus on ICT for democracy/HR and freedom of speech (and also regarding ICT and health and ICT and education).
dom of the press, access to the internet, the right to a fair hearing in court and the right to defense, that otherwise restricts civil rights and liberties.

Support is to be given primarily to individuals, groups or civil society organisations, including human rights defenders, trade unions, journalists, politically active and party-affiliated organisations, cultural actors, researchers, women’s rights groups, religious communities, youth associations and other relevant actors working for greater democratisation and freedom of expression.\(^90\) Within the ICT4D area Sida works both with direct efforts and with interventions that are integrated. The ones with direct action are primarily within the area of civil and political rights. Efforts to support documentation of offenders and crimes against human rights such as torture can be mentioned here. They may consist in supporting IT security for dissidents and activists, enabling net publishing or investigative journalism through social media, electoral support and the enhancement of radio broadcasting stations.\(^91\) The indirect ones, mainly concern public administration, computerized case management in the judiciary, production and publication of statistics. This is done in order for the public to be able to access statistical information, to enhance communication with authorities through text messages (SMS) and e-mail and more effective recovery of taxes.\(^92\)

In countries where Sida is actively involved there is a need for a higher capacity and competence to tackle human rights. Parliaments and judiciary need both space and capacity to enact and enforce laws which guarantee freedom of expression and right to information as well as equitable access to ICT. This is particularly the case between urban and rural areas. Likewise, public administration needs increased capacity to open channels including ICT in order to communicate with citizens. Government procurement services can be more transparent if bids are channeled through official websites which also counters corruption. Enhancing public financial management therefore becomes absolutely central to recognizing the right to information, according to Sida’s assessment. The number of states that have enacted constitutional protection regarding the right to information have increased fivefold since 1975, but there are also states where development appears to go backward such as South Africa discussed above. Political parties, civil society organisations, trade unions, student movements and other crucial actors need ICT. In many developing countries, access to the Internet is inadequate. What Sweden in particular can contribute is the perspective of the poor on development and a right perspective. This implies equal access to technology in combination with support to create conditions for poor people to use Internet in an open society where freedom of expression and right to information are met. Sida believes that approach is crucial in order diminish the gap between people with effective access to technology, in particular the Internet, and those with very limited or no access at all.

3.4 Conclusion

This analysis shows that there are strong links between freedom of expression and ICT. This new form of electronic intake of information hugely expands the capacity of individuals to enjoy their rights to freedom of opinion and expression. This combination of receiving and imparting information and ideas boosts and empowers individuals to participate in processes that may contribute to change.

\(^90\) Annex to Government decision of 29 March 2012 (UD 2012/21825/UD/UP).

\(^91\) Resultat för rättvisa och utveckling, s. 83.

\(^92\) It is not possible with any degree of certitude to estimate the amount of direct efforts with interventions that are integrated and the amount set aside for ICT4D overall. Sida follows the system that OECD DAC for statistical coding assistance and lacks sector code for ICT4D. However, Sida’s assessment is that the number of projects in which ICT4D is included has increased which is shown in Sida’s internal reportsystem (See Resultatbildaga till Sidas årsredovisning 2011, s. 84.)
Therefore, people must have the same rights online as offline. The normative structure of international human rights law underscores that there should be as little restrictions as possible on the flow of information and that information should be restricted in only exceptional cases prescribed by international human rights law. Furthermore, that any legislation restricting the rights to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory. There should be adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application as found in a democratic society governed by the rule of law.

This analysis also discerns that there is increasingly sophisticated blocking or filtering mechanisms used by States for censorship. This was particularly the case in the PRC. The lack of transparency surrounding these measures also makes it difficult to ascertain whether blocking or filtering is really necessary for the purported aims put forward by States for censorship. Furthermore using the explanation of protecting national security or countering terrorism cannot be used to justify restricting the right of expression, unless it can be demonstrated that it is intended to imminent violence, it is likely to incite such violence, and there is a direct and immediate connection between the expression and the likelihood or occurrence of violence.

It is also clear that while States are the primary duty-bearers of human rights, corporations also have a social responsibility to respect human rights, implying that they should act with due diligence to avoid infringing on the rights of others. Cyber-attacks constitute a States violation of its obligations to respect and protect freedom of opinion and expression. Websites of human rights organisations, people critical to government ruling, disclosing corruption, torture or other embarrassing facts to the State have increasingly become targets to cyber-attacks. Disregarding the fact that ICT hugely expands the capacity of individuals to enjoy their rights to freedom of opinion and expression there are still opposing forces, run by states that are trying to restrict dissemination of information. Full guarantees of the right to freedom of expression must be the norm, and that any limitation considered as an exception of this principle, should never be reversed.

ICT4D does right to focus on agents of change working to promote democratisation and freedom of expression in countries where these rights are threatened. Support should be granted to long-term and strategic activities to strengthen democratic development and freedom of expression and to urgent measures in order to assist individuals and civil society actors. Attempts should also be made to diminish the digital divide between people with effective access to digital information and those with very limited or no access at all.

---

93 The UN Guiding Principles on Business and Human Rights – Foundation and Implementation, supra note 51.
REFLECTIONS

• Popular uprisings equipped with ICT are powerful movements but they do not necessarily lead to democratic development.

• States discussed in this analysis have flaws and rule of law deficits, and therefore a relevant reflection is why not more emphasis is being put by donors on rule of law/legal empowerment and ICT4D.

• Many of the surveillance systems involved in suppressing “democratic” movements use technology from companies not only from North America, but also from Europe and other western countries.

• How can Sida guarantee that Swedish support for ICT4D is not channeled in a way that possibly can suppress democratic awakening?

• Why is not more emphasis being put by donors on CSR to control the flow of Internet surveillance technology?

• Many countries favor Internet neutrality and TOR’s but what about using the Internet to disseminate child pornography and when should sophisticated blocking or filtering mechanisms be permitted?