Chapter 15
Social Media Censorship vs. State Responsibility for Human Rights Violations

Case Study of the Arab Spring Uprising in Egypt

Joanna Kulesza

Abstract The chapter presents the contemporary international consensus on the limits of the right to free speech online. The author examines state-imposed online filtering in terms of its compliance with international law, especially with human rights treaties granting freedom of expression and access to information. The White House implemented "Internet Freedom" program, whose aim is to introduce software enabling the circumvention of local content control in "filtering countries", is thus subject to thorough analysis. The analysis covers recent (2011) events in Egypt, where the world's first successful attempt at shutting down the Internet within state borders was completed. Although enforced through legitimate state actions this first-ever Internet shutdown was circumvented with technology offered by U.S.-based Google. This technology and its use seemed to meet the goals of the "Internet Freedom" program, introduced by the White House a few months prior to the Egypt events. In the course of the argument, the author discusses international responsibility for the possible breach of their international obligations by both: Egypt and the U.S. She provides for the assessment of the legality of the actions of Egyptian authorities' executing a nationwide ban on Internet that constitutes an infringement of freedom of expression, as well as the responsibility of the United States for their failure to halt a U.S. legal entity enabling users to circumvent Egyptian blocking.

Keywords Internet • Free speech • State responsibility • International law • Internet governance • Sovereignty • Proportionality • Access to information • Human rights • Due diligence

J. Kulesza (✉)
Department of International Law and International Relations, University of Lodz, Kopcinskiego 8/12, 90-232 Lodz, Poland
e-mail: joannakulesza@gmail.com

B. Pătruţ and M. Pătruţ (eds.), *Social Media in Politics*, Public Administration and Information Technology 13, DOI 10.1007/978-3-319-04666-2_15,

15.1 Freedom to Access Information as a Human Right

Freedom of speech holds a well-recognized place in the human rights catalogue. The contents of this right have been defined in a series of international law documents, following the blueprint enshrined in Article 19 of the Universal Declaration of Human Rights (UDHR).[1] According to its stipulations, free speech is composed of three complementary rights: the right to hold opinions, the right to seek and receive information and last but not least the freedom to impart one's own views and ideas. Furthermore, according to this document, considered evidence of customary human rights law, freedom of speech may be exercised "through any media and regardless of frontiers". The non-binding 1948 compromise, worded in Article 19 of the UDHR took almost 30 more years to become the binding International Covenant on Civil and Political Rights (ICCPR),[2] which similarly phrases freedom of speech in its corresponding Article 19. It also confirms everyone's right to "hold opinions without interference" (par. 1), seek and receive as well as to impart information (par. 2) of all kinds. All those freedoms are granted to all regardless of national borders and may be exercised in any form: orally, in writing, print or through any other mean of expression. This article is fundamental to any media law regulation, granting all media the right to freely distribute information. Unlike in the UDHR however, which generally refers to any limitation on human rights in its Article 29 par. 2, Article 19 ICCPR directly deems the right to free speech a non-absolute one.[3] In its Article 19 par. 3, ICCPR identifies this particular freedom as inseparable from special duties and responsibilities resting upon each individual. Since the freedom of speech inherently brings the threat of infringing the rights and freedoms of others, be it through defamation or libel, it may be subject to certain restrictions. Any such restriction however ought to be provided for by law and introduced solely when necessary for guaranteeing the respect of the rights or reputation of others or for the protection of national security, public order, public health, or morals. What is more, it must be proportionate: any restriction is subject to case-specific assessment of the degree of interference confronted with the importance of the purpose of such a restriction.[4]

The UN Human Rights Council (HRC) has gone to great lengths to detail what this general limitative clause of Article 19 par. 3 means in practical terms, when providing its Resolution 12/16 on the freedom of opinion and speech.[5] Yet the

[1] United Nations 1948. Universal Declaration of Human Rights, further herein: UDHR.

[2] United Nations 1966. International Covenant on Civil and Political Rights, further herein: ICCPR.

[3] According to article 29 par. 2 UDHR everyone shall be subject to limitations determined by law states in the exercise of their rights and freedoms. Such limitations may be introduced only to safeguard "due recognition and respect for the rights and freedoms of others" or in order to meet the requirements of "morality, public order and the general welfare in a democratic society".

[4] See e.g.: Deibert (2008) at 81. In the ICCPR regime, the proportionality principle is derived from the word "necessary" used in Article 19 par. 3 discussing the limitative clauses. See e.g.: Yutaka Arai (2002) at 186.

[5] United Nations 2009.

application of those guidelines remains a challenge.[6] Regardless of the difficulties in defining grounds for limiting free speech, such as reasons of national security or protection of morality, it remains undisputed, that blocking access to all information provided through electronic means is a violation of the right to free speech, when exercised without a legitimate justification, based on an act of law applicable in a particular case. Any general blocking of Internet content, in particular keywords-based Internet filtering of websites or services, resulting in depriving all individuals within state jurisdiction of access to certain categories of information is not a proportionate restriction on the right to free speech, as defined by the international law documents cited above, as it infringes the complimentary freedom to seek and receive information. Yet the very fact of limiting access to certain content does not deem the infraction illegal, since, as already stated above, freedom of speech is not an absolute right. The UDHR in Article 29 par. 2 as well as the ICCPR in Article 19 par. 3 both provide for its limitations, however introducing those may only be case-specific, done solely for the grounds named above and based on a particular act of law. A general state-imposed and nation-wide limitation to seek and access information through a particular media or of a certain character may be considered a violation of the limitative clause enshrined in the ICCPR.[7] In some exceptional cases, however, such a general limitation may be considered justified, as described in the derogative clause of Article 4 ICCPR. Also the European Convention on Human Rights regime, which served as the blueprint for the ICCPR definitions of freedom of speech standards,[8] provides that a state's obligation to guarantee such freedom may be lifted in "time of war or other public emergency threatening the life of the nation".[9] Yet even in such a highly exceptional situation freedom of speech must remain granted to aliens while performing their political activities in all respects of Article 10, therefore includes state obligation to grant them the right to seek and share information through all media available.[10]

[6] See generally e.g.: Sadurski (2002).

[7] See Sect. 15.4 below.

[8] Council of Europe 1950. The Convention for the Protection of Human Rights and Fundamental Freedoms is usually referred to as the European Convention on Human Rights, further herein: ECHR. ECHR foresees for the right to free speech in its Article 10. The European Court of Human Rights' (ECtHR) jurisprudence implies a positive obligation of states to prevent any interference with that right, even when such intrusion comes from private third parties, rather than state authorities. See e.g. European Court of Human Rights (2008). In Khurshid Mustafa and Tarzibachi v. Sweden the Court asserted its jurisdiction in a case relating to national court decisions in a case between private parties, where effectively the national court practice disallowed state residents to enjoy rights guaranteed by the convention. See also: European Court of Human Rights (2001), where in VgT Verein Gegen Tierfabriken v. Switzerland the Court asserted that there is an inherent positive obligation of states to ensure the protection of fundamental rights guaranteed by the convention through their effective implementation in national legal systems.

[9] Article 15 ECHR.

[10] Article 16 ECHR.

OpenNet Initiative—an organization focused on monitoring national filtering practice worldwide[11]—defined four primary reasons states name when imposing limitations on the right to seek and impart information.[12] Among those, the social grounds for filtering, usually based on ethical standards shared by national or regional communities, referring to the protection of morality or religious values are the less controversial ones, while states openly claiming limiting access for the reasons of protecting the governing party or authoritarian state leader meet with strong criticism from NGOs and human rights violations allegations.[13] The criticism is usually aimed at state authorities although it is rarely them directly affecting the blocking. They usually introduce stringent legal regulations within acts of national law obliging Internet Service Providers (ISPs) to enforce a form of private censorship over content defined within such act as harmful or potentially dangerous to state interests.[14] As Internet filtering is no longer the domain of authoritarian states however, some democracies also introduce ISP imposed access limitations, yet usually enforced following a court order in a particular case.[15]

15.2 Technology and Regulation of Online Censorship

"Internet filtering" is a term describing a wide variety of activities.[16] Initially, it was used to refer to the practice of states considered to be authoritarian or undemocratic, such as China or Iran, where ISPs were legally bound to deny users access to certain content, e.g. pornographic or immoral according to national laws and local social

[11] The OpenNet Initiative is a collaboration of the Citizen Lab at the Munk School of Global Affairs, University of Toronto, the Berkman Center for Internet & Society at Harvard University, and the SecDev Group seated in Ottawa. See: Open Net Initiatve (2013).

[12] Deibert 2008 at 9. The declared grounds for Internet filtering include: "social" filtering enforced for the protection of morality and other social values, filtering done for political reasons, i.e. preventing criticisms of current political model, filtering done for state security reasons, i.e. aimed at preventing internal unrest, and subsequently limiting access to technical tools enabling circumvention of the blocking being imposed by ISPs.

[13] See e.g.: Noman and York (2011).

[14] See: Deibert (2008) at 32 ff.

[15] See e.g. the Italian court's decision on blocking Access to the Pirate Bay website because of alleged contributory copyright infringement: Doe (2008).

[16] Controlling access to various categories of electronic content may be affected by applying a combination of software and legal methods, but also with the use of extra legal tools and undisclosed methods, including ones outsourced to private parties. Internet filtering is being affected through i.e. hacking or the application of computer viruses, as well as DDoS attacks onto websites containing controversial or illegal content and servers hosting it. See: Deibert et al. (2010) at 6–7. *Distributed Denial of Service Attacks* consists of simultaneous requests for one IP number that is the target of such an attack, sent from various locations and different computers. Consequently, a domain located on a computer with a particular IP number ceases to respond.

standards.[17] That obligation meant that entrepreneurs offering Internet access were legally bound to verify whether online content was intact with national laws and moral norms. Service providers met those requirements in various ways. Initially they were using filtering programs,[18] based on key word searches,[19] also by putting together so-called black lists of prohibited website addresses, offering content deemed illegal within a certain jurisdiction or white lists of websites accessible throughout the country.[20] Some of them would hire administrators and volunteers, following all online content as it was entered online and reporting for takedown whatever part of it they felt was against the law or morality.[21]

Initially, any Internet filtering was considered undemocratic and therefore undesired within democratic states.[22] Individual protesters and NGOs would deem any state censorship contrary to free speech guarantees and the very idea of the World Wide Web, designed for free, global transfer of ideas.[23] Obliging ISPs to distinguish between legal and illegal or moral and immoral content seemed contrary to this basic prerequisite of the web and put them in a very difficult position. Forcing ISPs to verify each and every piece of data through the lens of national laws or morality brought about an undesired chilling effect, raising ISPs to the rank of preventive censors. They would rather disable access to content the legal character of which they found in any way doubtful then face legal charges for hosting it.

Yet, democratic societies were founded on the prohibition of any censorship.[24] Neither in Europe nor in America ISPs were or are obliged to render preventive

[17] In China any content that could endanger "national unity" is deemed illegal, in Myanmar, Egypt, or Malaysia any criticism of the governing party is disallowed. Liberia additionally requires the blocking of websites that include "anti-Liberian materials", while Zimbabwe limits access to any sites that could "raise unease or sorrow". See: Privacy International, GreenNet Educational Trust (2003) at 20.

[18] Filtering software often comes from U.S.-based companies. For example, Cisco software was one of the pillars of the Great Firewall of China, including server-operating programs and ones supporting the national educational networks. Cisco was also working on a Chinese "Next-Generation Network", the so-called ChinaNet Next Carrying Network, CN2. Doe 2004b.

[19] If a domain name or the website include any of the designated keywords, such as "sex" in the case of pornographic content or "Falun Gong" in case of politically motivated one, access to such a website was automatically blocked. Users would usually receive a 404 error message. See: Deibert et al. (2010) at 4–5.

[20] See: Deibert et al. (2010) at 529–530.

[21] Deibert et al. (2010) at 552.

[22] See: Doe (2004a) at 8–9. Yet until 2010 and the U.S. Internet Freedom program, discussed herein below, no state authority directly addressed the filtering policies as undemocratic.

[23] Doe 2004a at 8–9.

[24] Council of Europe (2011b): "Action by a state that limits or forbids access to specific Internet content constitutes an interference with freedom of expression and the right to receive and impart information. In Europe, such an interference can only be justified if it fulfills the conditions of Article 10, paragraph 2, of the European Convention on Human Rights and the relevant case law of the European Court of Human Rights." Furthermore, the Committee emphasized that "states should not, through general blocking or filtering measures, exercise prior control of content

censorship over the content they provide access to.[25] With time, states on both sides of the Atlantic found forever more reasons to limit free access to content, be it for the traditional interests of state security or new reasons like intellectual property protection.[26] Currently the majority of European and American states include in their legal systems so-called notice-and-takedown procedures, affecting free speech online. They provide for ISPs obligations to limit access to certain content deemed contrary to national laws following either a court decision or a notice received from individuals or corporations. ISPs themselves may also limit the amount of information they render access to, as defined within their terms of service. Yet, as a general rule neither in Europe nor in America are ISPs obliged to render preventive censorship, i.e. to verify all the content they host or enable access to for its legality.[27] They are rather obliged to act only when they are made aware of the illegal character of certain content that is already published. What follows is an eager debate on the form and contents of information that the ISPs should be in disposition of and the procedure, based upon which certain content is to be made inaccessible.[28] The notice-and-takedown procedure is being criticized as granting ISPs too much freedom in deciding on the legal character of individual content and censoring information based on their own assessment, without a court decision.[29]

Blocking access to certain content within particular jurisdictions remains therefore an eagerly disputed subject. Those opposing this form of online censorship feel that blocking access to certain content generates unreasonably high costs of filtering software deployed, while not solving the true problem behind illegal content available online. Quite the opposite—it adds to the difficulty in identifying and apprehending the culprits.[30] There is also the element of risk brought about by any form of censorship. Legitimizing it brings about the inevitable threat of authorities using such an exception for other purposes than those originally intended. Black lists of inaccessible websites are being kept secret by the ISPs working together with the police, only at times allowing for civil society participation in putting them together, yet making it impossible to verify through traditional democratic tools the information actually being blocked within a jurisdiction. The black lists are set

made available on the Internet unless such measures are taken on the basis of a provisional or final decision on the illegality of such content by the competent national authorities and in full respect for the strict conditions of Article 10, paragraph 2, of the European Convention on Human Rights." Such measures may only be applied towards "clearly identifiable content" and must be proportionate.

[25] See: Deibert (2008) at 120–123.

[26] See: Open Net Initiative 2013, Reporters without Borders (2013).

[27] But see the recent Delfi v. Estonia case where the ECtHR recognized ISP's editorial liability for user content. ECtHR (2013).

[28] See: European Court of Justice (2010). In the case *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* the Court found that a judicial order to enact prior content control of uploaded and downloaded user data, laid upon a Belgian service provider, is against community law.

[29] See e.g.: Chilling Effects Clearinghouse (2013).

[30] See e.g.: (McNamee 2013).

together by ISPs working together with police enforcement agencies, therefore it is difficult to assess what addresses they actually contain and may serve as a pretext for limiting access to information that is politically dangerous to those in power. Only unlimited access to electronic content may prevent a risk of candid state censorship.

Proponents of limiting access to certain detrimental online content claim that even though the filtering technologies are not perfect, they are one of the numerous preventive measures used to limit the harmful effects of illegal materials, such as child pornography. Effective crime enforcement requires the engagement of all tools available, both off- and online, meaning also disabling access for those who wish to access illegal content online.[31] Just because the method does not guarantee a perfect success rate does not mean one should not impose it. Proponents of such filtering policies include state authorities and law enforcement agencies, but also telecommunication companies, who exclude access to illegal content from the scope on their services, introducing filters for any service rendered.[32]

15.3 The Case of Egypt: The First Ever State Sponsored National Internet Blackout

In February 2011, authorities in riot-driven Egypt decided to take the state off the Internet—the last medium still available to their statesmen.[33] The blackout was achieved by applying the never before used practice of ordering all country-based ISPs to halt rendering their services.[34] This was the first ever case for a state to completely take its nation offline. Autocracies such as Cuba or North Korea scrupulously limit individual Internet access, be it through high price policy or formally restricting access to computers with an Internet connection, yet have never before decided to just switch off national critical Internet infrastructure. The reaction of the international community to the Egyptian precedent was also unique. Within a few days of the blackout, Google, a U.S.-based company,[35] offered its users located within Egypt the possibility to overcome the blocking enacted by

[31] See e.g.: Weckert (2000) at 105–111, who justifies the enactment of Internet filtering in Australia with those very arguments.

[32] One of the strongest proponents of Universal Internet filtering has been India, see e.g.: Agence France-Presse (2012).

[33] The same method was very likely used repeatedly a year later in Syria also entangled in internal turmoil. See e.g.: Coldewey (2013).

[34] According to Renesys, a company specializing in analyzing cyber espionage, Egyptian authorities probably ordered individual ISPs to disconnect all international Internet connections. Enforcing that decision did not however impact the international data flow to and from Egypt. Cowie 2011.

[35] Using a technology newly purchased from a start-up company SayNow, working together with Twitter, owned by a U.S.-based company: Obvious.

Egyptian law enforcement.[36] The solution used was a simple one, yet quickly brought about the intended aim: following a decision by the authorities, the ineffective blocking was ceased within 24 hours from introducing the ground-breaking Google service.[37]

This unprecedented incident clearly depicts the core of the problem with Internet filtering. The decision of Egyptian authorities to disallow any Internet access from state territory clearly was an interference with the individual freedom of speech. Google's reaction may be considered a first enactment of the 2010 "Clinton doctrine" for online freedom, aimed at states exercising online censorship as announced by Secretary Clinton in early 2010 during her engaging speech at the Newseum.[38]

This unprecedented practice provokes the question about the international law limits on free speech online, in particular the right to access information. International law's answer to questions on state responsibility for this particular limitations imposed on individual right to free speech are presented below.

15.4 State Immunity, State Sovereignty, and Limits of Individual Right to Free Speech Online

In order to answer the question on state responsibility for the infringement of individual human rights online, with particular attention paid to the right to access and share information, limited in early 2011 by Egyptian authorities a brief reference to the international law doctrine on state immunity ought to be made. This will allow us to classify a nation-wide Internet blackout as either sovereign state competence or a breach of an international obligation by that state bringing about its international responsibility. The contemporary understanding of state immunity reflects the limits of sovereign state power. It includes the distinction between *acta de iure imperii*—a term describing the exclusive, sovereign power of a state[39] and *acta de iure gestionis*—actions taken up by a state yet considered equal to those of private entities or individuals, since not restricted to sovereigns alone.[40] The latter include, for instance, engaging in private enterprises, taking on commercial endeavors, or entering so-called

[36] See e.g.: Doe 2011a, b.

[37] The system was based on using two particular international telephone numbers—information provided to those numbers was automatically, promptly published on Twitter with a keyword #Egypt. According to a Google representative, delivering information in this way did not require their authors to have Internet connectivity. Information so delivered was also available as audio under the very same telephone numbers or by accessing a devoted website: twitter.com/speak2tweet. See: Doe 2011a, b.

[38] Clinton 2010.

[39] Such as, primarily, enforcing legislative, executive or judicial jurisdiction, using treaty powers or the legation right.

[40] Performing, for instance; commercial activity. For the difficulties in assessing that divergence see e.g. the Libyan assets freeze case discussed in Rutzke 1988 at 241–282.

Bilateral Investment Treaties. In such cases, no state immunity is granted and a state may be held liable for any harm arising out of such activity, including civil litigation in foreign courts. On the other hand, the breach of state obligations falling into the *acta de iure imperii* category may lead to international responsibility of a state according to customary international law and the law of treaties, as described by the International Law Commission in its 2001 Draft Articles, yet may not be subject to the assessment of foreign national courts or other state organs.[41]

According to this distinction, the situation in Egypt clearly remains within the exclusive competence of a state, therefore represents an element of exercising state sovereignty. It may therefore be referred to in terms of a possible breach of international obligations laid upon Egypt at the time of the blackout, in particular its human rights obligations. Its legality may not however be assessed by national courts or other organs of another state. According to the UDHR or the ICCPR, state competence undoubtedly includes the right to restrict access to online content within state territory, yet international law introduces certain limitations on how and to what extend those restrictions are to be enforced.[42]

Assessment of the proportionality of that restriction and its compliance with international human rights norms, in particular the permissible limits of the right to access and impart information of Egyptian residents, remains a different issue. As already mentioned, the right to access information may be limited for particular reasons and in specific cases. A general ban on access to information ought to be assessed as the breach of Egypt's international obligations towards human rights protection, in particular those of the ICCPR, that Egypt is a party to. Article 19 ICCPR includes the above-mentioned requirement of proportionality that Egypt failed to meet. The derogative clause named in Article 4 ICCPR allows a state to "take measures derogating from their obligations under the Covenant (...) in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed". A state "availing itself of the right of derogation shall immediately inform the other States Parties to the present Covenant, through the intermediary of the Secretary-General of the United Nations, of the provisions from which it has derogated and of the reasons by which it was actuated". Egypt never met that requirement, therefore no justification for the restriction according to Article 4 ICCPR may be found. Such interpretation seems confirmed by a recent ECtHR decision in a similar case against Turkey discussed below.

[41] International Law Commission 2001 at 62.

[42] There is no doubt that state authorities were not deprived of their power at the time of the Internet blackout, therefore the fact of effectively disabling Internet access ought to be regarded as an act of legitimate state power being enforced. Separate is the issue of proportionality of the enforced limitation.

15.5 The Yıldırım Case

The assessment of the nation-wide Internet blackout as a breach of international obligation in the case of Egypt might follow the very same line of reasoning, justifying state's responsibility for the breach of its international obligation, as provided for by the ECtHR in the recent Yıldırım case.[43] A brief look at this groundbreaking case on Internet filtering shows a Turkish Internet user, Ahmet Yıldırım, who was deprived by Turkish authorities of the technical capability to share his ideas online through a personal website he had maintained within one of the numerous services offered in Turkey by Google: Google Sites. The restriction of access to all Google sites available in Turkey, including that run by the plaintiff, followed a court decision on content deemed illegal in Turkey, whose author could not be identified nor—consequentially—trialed. The regional court in Denizli issued an order directed at the national office for telecommunication (*Tur*.: Telekomünikasyon İletişim Başkanlığı, further herein: TİB) to disable access to all Google services in Turkey, claiming no other effective method of limiting access to the one website containing incriminating data was at hand. All of the almost 35 million Internet users in Turkey, that is nearly half of the Turkish population, lost access to all Google services offered in that country.[44] Their right to receive and impart information was infringed. This alleged violation of Article 10 ECHR was the basis for a successful claim by Mr. Yıldırım. The ECHR found that disallowing access to millions of websites because one of them contains information deemed illegal is a clear breach of the proportionality requirement included in the delimitative clause of Article 10 par. 2. Mr Yıldırım was awarded 7500 EUR as indemnification and 1000 EUR as costs reimbursement. The ECtHR clearly identified the proportionality prerequisite, present in Article 10 as one requiring a limitation enforced against individual in particular cases, where a nation-wide blocking of particular content did not meet that standard.

Should the same analysis be provided following the ICCPR standards and its fulfillment by Egypt in the case discussed, Egypt would also fail to meet the proportionality requirement as under no circumstances may disabling all Internet access be considered "proportional" or "case-specific" in terms of the HRC guidelines. Yet, one must keep in mind that the ICCPR regime offers no effective regime for enforcing its applicability, unlike the ECHR. While analyzing the international responsibility of Egypt, one must realize that any prosecution of that breach, not to mention enforceable international responsibility of the state is highly unlikely. Despite Egypt's participation in the ICCPR system and its obligation to impose any limitations solely within the rigid framework of HRC comments, the existing human rights violations assessment procedures give little hope for effective enforcement of free speech violations sanctions, even though the abovementioned

[43] European Court of Human Rights. 2012. Yıldırım v. Turkey.

[44] Miniwatts Marketing Group, World Internet Stats, http://www.internetworldstats.com/europa2.htm#tr (accessed Nov. 19, 2013).

UN HRC Resolution 12/16 on freedom of speech clearly disallows state parties to impose any limitations on the right to peaceful assembly and access to ICTs.[45]

All the procedures, the one on individual complaint[46] as well as the special ones created within the UN to protect human rights, are primarily initiated by the HRC, which is currently dominated by African and Muslim states, supported by China and Russia, who all represent a vision of free speech different from the one present in European or American legal systems.[47] The effectiveness of the Council's action has been strongly criticized over the years and even the introduction of a U.S. member, aimed at amending the unsatisfactory current situation proved futile.[48] In this context, chances to find international support and legitimization for sanctions against extensive Internet filtering in Egypt or elsewhere seem weak. Without such international authorization, any action aimed at limiting excessive exercise of state sovereignty over the access to online content remains contrary to the procedures adopted in international law. The controversial concept of humanitarian intervention, which claims legitimate the use of force by one or numerous states in defense of human rights violations victims may not be applied to violations of freedom of speech, freedom to communicate or freedom of assembly, since no peremptory norms safeguard those particular liberties, unlike in the case of e.g. genocide.[49]

The assessment presented above clearly shows that state imposed Internet blackout regarded as a restriction of access to any media may be recognized as a violation of international law, but lacks efficient international tools to counteract. The 2010 proclaimed U.S. Internet Freedom doctrine, aimed at helping victims of free speech violations worldwide, in particular in the Arab Spring entangled states, remains therefore a challenging piece of legal analysis discussed herein below.

15.6 The Clinton Doctrine and State Jurisdiction

On January 21, 2010, U.S. State Secretary Hilary Clinton declared war on Internet censors. Her speech, intentionally held at the free speech museum in Chicago, was acclaimed as the start of the Clinton Doctrine in foreign American politics. A term re-used to denote the relevance of the online human rights policy to President Clinton's commitment, in 1999, to protect ethnical minorities in Kosovo. The U.S. Secretary of State at the time of the Arab Spring proclaimed the White

[45] United Nations 2009.

[46] Egypt is not party to the First Optional Protocol introducing the individual complaint procedure.

[47] Evans 2008.

[48] See e.g.: Robertson (2006) at 1–40.

[49] See: e.g. Newman (2002) at 102–120. Such an intervention might be deemed legal should acts of genocide or war crimes be accompanied by the Internet blackout.

House intended to protect human rights abroad again, yet this time in a different setting and in another environment. The rights to be protected were also different: Clinton claimed U.S. aimed at protecting free speech, right of access to information, freedom of assembly and freedom of religion expressed online.[50] She clearly condemned China, North Korea, Egypt, Vietnam, Tunisia, Uzbekistan, and Saudi Arabia for the limits they impose within their territories on freedom of expression and flow of information online. She identified such practices as a clear violation of those states residents' right to access information. The analysis presented above confirms such assessment.

Clinton went a step further and—regardless of the existing, yet ineffective, UN human rights protection system—announced U.S. help for all residents of the states limiting access to information through Internet filtering in exercising the individual right to access information.[51] She announced U.S. plans to develop and deploy technology allowing to circumvent any state-imposed blocking. Clinton was the first state official to directly speak out against state-imposed Internet censorship. Until then, the tacit consensus among states was that online filtering remained within the exclusive competence of each state. It was a year after her Newseum speech that Clinton introduced the Internet Freedom program, which consisted of specific plans to help individuals deprived of their human right to freely access information.[52] The Internet Freedom program, even before it came to its fruition in Egypt, might have been critically assessed from international law's point of view. On behalf of one of the most powerful states in the world, Clinton announced she intended to support individuals residing in territories of foreign states in their breaching of local laws.

The initial question brought about by Clinton's statement is not new to international law disputes: it is the question of the hierarchy between human rights principles and state sovereignty. All that was new in this case was the fact that the human right in question was to be exercised online. Internet adds to this long-lasting dispute by including the question of limits of state power over critical elements of the network, including root servers or domain registries, the proper functioning of which is the necessary element of enabling free exercise of the right discussed herein. The question on permissible state interference in the daily operation of critical Internet infrastructure, as that operated by Egyptian ISPs, is a direct reflection of the question of limits of state interference with individual rights. The challenge with answering that question relates directly to the transnational character of the non-territorial cyberspace when confronted with the primarily territorial specific of exercising national jurisdiction.[53]

[50] Clinton 2010.

[51] For the definition of Internet filtering see e.g. Deibert (2008) at 15.

[52] Clinton 2011.

[53] For critical remarks of the implications of applying territorial jurisdiction over the cyberspace see: Kulesza (2012) at 1–30.

There is no doubt that any state action, which results online, regardless whether aimed at content—blocking access thereto or removing it, or at infrastructure-through a DDoS attack which disables certain hardware, brings about transboundary effects. An e-mail message that fails to reach its recipient (i.e. a U.S. resident) outside the jurisdiction of state where the sender is located (i.e. Egypt) limits the right to exchange information of both parties involved. Similarly, blocking the publication of information on current events in Egypt limits the right to access information of anyone outside Egyptian territory, including those in the U.S. One could raise the argument that such information, particularly if published in English, might have been targeted at those outside Egyptian territory. In this hypothetical situation, the U.S. would have the right or might even be considered obliged[54] to protect the right to access information of its residents, recalling the effective jurisdictional principle, since the harmful effects were present within its territory, where the recipients never gained access to information intended to reach them, or that of passive personal jurisdiction, allowing the state of the victim's nationality to exercise its powers. The U.S. would then be authorized to act in order to safeguard the right to access information of its residents, should that right be endangered following an act of law of a third party.[55] Such an interpretation of jurisdictional principles may bring unaccountable consequences, since any restriction on electronic content accessibility inherently holds unavoidable, global consequences on right to access information. The principles of effective or passive personal jurisdiction must therefore be applied with great caution. Content published online is simultaneously accessible everywhere where the Internet is, and the act of such content being removed deprives potential recipients of information contained therein of their right to access information.

The 2011 case of the U.S. citizen, Joe Gordon, sentenced in Bangkok to two and a half years in prison offers the perfect example of the threat engendered by applying effective jurisdiction to online activities, and in particular to free expression. Gordon posted links to the unauthorized biography of the Thai king while residing in the U.S.[56] and was considered by Thai authorities to have committed a *lese majeste* crime as per the Thai criminal code.[57] Upon his arrival to Bangkok for family holiday, this U.S. citizen was arrested, tried and sentenced to prison for the crime he committed online while in his U.S. home, yet the effects of which were felt in Thailand. The Thai courts applied effective jurisdiction, well recognized in international law. What is more, they have passed a new Computer Crimes Act that explicitly surrenders all insults to the monarchy committed online or through mobile phones to Thai jurisdiction. Its application to online activities creates a new threat to the rule of law. No one publishing online may any longer be certain

[54] See: European Court of Human Rights (2008).

[55] See: U.S. District Court for the Eastern District of Virginia, Alexandria Division (2010).

[56] Doe 2011b.

[57] Thai *lese majeste* laws mandate a jail term of 3–15 years for anyone who "defames, insults, or threatens the King, the Queen, the Heir-apparent, or the Regent." Thai National Administrative Reform Council (1956).

whether the content he or she uploads breaches the laws of a state where the Internet is accessible making him or her one of the Joe Gordon's of the Internet age. Applying effective jurisdiction to online activities unavoidably brings about an undesired chilling effect and deprives all authors of online content of any legal security. What is interesting about the original Joe Gordon case is the fact that the U.S., after having proclaimed their Internet freedom doctrine, chose not to intervene in any way in order to protect their citizen and his individual right to free speech online. Commentators justified this lack of reaction with the strong economic and political ties binding the two countries.[58]

As explained above the tacit consent granted by the White House to Google services in Egypt may hardly be justified by the human rights doctrine, yet may be considered contrary to the U.S. obligation to undertake any diligent action to prevent private interference with foreign sovereignty. According to the principle of due diligence, recognized in international law, the U.S. might be held internationally responsible for lack of due diligence of its authorities in preventing Google's interference with foreign states' sovereignty.[59] This aspect of the interrelationship between human rights and state sovereignty is discussed in more detail below.

15.7 "Internet Freedom" vs. State Responsibility

Both Clinton's declarations discussed above are material sources of international law. They constitute unilateral acts of state.[60] It is also clear that such acts have no direct effect on national laws and jurisprudence. They bring no obligation of U.S. individuals or companies to prevent any online censorship. Such an obligation, in order to be effective, would need to be enshrined within a national act of law. It would also be difficult to show that the particular actions taken on by Google in Egypt were the direct result of any U.S. official policy, less the Clinton statements. Neither of those statements includes a direct authorization for any entity to act on behalf of the U.S. and should they even include one, as already mentioned, such declarations are not a source of national U.S. law. The U.S. therefore holds no direct responsibility for the actions of Google in Egypt. Google did not act on behalf of or following an authorization of the U.S. authorities. Yet this does not mean that the U.S. may not be considered liable for the effects of Google's actions.

Legitimate decisions of Egyptian authorities require the respect of other states, which is a direct consequence of the principle of sovereign equality, fundamental to any international law regulation or practice. The principle of state sovereignty and the obligation of other states to respect it is usually derived from Article 2 par. 4 and

[58] Associated Press 2011.

[59] Pisillo-Mazzeschi 1992 at 9–51.

[60] International Law Commission 2006.

confirmed by par. 7 of the very same article in the United Nations Charter (UNC).[61] As rightfully pointed out by R. Vark, the obligation to respect other states' sovereignty includes an obligation to prevent potentially damaging acts originated within state territory. This duty of prevention also includes the obligation to cooperate with potential victim states in any way necessary to eliminate the harmful effects of the interference.[62] This obligation means that even when a state is not able to effectively protect the rightful interests of another sovereign state it may not passively allow for private parties to use its territory or other resources within its jurisdiction to interfere with those interests. This principle of due diligence in preventing the harmful use of state resources has been confirmed by rich jurisprudence, with the leading Teheran hostages case.[63] In its decision, the ICJ confirmed Iran's responsibility for the inaction of its authorities aimed at preventing harm to U.S. interests represented through its diplomatic mission in Teheran, which was raided upon by individual, private Iranians protesting against the U.S. interference in the region. The ICJ confirmed, that even though those actions of the individuals may not be directly attributed to the state, the latter is nevertheless responsible for the lack of preventive actions on the side of its authorities contractually obliged to actively protect the diplomatic mission in Teheran. As the ICJ explained, the fact that the acts of the militants may not be directly attributed to Iranian authorities "does not mean that Iran is, in consequence, free from any responsibility in regard to those attacks, for its own conduct was in conflict with its international obligations. (. . .) Iran was placed under the (. . .) obligations (. . .) to take appropriate steps to ensure protection" of U.S. diplomats and their mission.[64] The ICJ confirmed, that Iran "failed to take appropriate steps" to protect U.S. personnel and that "the total inaction" of Iranian authorities was contrary to its international obligations.[65]

The court identified the duty of a state to act with due diligence when fulfilling its international obligations with the possibility to attribute to it harmful consequences of private individuals' actions, should those follow the lack of due diligence on behalf of state organs.[66] Enabling state territory for individuals or entities attempting to cause harm in other jurisdictions may be identified as an internationally wrongful act and give grounds to state responsibility for the lack of due diligence on behalf of state authorities in preventing such transboundary damage.[67] This conclusion is justified by the contents of Article 14 par. 3 of the 1992 ILC's

[61] United Nations 1945.

[62] Vark 2006 at 192.

[63] International Court of Justice 1980 at 3.

[64] International Court of Justice 1980 at 31.

[65] International Court of Justice 1980 at 32.

[66] Bratspies and Miller 2006 at 233, who conclude that the existence of such a preventive obligation allows attributing to the state the very actions of private individuals. The ILC doctrine on transboundary harm emphasizes however that it is the lack of action of state authorities in preventing harmful events rather than the actions themselves which give ground for state responsibility.

[67] International Law Commission 2001 at 62.

Draft Articles on state responsibility, as according to its leading editor, the Committees Special Rapporteur on state responsibility J. Crawford, the rules defined within the draft relate also to "the breach of obligation to prevent a given event".[68] An obligation to prevent a given effect is usually defined as a best efforts obligation, requiring states to undertake any reasonable or necessary means in order to prevent a given effect, however without the guarantee that such an event will not take place. The standard of due diligence in set for each individual case, depending on its circumstances.[69] According to the UN Special Rapporteur on transboundary harm issues, P. S. Rao, "a breach of the due diligence obligation could be presumed" also "when a State had intentionally or negligently caused the event which had to be prevented or had intentionally or negligently not prevented others in its territory from causing that event or had abstained from abating it."[70] A state may therefore be considered responsible for the consequences of not introducing appropriate legislation, not executing national laws, or not preventing illegal activities within its jurisdiction or control.[71] The breach of a due diligence obligation also occurs when state authorities knew or should have known, regarding the circumstances, that a particular activity may result in transboundary harm.[72]

The U.S. government was aware of the action undertaken by Google that was aimed at making ineffective the procedures introduced by the legitimate Egyptian authorities,[73] yet took no action to prevent Google's plans. The due diligence obligation derived from Article 2 par. 4 UNC would require the U.S. authorities to make the company cease rendering the service effectively harmful to Egyptian internal policy. This conclusion, implied by the current international law jurisprudence, seems unsatisfactory to those seeking effective tools for preventing human rights violations online. A more optimistic answer may be proposed when reexamining the notion of state sovereignty, referred to above.

15.8 State Sovereignty in Cyberspace

In so far as extensive content filtering exercised by states like Egypt or China is considered undemocratic in Europe or America, international law foresees for no effective tools to prevent it. What is more, the existing catalogue of peremptory

[68] International Law Commission 1992.

[69] Brownlie 1983 at 45 names as criteria for attributing state responsibility the causal link between the negligence of a state authority and a breach of international law.

[70] United Nations 1999 at 8.

[71] United Nations 1999 at 8.

[72] United Nations 1999 at 8 where the issue of responsibility for transboundary damage in international watercourses is discussed.

[73] Google's service was so successful that the very next day after its employment Egypt re-enabled Internet access throughout the country.

norms clearly confirms that any state willingly or even negligently enabling its territory to infringe other state's sovereignty is in breach of its international obligations and may be subject to international responsibility. It requires other states to respect the sovereign decisions of state authorities, unless the UN Security Council finds them contrary to international law and allows for an intervention in the internal affairs of a state.[74]

This state of affairs seems undesired for two reasons named above. Any state activity regarding online content brings instantaneous and unavoidable transboundary effect wherever the Internet is accessible. Regarding the lack of effective international solutions to this undesired transboundary effect, every state whose residents have been harmed by such national decisions limiting access to online content, could individually address the breach based on its effective or passive personal jurisdiction. For this particular reason—the unavoidable interdependence between local and transboundary effect of Internet filtering—the international community is forever more strongly addressing states' obligation to refrain from interference with online content.[75]

Defining the limits of free speech has always been strongly rooted in culture and since its very recognition was identified within states' exclusive competence, unless states were willing to share it within a treaty regime or an international organization based upon such a treaty. The universal character of the global network that allows for instantaneous global communications seems to require a change in this contemporary paradigm. A universal standard for free speech online seems a necessary condition for preserving the unique global information network and saving it from fragmentation. What is being defined as *public service value of the Internet*[76] or the recognition of Internet access as a civil right within national legal regimes[77] justifies such a demand. At the same time, a proposed international obligation to freely provide access to online content is being narrowly defined—it refers solely to the obligation to ensure transboundary data flow.[78]

At a time of ever-growing globalization and when one-third of world's population is online,[79] it is necessary to stimulate the debate on fundamental values that

[74] As already mentioned, the idea of humanitarian intervention remains controversial and therefore still may not be accounted for as one of the universally recognized international law concepts, primarily due to the lacking uniform and universal *opinio iuris*. See supra 45 above.

[75] See e.g.: Council of Europe (2003) or Council of Europe (2011a, b, c).

[76] See e.g.: Council of Europe (2007).

[77] Internet access is recognized as a fundamental right in Finland or Lithuania.

[78] What is meant here would be a situation where blocking the free flow of information online in one state causes significant limitations to Internet access in another jurisdiction, which uses the filtering states' infrastructure. An example of the 2008 conflict between Russia and Georgia may be named. Georgian electronic infrastructure was blocked, which was followed by Armenia losing any Internet connectivity, as it was solely dependent on the Fibre Optical Cable System Trans Asia Europe, running through Georgia. See: Council of Europe (2009) at 22.

[79] According to Miniwatts Marketing Group, specializing in Internet statistics, 34.3 % of world's population had Internet access by the end of 2012; see: http://www.internetworldstats.com/stats.htm. Accessed 23 May 2013.

should be protected online and the ways and means in which to protect them.[80] In the course of that debate, the particular character of the medium discussed must be of major consideration. Regarding the architecture and governance structure of the network it seems a modification of the traditional notion of sovereignty is necessary due to the increasing need for enhanced human rights protection online.[81]

It is for those reasons that some authors propose the idea of *cooperative sovereignty,*[82] derived from the concept of treaty-based shared sovereignty, recognized, for instance, within the European Union, as an alternative to the existing derivative of the Westphalian order, fundamental to the current geopolitics.[83] This proposal seems well fitted with the unique principle of multistakeholderism in Internet governance.[84] According to this principle, Internet governance is executed jointly, although "in their respective roles" by three stakeholder groups and any effective consensus requires their cooperation.[85] Next to states, the stakeholder groups include business and civil society, with the latter covering NGOs, academia and individual users.[86] Following the multistakeholder principle decisions on the accessibility of online content, as any other on the issue of Internet governance, ought to be made by consensus of representatives of the three stakeholder groups. Unlike in international relations known thus far, it is no longer the states that hold the decisive voice in determining the future of this unique medium that is the Internet.

This interesting concept so far remains largely in the dogmatic sphere. It seems yet distant from becoming binding international law, as that would require either its recognition within an international treaty, adopted by states, yet open to other stakeholders[87] or a uniform customary practice of states supported by an *opinio iuris*. Both solutions would require time for their development and do not guarantee the current flexibility of governance, necessary for the quickly evolving nature of the cyberspace as its subject matter. Those shortcomings require for at least a temporary resolution to international soft law mechanisms,[88] yet the cooperative sovereignty proposal is worth remembering. As already mentioned the transboundary character of cyberspace, creating a direct threat to national rule of law and legal security of state nationals calls for the reconsideration of the notion of sovereignty. The *cooperative sovereignty concept* is based on the presumption that

[80] See: Council of Europe (2011a, b, c).

[81] See generally: Kreijen (2002).

[82] See e.g.: Weber (2010) at 19, Perrez (2000) at 264 f. proposing the general duty to cooperate as a principle of international law.

[83] See: Krasner (2004) at 19 ff.

[84] Weber 2010 at 14.

[85] See: United Nations (2005) at 4.

[86] See: Kleinwächter (2005) at 79.

[87] See: Kulesza (2012) at 152–155 where the author presents the concept of an Internet framework convention.

[88] See: Council of Europe (2010).

it is possible to identify shared values undermining different interpretations of sovereignty, which will then allow for the identification of universally accepted, fundamental values. Cooperative sovereignty could then stimulate any further discussion on the possible compromise on sharing state powers.[89] Such a compromise would need to envisage the sovereignty-based state prerogatives with obligations laid upon states according to international law, in particular human rights law. Weber suggests that states share a joint, international obligation to create and implement policies focused on human rights protection.[90] Perez identifies the cooperative sovereignty with the international obligation to cooperate as one of the principles of international law.[91] It is in that context that the need to identify and implement a universal standard for protecting free speech online should be understood. Achieving such a compromise seems possible in the light not only of the rapid development of human rights law in the last 60 years, but particularly in the recent U.N. Human Rights Council's First Resolution on Internet Free Speech—a soft law document, symptomatic for the increasing interest of the UN in international Internet law issues.[92] The Council calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries.[93] A hard-law follow-up remains to be expected.

References

Agence France-Presse. (2012). India defends internet censorship. *The Jakarta Globe*, August 24. http://www.thejakartaglobe.com/archive/india-defends-internet-censorship/. Accessed 23 May 2013.

Associated Press. (2011). American sentenced to prison for Thai royal insult. *3 News*, December 8. http://www.3news.co.nz/American-sentenced-to-prison-for-Thai-royal-insult/tabid/417/articleID/235841/Default.aspx. Accessed 23 May 2013.

Bratspies, R. M., & Miller, R. A. (Eds.). (2006). *Transboundary harm in international law: lessons from the Trail Smelter arbitration*. Cambridge: Cambridge University Press.

Brownlie, I. (1983). *System of the law of nations, part I: State responsibility*. Oxford: Oxford University Press.

Chilling Effects Clearinghouse. (2013). The chilling effects clearinghouse homepage. http://www.chillingeffects.org/

Clinton, H.R. (2010). Remarks on internet freedom. http://www.state.gov/secretary/rm/2010/01/135519.htm. Accessed 23 May 2013.

Clinton, H.R. (2011). Internet rights and wrongs: Choices & challenges in a networked world, remarks. http://www.state.gov/secretary/rm/2011/02/156619.htm. Accessed 23 May 2013.

[89] Weber 2010 at 14.

[90] Weber 2010 at 16.

[91] Perrez 2000 at 264 ff.

[92] Human Rights Council 2012. On international Internet law, its genesis and principles see generally: Kulesza (2012), 130 ff.

[93] Human Rights Council 2012 at 2.

Coldewey, D. (2013). Syria goes dark again in widespread Internet blackout. *NBC News*, May 7. http://www.nbcnews.com/technology/syria-goes-dark-again-widespread-internet-blackout-6C9830083. Accessed 23 May 2013.
Council of Europe. (1950). Convention for the protection of human rights and fundamental freedoms as amended by protocols No. 11 and No. 14. Council of Europe Treaty Series No. 194.
Council of Europe. (2003). Declaration of the committee of ministers on freedom of communication on the Internet.
Council of Europe. (2007). Recommendation of the committee of ministers to member states on measures to promote the public service value of the Internet.
Council of Europe. (2009). Internet governance and critical internet resources.
Council of Europe. (2010). International and multi-stakeholder co-operation on cross-border Internet. Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international. http://www.coe.int/t/dghl/standardsetting/media/mc–s–ci/default_EN.asp. Accessed 23 May 2013.
Council of Europe. (2011a). Declaration by the committee of ministers on internet governance principles.
Council of Europe. (2011b). Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings.
Council of Europe. (2011c). Recommendation of the committee of ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet.
Cowie, J. (2011). Egypt leaves the internet. *Rensys*, January 27. http://www.renesys.com/blog/2011/01/egypt–leaves–the–internet.shtml. Accessed 23 May 2013.
Deibert, R. (Ed.). (2008). *Access denied: the practice and policy of global Internet filtering*. Massachusetts: MIT Press.
Deibert, R., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Massachusetts: MIT Press.
Doe, J. (2004). A starting point: Legal implications of internet filtering. OpenNet Initiative. https://opennet.net/docs/Legal_Implications.pdf. Accessed 23 May 2013.
Doe, J. (2004). Cisco announces IP next-generation network advancements for service providers. http://newsroom.cisco.com/dlls/2004/prod_120604.html. Accessed 23 May 2013.
Doe, J. (2008). Italy cracks down on Pirate Bay. *New York Times*, August 14. http://www.nytimes.com/2008/08/14/technology/14iht–webpirate.15301147.html. Accessed 23 May 2013.
Doe, J. (2011a). Egypt crisis: Google launches 'speak to tweet' service. *The Telegraph*, February 1. http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8295219/Egypt-crisis-Google-launches-speak-to-tweet-service.html. Accessed 23 May 2013.
Doe, J. (2011b). Thailand jails US man Joe Gordon for royal insult. *BBC online*, December 8. http://www.bbc.co.uk/news/world-asia-16081337. Accessed 23 May 2013.
European Court of Human Rights. (2001). VgT Verein Gegen Tierfabriken v. Switzerland. Case number 24699/94.
European Court of Human Rights. (2008). Khurshid Mustafa And Tarzibachi v. Sweden. Case number 23883/06.
European Court of Human Rights. (2012). Yıldırım v. Turkey. Case number 3111/10.
European Court of Human Rights. (2013). Delfi v. Estonia. Case number 64569/09.
European Court of Justice. (2010). Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Case number C-70/10.
Evans, R. (2008). U.N. chief tells rights body drop rhetoric, blocs. *Reuters*, December 12. http://www.reuters.com/article/2008/12/12/us–un–rights–idUSTRE4BB67820081212. Accessed 23 May 2013.
Human Rights Council. (2012). The promotion, protection and enjoyment of human rights on the Internet. U.N. Doc. A/HRC/20/L.13.

International Court of Justice. (1980). United States Diplomatic and Consular Staff in Tehran.
International Law Commission. (1992). Draft articles on state responsibility: Titles and texts of articles adopted by the drafting committee. U.N. Doc. A/CN.4/L.472.
International Law Commission. (2001). Draft articles on responsibility of states for internationally wrongful acts, with commentaries. U.N. Doc A/56/10.
International Law Commission. (2006). Guiding principles with commentaries applicable to unilateral declarations of states capable of creating legal obligations. U.N. Doc. 61/10.
Kleinwächter, W. (2005). Multistakeholderism and the IGF: Laboratory, clearinghouse, watchdog. In W. J. Drake (Ed.), *Reforming Internet governance: perspectives from the Working Group on Internet Governance (WGIG)* (pp. 535–582). New York, NY: UN Publishing.
Krasner, S. D. (2004). The hole in the whole: Sovereignty, shared sovereignty, and international law. *Michigan Journal of International Law, 25*(4), 1075–1101.
Kreijen, G. (2002). *State, sovereignty, and international governance*. Oxford: Oxford University Press.
Kulesza, J. (2012). *International internet law*. London: Routledge.
McNamee, J. (2013). MEPs propose web blocking yet again, Digital Civil Rights in Europe. *EDRigram newsletter*, April 24. http://www.edri.org/edrigram/number11.8/web-blocking-gambling-again. Accessed 23 May 2013.
Newman, E. (2002). Humanitarian intervention, legality and legitimacy. *International Journal of Human Rights, 6*(4), 102–120.
Noman, H., York J.C. (2011). West censoring east: The use of western technologies by middle east censors, OpenNet Inititive. http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011. Accessed 23 May 2013.
Open Net Initiatve. (2013). Open net initiative homepage. https://opennet.net/. Accessed 23 May 2013.
Perrez, F. X. (2000). *Cooperative sovereignty*. The Hague: Kluwer Law International.
Pisillo-Mazzeschi, R. (1992). The due diligence rule and the nature of international responsibility of states. *German Yearbook of International Law, 35*, 9–51.
Privacy International, GreenNet Educational Trust (2003). Silenced, an international report on censorship and control of the internet. http://www.docstoc.com/docs/147504632/Silenced—an-international-report-on-censorship-and-control-of-the-internet. Accessed 23 May 2013.
Reporters Without Borders. (2013). The list of Internet enemies. http://en.rsf.org/internet.html. Accessed 23 May 2013.
Robertson, G. (2006). *Crimes against humanity*. New York, NY: The New Press.
Rutzke, C. R. (1988). The Libyan asset freeze and its application to foreign government deposits in overseas branches of United States banks: Libyan Arab Foreign Bank v Bankers Trust Co. *American University International Law Review, 3*(1), 241–282.
Sadurski, W. (2002). *Freedom of speech and its limits*. Dordrecht: Kluwer Academic Publishers.
Thai National Administrative Reform Council. (1956). Order (No. 41) Full text available in English at: http://thailaws.com/law/t_laws/tlaw50001.pdf. Accessed 23 May 2013.
U.S. District Court for the Eastern District of Virginia, Alexandria Division. (2010). Microsoft Corporation v. John Does 1—27, case number 1_10CV156 (LMBIJFA).
United Nations. (1945). United Nations Charter.
United Nations. (1948). Universal declaration of human rights. U.N. Doc. A/RES/(III).
United Nations. (1966). International covenant on civil and political rights. U.N. Doc. A/6316.
United Nations. (1999). Second report on international liability for injurious consequences arising out of acts not prohibited by international law by Mr. P.S. Rao, Special Rapporteur, U.N. Doc A/CN.4/501.
United Nations. (2005). Report of the Working Group on Internet Governance. www.wgig.org/docs/WGIGREPORT.pdf. Accessed 23 May 2013.
United Nations. (2009). Resolution adopted by the human rights council, freedom of opinion and expression. Un. Doc. A/HRC/RES/12/16.

Vark, R. (2006). State responsibility for private armed groups in the context of terrorism. *Juridica International, 11*, 184–193.

Weber, R. H. (2010). New sovereignty concepts in the age of internet. *Journal of Internet Law, 8*, 12–20.

Weckert, J. (2000). What is so bad about internet content regulation? *Ethics and Information Technology, 2*(2), 105–111.

Yutaka Arai, Y. (2002). *The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR*. Antwerp: Intersentia.