Human Rights in the Information Society

Spring 2011, markus.sabadello@gmail.com

"I am what I am because of who we all are."

Translation of the term “Ubuntu”, which is both an African philosophy
encompassing the essence of the “Golden Rule” of Human Rights,
and the name of a successful Open Source operating system.

Contents

1. Introduction

In today's globalized Information Society – enabled to a large part through the widespread availability of Information and Communication Technologies (ICTs) such as mobile phones and the Internet – we are experiencing a multitude of fast and transformative developments within societies, cultures and economies, enabled by new ways in which individuals interact with each other. And whenever there is interaction between individuals, Human Rights should provide the framework and the supreme set of guiding ideas, always affirming the equal dignity and value of all human beings, and telling us what should be done and what should not be done. In an environment as dynamic and interconnected as the Internet, such guiding ideas are especially important. Much has been said about the potential threats and opportunities of modern communication technologies, and about whether they provide a liberating potential at the human level, or whether they constitute yet another mechanism for reinforcing old structures and for transferring wealth from the poor to the rich. In light of such discourses and in the best tradition of the "Golden Rule" of Human Rights, we must lay out a system of freedoms and obligations for a prosperous and just Information Society, in which we all do (not) to others what we (do not) want others to do to us.

This paper is an attempt to identify those Human Rights that apply to various aspects of ICTs and the Information Society they enable, as well as to analyze in which ways states should respect, protect and fulfill those rights. And as always when applying Human Rights to practical situations, one important objective must also be to balance any individual's rights with the rights of others, and to evaluate limits and restrictions wherever necessary.

I will use and refer to the following important Human Rights related documents throughout this paper:

- The *Universal Declaration of Human Rights* (UDHR)
- The *International Covenant on Civil and Political Rights* (ICCPR)
- The *International Covenant on Economic, Social and Cultural Rights* (ICESCR)
- The *Convention on the Rights of People with Disabilities* (CRPD)
- The *European Convention on Human Rights* (ECHR)
- The *Charter of Fundamental Rights of the European Union* (CFREU)
- The *Human Rights Handbook for Parliamentarians* (HRHP)

Other important sources for this endeavor include some nations' domestic laws, the guidelines of regional organizations, as well as the set of outcome documents of the World Summit on the Information Society[1], which culminated in its second phase in 2005 in Tunis, where the United Nations as well as a large amount of other stakeholders worked on evaluating the opportunities and risks of the now ubiquitous Information Society. The *Tunis Commitment* and the *Tunis Agenda* both explicitly refer to the UDHR and provide statements about the concrete application of Human Rights to the Information Society.

In this paper, I will look at three broad and interrelated areas where Information and Communication Technologies and Human Rights meet: The availability of ICTs, the right to freedom of expression and the right to privacy. Finally, I will also look at and discuss certain forms of discrimination that might occur in the online world.

[1] See http://www.itu.int/wsis/

2. Balancing Considerations

Human Rights are not absolute. They are guiding ideas that must be applied to individual cases as appropriate. In some cases, they can be limited and derogated, especially in situations where one Human Right appears to contradict another, or when the upholding of one individual's rights threatens to violate those of another individual.

Such balancing considerations often revolve around a tradeoff between the desirable goals of security and freedom, in other words, around the question to what extent a state should establish rules that confine individual liberties. Sometimes, such "allowed" limitations are explicitly mentioned in Human Rights documents. Other times, they must be identified and evaluated by a concrete situation a hand.

The UDHR in its Article 29.2 summarizes this need for balancing and potentially limiting individual rights:

> *"In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."*

Sometimes, universal Human Rights documents, regional guidelines and national legislation may turn out to be in conflict with each other. The Global Network Initiative[2] – a coalition of ICT companies, civil society organizations, investors and academics – dedicates itself to "protecting and advancing freedom of expression and privacy in Information and Communications Technologies", and states that

> *"All over the world – from the Americas to Europe to the Middle East to Africa and Asia – ICT companies face increasing government pressure to comply with domestic laws and policies in ways that may conflict with the internationally recognized human rights of freedom of expression and privacy."*

[2] See http://www.globalnetworkinitiative.org/

3. Availability of ICTs

The ability for individuals to access information through the use of ICTs is the most fundamental prerequisite for participating in the Information Society. This includes the availability of technical infrastructure as well as the education and knowledge of how to effectively use it. While the ability to access and use communication technologies is certainly not as essential as other basic rights and needs such as water, shelter or physical security, it is still a key requirement for participating in today's highly interconnected world and should therefore be considered a Human Right.

One big obstacle on the road toward the goal of universal availability is the phenomenon known as the Digital Divide (or Digital Gap), which refers to the current unequal distribution of Information and Communication Technologies. This applies both to unequal availability in different geographical regions and within societies. There are legitimate concerns that this phenomenon may actually increase the gap between rich and poor, which is in stark contrast to early hopes that technologies such as the Internet and mobile phones would lead to a fairer and more equal world. Therefore, in any attempt to use ICTs for building an inclusive Information Society based on Human Rights, bridging the Digital Divide must be a central objective.

One other concept that is closely related to basic availability of ICTs is that of accessibility (see section 6.2), which is concerned with discrimination and barriers to the practical use of ICTs even in situations where basic availability of the technical infrastructure is ensured.

3.1. Applicable Sources

Article 19.2 of the ICCPR mentions the

> *"… freedom to 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."*

While this article does not explicitly mention a right for availability to ICTs, it can be interpreted to imply such a right, given today's importance of these technologies.

One source that gets more concrete in this area is the *Human Rights Handbook for Parliamentarians*, which is a guideline for policy makers on how to apply Human Rights in practice. In its "Box 70" (*"Safeguarding freedom of the media"*), it mentions a set of important measures, including:

> *“Promoting universal access to the Internet.”*

The *Tunis Commitment* in its Article 9 affirms this same need in a similar manner:

> *“We reaffirm our resolution in the quest to ensure that everyone can benefit from the opportunities that ICTs can offer, by recalling that governments, as well as private sector, civil society and the United Nations and other international organizations, should work together to: improve access to information and communication infrastructure and technologies as well as to information and knowledge.”*

The *Tunis Agenda* in its Article 8 makes an explicit reference to the Digital Divide and gives a quick overview of possible high-level approaches for bridging it:

> *“We recognize the scale of the problem in bridging the digital divide, which will require adequate and sustainable investments in ICT infrastructure and services, and capacity building, and transfer of technology over many years to come.”*

Several other Articles make similar statements to underline the importance of universal availability of ICTs and bridging the Digital Divide, for example Articles 7, 10, 16, 17, 18, 19, 23, 26, 31 of the *Tunis Commitment* and Articles 7, 9, 13, 17, 28, 49, 53, 84, 87, 89, 113, 114, 119, 121 of the *Tunis Agenda*.

In addition to the sources mentioned above, when arguing for a basic right for access to information, one might even go as far as mentioning Article 1.1 of the ICESCR,

> *“All peoples have the right to … freely pursue their economic, social and cultural development.”*

Since in today’s world economic, social and cultural development is so heavily dependent on communication technologies, the above statement can potentially be interpreted to immediately imply a right for access to ICTs such as the Internet, even though technology is not explicitly mentioned in the article.

3.2. Balancing Considerations

The identification of the availability of ICTs as a Human Right does not mean that states actually have an obligation to directly provide their citizens with access to ICTs infrastructure. Rather, it is their obligation to guarantee a fruitful political and economic environment, where such infrastructure will evolve for the benefit of all its citizens.

Several states have however included an explicit right to access to the Internet in their domestic legislation, for example Spain guarantees their citizens the right to broadband Internet access at any location for a fixed price[3]. Similar rights also exist in Estonia, France, Finland and Greece.

[3] See (Morris, 2009)

4. Freedom of Expression

Another key topic to consider when looking at the intersection of ICTs and Human Rights is freedom of expression, which is directly related to the right to basic availability of ICT access. As a concept that has a long history in traditional media, the right to freedom of expression has gained new relevance with the widespread availability of the Internet.

In 1990, the U.S. Secret Service raided a company called Steve Jackson Games in Austin, Texas, based on suspicions about the illegal distribution of an electronic file[4]. During this operation, servers and other computer hardware were confiscated and only returned several months later. One of the servers was used to operate an electronic discussion forum where users could exchange messages with each other online. As it turned out in an ensuing court case, not only were claims for illegal activity of the company unjustified, but also did the Secret Service violate privacy laws by interfering with electronic communication of users of the affected server. This incident was one of the first to raise awareness for the need to apply and uphold Human Rights in the context of electronic communication networks. It has led to the creation of the Electronic Frontier Foundation[5], which up to today is active in defending individual civil liberties on the Internet.

Today, Internet services such as Facebook, Twitter and Youtube are playing important roles in popular movements such as the popular revolutionary movements in Iran, Tunisia, Egypt, Libya and others, where ICTs have been used both to organize the movements and for public dissemination of political messages. Therefore, these technologies can be considered an important cornerstone of a civil society aiming to counterbalance an overwhelmingly strong state authority and to contribute to a democratic society. It is obvious that for such activities to flourish, the guarantees for freedom of expression and non-interference by state authorities are important ingredients.

4.1. Applicable Sources

The UDHR in its Article 19 says:

> *"Everyone has the right to freedom of opinion and expression."*

[4] See http://www.sjgames.com/SS/ for a detailed description

[5] See http://www.eff.org/

This is further repeated and reaffirmed in the ICCPR, which in its Articles 19.1 and 19.2 says:

> *"Everyone shall have the right to hold opinions without interference."*
>
> *"Everyone shall have the right to freedom of expression."*

The ECHR makes a similar statement in its Article 10.1:

> *"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."*

The above statement is repeated word-by-word in the CFREU in its Article 11.1.

In Article 4 of the *Tunis Commitment*, this right is put into the context of ICTs:

> *"We recognize that freedom of expression and the free flow of information, ideas, and knowledge, are essential for the Information Society and beneficial to development."*

4.2. Balancing Considerations

While the right to freedom of expression is a fundamental Human Right that is equally valid in the context of ICTs as it is in more traditional media, sometimes this right – just like others – can be limited.

While in the ICCPR in its Articles 19.1 and 19.2 asserts the rights to freedom of opinion and expression without interference, Article 19.3 states reasons for possible exceptions:

> *"The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> *(a) For respect of the rights or reputations of others;*
>
> *(b) For the protection of national security or of public order (ordre public), or of public health or morals."*

The ECHR in a similar manner states the right to freedom of expression in its Article 10.1, while in its Article 10.2 describes possible limitations:

> *"The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."*

Some recent, concrete examples of situations, in which the right to freedom of expression has turned out to be in conflict with other goals, are the popular revolutionary movements in the Arab world, such as the Iranian Green Movement of 2009, the Tunisian "Jasmine" revolution of 2011, or the Egyptian revolution of 2011. In these movements, on one hand, ICTs such as the Internet and mobile phones were heavily used by the popular opposition to organize their movements and for political outreach[6]. On the other hand, the governments of the respective states undertook steps to try to limit the freedom of expression by various restrictive technical measures, such as censorship or the shutting down of Internet services altogether[7].

From a Human Rights perspective, the challenge is to balance the various interests, and to evaluate in each such case, whether restrictions are justified and which right is to take precedence over the other. Another interesting detail in this discussion is the fact that in light of governmental repression, some opposition actors found technological ways to circumvent restrictions, for example by using so-called proxy servers, ad-hoc networks or anonymizing peer-to-peer networks. Depending on one's Human Rights perspective, it could be argued that such actions may be covered by the UDHR's preamble, which states that

> *"Whereas it is essential, if man is not to be compelled to have recourse, as a last resort, to rebellion against tyranny and oppression."*

[6] See (Zuckerman, 2011) for a discussion on the role played by ICTs during the Arab popular movements

[7] For example, see (Kanalley, 2011)

5. Personal Data and Privacy

Just like freedom of expression, a right to the protection of personal data and privacy – the ability to selectively seclude information about oneself – is an old and broad concept that has gained a new, special relevance with the rise of ICTs. The key point is that when using the Internet or mobile phones, significant amounts of personal data are being stored and transmitted, often without our explicit consent or even knowledge.

This happens in ways and dimensions that are unparalleled in any other media or communication method. With every step we take on the Internet or on our mobile phone, every piece of information we type on the screen, every mouse click we perform on the web, we are adding more data to our online identity, our digital fingerprint. Based on this data, specialized methods and technologies can be applied which are aimed at extracting useful patterns from the data that individuals produce as they use online services. This process called data mining can be used either for the advantage or disadvantage of individuals. On the positive side, sophisticated programming based on our data can help us customize the services we use, provide for a better overall online experience and potentially even mitigate the challenges posed to us by Information Overload[8]. On the negative side, there is a vast amount of potential abuse by those companies in control of our data, which can range from direct monetization of our information by the means of targeted advertising, to the conscious and malicious manipulation of what we see and do online, leading to influence on our consumption behavior and political views.

The amount of data that is being collected and analyzed is typically much larger than the average individual would expect. The perceived freedom and user-centricity that seem to be inherent to the way we have been educated to use the Internet can all too easily hide the fact that between individuals and companies, there is almost always a huge imbalance of control over data in favor of the latter. An entire industry has emerged that has specialized in developing technologies for data collection and data mining. All of the largest and most popular Internet companies – such as Google, Facebook, Twitter and Youtube – are based on the idea of offering supposedly "free" services in exchange for collecting and monetizing valuable data about their users[9].

[8] Information Overload, first coined in (Toffler, 1970), refers to the problem that the too much information can lead to difficulties when trying to select and process the relevant from the useless.

[9] For a discussion on hidden costs behind seemingly "free" services, see (Krotoski, 2010)

In a hearing conducted by a subcommittee of the U.S. House of Representatives in 2010, Professor Eben Moglen of the Columbia University Law School stated that

"Facebook holds and controls more data about the daily lives and social interactions of half a billion people than 20th-century totalitarian governments ever managed to collect about the people they surveilled."

It should therefore be obvious that privacy as a Human Right deserves special attention in the context of ICTs. Strategies to introduce better privacy and data protection are possible both on the technological and legal side.

On the technological side, possible approaches include the use of cryptographic methods (such as digital signatures and encryption), as well as software architectures that are designed from the bottom up with the concept of user-centricity in mind, which refers to the realization that all control over one's identity and data should rest within the individuals. In a rousing speech, Professor Eben Moglen argues that the 4th Amendment in the United States implies a technology architecture that is not "in the cloud" but rather is within our homes, where an individual's protections against unreasonable search and seizure are strongest[10].

Various communities are working on such architectures, for example:

- "OpenID"[11] is an architecture and protocol for establishing a single, user-centric identity on the Internet, which can be used to authenticate to many different companies and organizations. With this technology, every time one's personal data is transferred, an individual has to give permission to approve this step.
- "Information Cards"[12] are based on the idea of owning a "digital wallet" on one's computer. This wallet contains digital cards, each of which represents a certain part or aspect of one's identity on the Internet. These cards as well as the personal data on them always remain under the control of the individual and can be selectively shared.
- The "Personal Data Ecosystem"[13] is a community working on so-called "Personal Data Store" technologies, which will allow individuals to fully control their personal information online from a single point, to selectively disclose as well as

[10] See http://www.youtube.com/watch?v=QOEMv0S8AcA

[11] See http://openid.net/

[12] See http://informationcard.net/

[13] See http://personaldataecosystem.org/

monitor the use of this personal information, to update and delete personal information, and to freely transfer their personal information from one company or organization to another.

5.1. Applicable Sources

Numerous references to privacy can be found in the relevant Human Rights documents.

The UDHR in its Article 12 says

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."*

This wording – explicitly mentioning "correspondence" – should be broad enough to cover many privacy risks in the context of ICTs, considering that for example E-Mails or messages within social network services are also a kind of correspondence.

The ICCPR in its Article 17 makes an almost equivalent statement to the one above:

> *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."*

In a similar way, the topic of privacy is also covered by the ECHR in its Article 8:

> *"Everyone has the right to respect for his private and family life, his home and his correspondence."*

The CFREU in its Article 7 repeats the previous statement in a more gender-neutral manner:

> *"Everyone has the right to respect for his or her private and family life, home and communications."*

However, the CFREU even goes one step farther by explicitly mentioning the "protection of personal data" and stating in its Articles 8.1 and 8.2:

> *"Everyone has the right to the protection of personal data concerning him or her.*
>
> *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."*

Many states have laws covering the topics of personal data and privacy. Also, some regional organizations provide relevant legislation or guidelines. Examples include:

- The *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data* of the Organisation for Economic Co-operation and Development (OECD)
- The *Privacy Framework* of the Asia-Pacific Economic Cooperation (APEC)
- The *Data Protection Directive (Directive 95/46/EC)* of the European Union
- The *Fair Information Practice Principles* of the United States Federal Trade Commission (FTC)

The key requirements that most national or regional approaches have in common are that collected personal data must be sufficiently secure and protected, that only the minimal amount of data which is relevant for a particular purpose should be collected, that personal data should only be collected, used and made available with the explicit knowledge and consent of the individual, and that individuals should have access to the personal data that is collected about them, including ways to complete, rectify or delete data which is incorrect.

It should be pointed out that because of cultural and historical differences, privacy legislation is sometimes not "compatible" between countries, which could hinder international commerce. For example, the *Data Protection Directive (Directive 95/46/EC)* of the European Union prohibits the transfer of personal data to countries such as the United States which do not meet the very strict European standard. To bridge such differences, frameworks such as the *U.S.-EU Safe Harbor* program[14] can be implemented.

One recent national initiative, which could become a standard for the future treatment of these sensitive issued in the context of ICTs, is a proposal made in the U.S. Senators John McCain and John Kerry are circulating proposed legislation to create an "online privacy bill of rights"[15]. The bill would require companies to ask a person's permission to share data about him or her with outsiders. It would also give people the right to see the data that companies collected on them.

[14] See http://export.gov/safeharbor/eu/eg_main_018365.asp

[15] See (Bentley, 2011)

5.2. Balancing Considerations

Just like in the case of freedom of expression and other Human Rights, the right to privacy must sometimes also be balanced, evaluated and possibly restricted for the purpose of protecting other rights. In the field of law enforcement, conflicts between the right to privacy and the requirements during the investigation of a crime are commonplace. For example, in many states the police may not arbitrarily search a person's house, but may do so in cases where there is a reasonable suspicion that the person is involved in a crime.

In the context of ICTs, many kinds of criminal activities exist, for example the distribution of spam, the unauthorized breaking into computer system, the distribution of illegal material such as extremist propaganda or child pornography, or identity theft. To counter such activities, state authorities typically have various means at their disposal, for example the surveillance of an individual's electronic communication.

One recent, controversial initiative aimed at restricting the right to privacy for the purpose of law enforcement is the *Data Retention Directive (Directive 2006/24/EC)* of the European Union, which requires member states to store sensitive telecommunications data for a period of six to twenty-four months. The key element from a Human Rights perspective is that such storage takes places on a precautionary principle, without any concrete suspicion against individuals. However, for actually accessing the data, a good reason and a court order will be required.

The discussions as well as various legal proceedings around this directive are ongoing. While some states such as France, the United Kingdom and Hungary have implemented it, others such as Sweden and Austria have not. Yet others, such as Germany, Romania and the Czech Republic, have begun implementing it, until it was stopped. For example, in Romania the constitutional court has declared the directive to be in violation with the ECHR[16].

[16] See (Heise Online, 2009)

6. Discrimination on the Internet

The term discrimination refers to the exclusion or rejection of individuals or a group of individuals from opportunities, based solely on grounds such as race, color, sex, language, religion, national or social origin, property, ethnicity, sexual orientation, age or disabilities[17]. As ICTs reach into all parts of our everyday lives and we are becoming more and more dependent on their use, a multitude of examples of discrimination can also be observed when it comes to the development and use of ICTs.

It is important to point out that situations of unequal treatment with good reasons may not necessarily constitute discrimination. Just like when applying Human Rights to concrete cases, evaluating potential cases of discrimination also requires careful balancing considerations. If there are legitimate, objective grounds, then unequal treatment may be justified rather than constitute a discriminatory act.

6.1. Net Neutrality

The term net neutrality refers to the desired practice of treating all forms of transmission over the Internet equally. In contrast to other communication networks such as land-based telephone systems, the Internet's lower technical layers work on a "connectionless packet switching" basis, which means that not every single piece of information is treated in the same way. Therefore, sometimes trade-offs can be made with regard to what transmissions should be allowed or denied, or preferred over others. If certain kinds of transmissions are treated differently from others in a systematic way, a violation of net neutrality is taking place. This can be engineered based on a transmission's contents (e.g. the text in an e-mail) or based on its "metadata" (e.g. the sender's and receiver's addresses, or the kind of application initiating the transmission). Concrete examples of the violation of net neutrality include the selective censoring of content or the artificial slowing down of certain applications such as Skype conversations or music downloads.

In some cases, the unequal treatment of transmissions is not considered a violation of net neutrality. For example, certain data that is known to be clearly harmful to the technical infrastructure – such as viruses, spam or denial-of-service attacks – may be blocked by firewalls. Another example is the application of "quality of service" strategies,

[17] Exact definitions of discrimination vary between Human Rights documents, for example the element of "age" is included in the CFREU, but not in the ICCPR.

which aim at preferring certain applications over others with the goal not being the discrimination of some transmissions, but rather the overall optimization of certain technical parameters such as throughput and latency.

In protecting or violating net neutrality, Internet Service Providers (ISPs) play a crucial role. It is their position in the global Internet infrastructure that allows them to influence transmissions between individuals. In the past, ISPs have sometimes been found to discriminate against certain kinds of transmissions[18].

One special kind of violation of net neutrality is the selective filtering of access to ICT services based on the origin of the request for access. Again due to the technical infrastructure of the Internet, it is possible for any provider of content or services to identify and discriminate against the nationality of individuals. A well-known example for this is the so-called "Nigerian Blocklist"[19], which has become a popular tool among system administrators of web and e-mail servers. While the application of this tool effectively prevents (perceived high numbers of) malicious attacks from Nigerian criminals, it also rules out access for every legitimate access coming from Nigeria. Similar tools also exist for preventing access from other countries such as Russia or China, or even for entire continents such as South America.

From a Human Rights perspective, one must ask whether such techniques are legitimate. On one hand, it can be argued that discrimination is clearly taking place, because a large group of individuals is excluded from opportunities based solely on their nationality. On the other hand, it can be argued that for technical reasons such "blocklists" are the only possible way (with a reasonable amount of effort) to protect ICT systems from large-scale, malicious attacks, which could potentially render such systems damaged altogether.

6.2. Accessibility

The term accessibility describes the degree by which products, services or activities are available for use by all people, irrespective of any disabilities or special needs. Limited accessibility reduces opportunities for affected people. Accessibility is thus a desirable goal in order to avoid discrimination against people with disabilities or special needs.

[18] For example, see (Svensson, 2007)

[19] See http://www.wizcrafts.net/nigerian-blocklist.html

This concept is closely linked to the basic availability of ICTs (see section 3). However, even in situations where ICT infrastructure is available, full accessibility for everyone is not necessarily guaranteed.

Article 9 of the CRPD lays out the right to accessibility and makes specific references to ICTs:

> *"State Parties shall also take appropriate measures to:*
>
> *g. Promote access for persons with disabilities to new information and communications technologies and systems, including the Internet;*
>
> *h. Promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, so that these technologies and systems become accessible at minimum cost."*

The means to achieve accessibility for ICTs vary depending on the exact situation and a person's needs:

- Sometimes, simple configuration settings in a computer's operating system can improve accessibility. Examples include the abilities to magnify a portion of the screen to improve readability, to avoid having to press more than one key at the time, or to have the computer read out text that is written on the screen.
- Sometimes, a computer system can be extended by installing so-called "assistive technologies" (hardware or software). Examples include voice recognition systems or specially manufactured keyboards that allow for easier input.
- Sometimes, rules and best practice guidelines can help to improve accessibility.

The last item in this list is especially important on the Internet. The freedom of audio-visual design and the existing multitude of different and fast evolving technologies can on one hand support a diverse and flourishing ecosystem of content and creativity, but on the other hand it can also make it difficult to read e-mails, to search for information, and to understand and navigate on complex websites. To counteract such difficulties, the World Wide Web Consortium (W3C) has published the *Web Content Accessibility Guidelines*[20], which contain advice for developers on how to make content on the Internet accessible for all people.

[20] See (World Wide Web Consortium (W3C), 1999)

7. Conclusions

The introduction of new technologies has always been a central element in human progress, up to today's world in which many aspects of our lives depend on modern communication. It is obvious that in our globalized and interconnected world, the availability and use of ICTs are a big source of both opportunity and risk. Modern Information and Communication Technologies have often been described as "neutral tools", which can be used for either good or evil. Therefore they also offer great potential for development and can lead to growth and more overall human comfort in disadvantaged regions or parts of societies.

Much of my work in this paper is based on the outcome documents of the World Summit on the Information Society. During the opening ceremony of its Tunis conference, the then Secretary General of the UN, Kofi Annan, said *"Where most global conferences focus on global threats, this one will consider how best to use a new global asset."*

I am convinced that in the ongoing quest to using ICTs in beneficial ways, to building better and fairer democratic societies, and to improving people's lives and well-being, the upholding of Human Rights is and will continue to be the key element, especially in the face of the numerous still unsolved challenges. The Digital Divide is one of the biggest problems, which will require adequate and sustainable investments in ICT infrastructure and services as well as the necessary political will, especially in regions and societies where access to such infrastructure is currently underdeveloped. The freedom of expression, the protection of data and privacy online must be fundamentally guaranteed and enforced both on the legal side and by technological means. Any limitations to these freedoms must be based on good reasons, carefully considered, transparent, and of a temporary nature. Special attention must also be given to cases of discrimination in the context ICTs, such as violations of net neutrality or insufficient accessibility for people with disabilities or special needs.

A number of admirable organizations work on defending Human Rights online, such as the Global Network Initiative[21], the Electronic Frontier Foundation[22] and the European Digital Rights Initiative[23]. As our world continues to become more and more interconnected, the importance of their work will also increase.

[21] See http://www.globalnetworkinitiative.org/

[22] See http://www.eff.org/

[23] See http://www.edri.org/

8. Bibliography

Asia-Pacific Economic Cooperation. (n.d.). *APEC Privacy Framework.* Retrieved from http://publications.apec.org/file-download.php?filename=05_ecsg_privacyframewk.pdf&id=390

Bentley, L. (2011, 3 15). *Sens. Kerry, McCain Promote Online Privacy Bill of Rights.* Retrieved from IT BusinessEdge: http://www.itbusinessedge.com/cm/blogs/bentley/sens-kerry-mccain-promote-online-privacy-bill-of-rights/?cs=45976

Council of Europe. (1950, November 4). *European Convention on Human Rights.* Retrieved from http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

European Convention. (2000, December 7). *Charter of Fundamental Rights of the European Union.* Retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Union. (1995, October 24). *Data Protection Directive (Directive 95/46/EC).* Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Union. (2006, March 15). *Data Retention Directive (Directive 2006/24/EC).* Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

Heise Online. (2009, November 27). *Rumänisches Verfassungsgericht: Vorratsdatenspeicherung verstößt gegen Menschenrechte.* Retrieved from Heise Online: http://www.heise.de/newsticker/meldung/Rumaenisches-Verfassungsgericht-Vorratsdatenspeicherung-verstoesst-gegen-Menschenrechte-870904.html

Kanalley, C. (2011, January 27). *Egypt's Internet Shut Down.* Retrieved from The Huffington Post: http://www.huffingtonpost.com/2011/01/27/egypt-internet-goes-down-_n_815156.html

Krotoski, A. (2010, February 12). *Virtual Revolution: The Cost of Free.* Retrieved from The Guardian: http://www.guardian.co.uk/technology/blog/2010/feb/12/virtual-revolution-bbc-aleks-krotoski

Morris, S. (2009, November 17). *Spain govt to guarantee legal right to broadband.* Retrieved from Reuters: http://www.reuters.com/article/2009/11/17/spain-telecoms-idUSLH61554320091117

Organisation for Economic Co-operation and Development (OECD). (1980, September 23). *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data.* Retrieved from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Svensson, P. (2007, October 19). *Comcast blocks some Internet traffic .* Retrieved from MSNBC: http://www.msnbc.msn.com/id/21376597/

Toffler, A. (1970). *Future Shock.* New York: Random House.

United Nations. (1948). *Universal Declaration of Human Rights.* Retrieved from http://www.un.org/Overview/rights.html

United Nations High Commissioner for Human Rights. (1966, December 16). *International Covenant on Civil and Political Rights.* Retrieved from http://www2.ohchr.org/english/law/ccpr.htm

United Nations High Commissioner for Human Rights. (1966, December 16). *International Covenant on Economic, Social and Cultural Rights.* Retrieved from http://www2.ohchr.org/english/law/cescr.htm

United Nations High Commissioner for Human Rights. (2005). *Human Rights Handbook for Parliamentarians.* Retrieved from http://www.unhcr.org/refworld/docid/46cea90d2.html

United Nations High Commissioner for Human Rights. (2006, December 13). *Convention on the Rights of Persons with Disabilities.* Retrieved from http://www2.ohchr.org/english/law/disabilities-convention.htm

United States Federal Trade Commission (FTC). (n.d.). *Fair Information Practice Principles.* Retrieved from http://www.ftc.gov/reports/privacy3/fairinfo.shtm

World Summit on the Information Society. (2005, November 18). *Tunis Agenda.* Retrieved from http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

World Summit on the Information Society. (2005, November 18). *Tunis Commitment.* Retrieved from http://www.itu.int/wsis/docs2/tunis/off/7.html

World Wide Web Consortium (W3C). (1999, May 5). *Web Content Accessibility Guidelines 1.0.* Retrieved from http://www.w3.org/TR/WCAG10/

Zuckerman, E. (2011, January 14). *The First Twitter Revolution?* Retrieved from Foreign Policy: http://www.foreignpolicy.com/articles/2011/01/14/the_first_twitter_revolution