Thus cyber justice is defined by good governance principles and human rights norms and their realization in cyberspace through mobile technologies and the Internet. The cyber justice concept aims to achieve more accountability, transparency, and participation by and for all Internet users and service providers and moves and ‘live’ in cyberspace. Cyberspace as a borderless public space in which Internet is a network and a tool that allows different digital devices to connect and communicate and in which human rights principles, norms and standards apply in the same way as they do offline. But this space is yet without enforceable rules, because it lacks a global and transnational ‘judiciary’ such as a cyber court, or government, or police or parliament that would protect and foster people’s activities within that space globally. Nowadays, there is little to no dispute about the fact that governments, private enterprises such as service providers or companies, civil society organizations and the day-to-day internet users all share responsibilities to uphold human rights in cyberspace. The question is how this can be realized and turned into a ‘cyber constitutions’ and rule of law for the use of the Internet?

INTRODUCTION

Cyber Justice as a viable approach for promoting good governance based on human rights norms in the Internet. The author defines cyberspace as a borderless public space in which Internet is a network and a tool that allows different digital devices to connect and communicate. Cyberspace has more and more converted into ‘one-space’ in which we move, an online and an offline space. But the main difference between the offline and online space and world we move, live and work in is that, the online space lacks of

* Anja Mihr is Founder and Program Director of the HUMBOLDT-VIADRINA Center on Governance through Human Rights in Berlin, Germany. Her fields of research are Internet Governance, Human Rights, Public Policy, Transitional Justice and International Relations.
justiciability and liability of actors and institutions that provide online service that we use. Whereas there is no longer a controversy whether human rights are valid norms offline as well as online, the controversy is around the way, the means and the litigability of these norms and standards when using the Internet and the services it provides. Thus the cyberspace in general is a space without enforceable rules, because it lacks a common ‘judiciary’ such as a cyber court, or government, or police or parliament that would protect and foster people’s activities within that space globally. Nowadays, there is little to no dispute about the fact that, national governments or regional organizations such as the European Union (EU) or the Organization for American States (OAS) alone cannot safeguard these rights, let alone enforce or protect them. The solution must be a global governance regime based on human rights norms, good governance and multi-stakeholder principles.

Thus cyber justice is based on good cyber governance and its human rights-based approach for (1) more accountability, (2) more transparency, and (3) more participation by multiple stakeholders and actors through the use of cyber tools, such as the Internet and other mobile devices. Moreover, good cyber governance fosters human rights and protects them through technologies.

The cyberspace and the Internet as its communication tool allows for various such activities. But because there is no globally adhered code of conduct (yet) that would discipline or limit us users and providers the misuse and abuse of this communication and information tool, a cyber governance regime is needed. At the same time, people have rapidly adapted to the challenges and threats that cyberspace provides, in particular when it comes to their human right to privacy. These cyber-citizens or users have become more conscious of posting information and data that might potentially be used against them in international or national law suits—if these persons happen to touch physically ground in the respective country or territory. Consequently, it is possible to manage the behavior and to establish a rule of law for the cyberspace. The two main avenues to pursue are (1) to establish a societal and legally binding ‘cyber constitution’ and (2) to establish global enforcement and monitoring bodies, such as courts, multi-stakeholder committees or otherwise rotating, participatory and transparent governance regimes.

As for the time being, this cyber space does not yet have any enforceable common rules or standards, government or control globally agreed and adhered mechanisms that would protect and foster people’s activities in this space. Universal human rights norms and standards or
customary international law can serve as guidance and benchmarks for setting up governance regimes in cyberspace. Through new technologies, cyberspace offers an environment that consists of many participants who have the ability to affect and influence each other. This space is transparent and neutral in its nature but often defined, broadened, limited, or censored by the people who use it. Communication via the Internet is therefore often anonymous and used and shared with the worldwide public, which remains, in large part, unknown to the individual Internet user, namely each of us.

We nonetheless share our most private and personal data with this anonymous audience. Today, this worldwide public number around 2.5-3 billion Internet users, with a dramatically rapidly increasing daily ‘birth-rate’. If cyberspace were a country, it would be the largest and most populated in the world, albeit one without any constitutions or government. This “space” has no legislative or otherwise democratic decision making bodies. It has no police or law enforcement mechanism, let alone protection mechanism for all Internet citizens to safeguard their human rights. The human rights that is most in the focus of rights in the Internet and cyberspace is that of ‘privacy’. It is a right that defines our privacy as a sphere in which we enjoy and pursue our family life, friends, health and personal development. But this privacy sphere is hardly globally defined, except for Articles 7 and 8 in the Charter of Fundamental Rights of the European Union from 2000. Yet, it will take time to globally define it to make it legally enforceable and thus turn it into a protection mechanism for us moving in this ‘one-space’ world, in which we can share publically our professional life and privately our family lives, for example.

This chapter will elaborate on the genesis and development of human rights in cyberspace over the recent years.

I. PUBLIC PRIVACY AND HUMAN RIGHTS

‘Public privacy’ is a notion that aims to describe the dilemmas and achievements of promoting, safeguarding but also the threat that basic freedom rights face nowadays when using the Internet. Needless to say, those freedom and other human rights, such as the right to health and privacy that apply offline also apply online. The advantage of cyber space is that, it allows for any nationality, ethnicity, political orientation, disabilities, gender or otherwise background to communicate and to interact without prior burden that would discriminate the user because of these characters. Through new technologies, cyberspace offers an environment that consists of many participants with the ability to affect and influence each other. This space is
transparent and neutral in its nature but often defined, broadened, politicized, limited and censored by people who make use of it. Communication via the Internet is therefore often anonymous and yet used and shared with a worldwide public, which remains, to the large part, personally unknown for the individual Internet user, namely us. It is in a way a schizophrenic situation, because we tend to manage our most private data, such as health insurance, bank accounts and family issues in ‘clouds’ and public service providers, assuming that they would not be accessible for others.

Why do we then share some of our most private and personal data with the global community? The fact that most of this community and audience of our data is anonymous leaves us in the illusion of privacy. However wrong that is, in the context of human rights, the ‘right to privacy’ is thus one of the key issues to be discussed when promoting human rights in and through the internet. Privacy rights thus also encompass safety and security rights but also rules for participation. We assume that, without a commonly accepted ‘cyber-constitution’ based on human rights, and the rule of law based on effective measures and mechanisms to enforce these rules, the internet-citizens or citizens 2.0 of this world will have difficulties to protect and enjoy their human rights in cyberspace.

By sharing private information to a unknown public and potential hackers, security agencies or simply agents of banks and insurances, Internet users have already created virtual twins in this new space, without ever having a chance to delete information. Personal relationships and ‘being friends’ through social networks such as Renren and Facebook can be anonymous on the one side, and yet provide a vast amount of personal data and private messages. We will also see that, those thousands of refugees communicating their paths and resources through Facebook have left data that for immigration offices and asylum claims already matter. Such unintentional transparency can also close the door to many of those who aim for more security and safety. Our private and professional data has already become the new currency, the byte, with which we pay online services, in particular those services that are free of charge, such as offered by Google, Facebook, Alibaba, Whats-App or Amazon.

Data that is acquired through businesses and enterprises, education and training, finances and economics, private correspondence, and even health and personal issues are now dealt with by anyone who seeks access to it in this ‘endless’ space.¹ The vehicle, device or tool by which information

¹ Mindaugas Kiskis, Entrepreneurship in Cyberspace: What Do We know?, 1(1) SOCIAL TECHNOLOGIES 37-48 (Mykolas Romeris University 2011). Available at http://www.doaj.org/doaj?func=fulltext&aid=1045782 (last visited December, 2013).
moves in this cyber space is the Internet, and it moves on the highway called World Wide Web which is dramatically growing. But seemingly to national space and territory that we call a country or a state, the way people and actors behave and make decisions in this space is guided through principles and norms usually written down in constitutions or laws. Ideally the citizens set up these rules, regulations and laws for the citizens or users for users. That process of setting up common and joint rules and standards by internet-users for internet-users has not taken proper place in cyberspace, yet, although organization such as the UN Internet Governance Forum (IGF) which claims for finding multi-stakeholder based global solutions, including governments, CSOs, business and service provides for their advice. Although this forum is still largely focused on security threats such as cyber war and cyber espionage and thus how to deal and control theses developments, it recently focuses on how to uphold human rights online. But since the human rights based approach in the offline worlds is still facing major challenges and obstacles, the online approach is too. Thus, the online-world only mirrors our successes or failures to implement human rights in the offline-world.

Since the launch of the Universal Declaration for Human Rights (UDHR) in 1948, and the subsequent covenants and conventions we have sought over 60 years of experience that national mechanism to uphold these standards so far has been ill-suited. International and regional approaches have often been insufficient but also indispensable. Nevertheless, some of the normative legal and political frameworks that have successfully proven to protect human rights offline and which we find within state borders mainly in democratic countries, could also be transferred to the cyberspace, such as claims procedures, code of conducts, fair trials, penalties and limitations based on rule of law and others.

Ultimately, what is missing in cyberspace is a quasi-government or cyber-governance regime based on good governance principles (some would call them democratic principles) that allow to govern the needs and claims of its citizens through monitoring and enforcement bodies. These would include effective monitoring and decision-making bodies, independent enforcement mechanisms and broad and continuous participation of users and business in this process. All actors regularly advise, revise and consult with and respond to each other. In the case of cyberspace, these CSOs and business are Internet users and service providers all around the world.

Thus, public privacy is a notion that encompasses the respect for human rights and fundamental freedoms fostering in the protection of our data, security and privacy in the cyberspace. It is the freedom of information
and expression in the Internet on the one side, and security and privacy on the other side in the cyberspace. According to international standards and definitions, privacy is a private and personal space in which we develop our personality in a confident and free way and exercise our skills and capacities, maintain our health and enjoy social relationships with family and friends.

Hence, privacy in the cyberspace means using the Internet as a service tool for private purposes without fearing that third parties, such as governments or companies (i.e., national security agencies, Google+ or Microsoft) are accessing, selling or publicly posting our data for security or business purposes without our consent.

The right to freedom is stated in various international treaties and agreements. It encompasses the right of free expression, which includes the freedom to hold opinions and to receive and impart information and ideas without State interference. This right also includes the right to communicate and to express oneself in any medium, including through words, pictures, images and actions including exchanging ideas and thoughts through social networks or other internet platforms, to protest against misconduct and to demonstrate. Freedom means the right to political expression including comments on matters of general public interest; artistic expression and commercial expression, particularly when it also raises matters of legitimate public debate and concern. Because most democratic countries foster the installment of Internet for market economy reasons and better communication, political expression is given particular precedence and protection. To ensure that free expression and debate is possible, there must be protection for elements of a free internet and media such as printed and online press, including protection of journalistic or investigative sources.

Eventually, the challenge Public Privacy is facing is how to balance our personal, professional and private interests using the Internet as a free and open access communication tool, and benchmark our actions and rules against privacy and freedom rights for all.

The debates and discussions around freedom and privacy rights in the Internet are of fundamental importance under the notions of data protection, cybersecurity, cyber surveillance or cyberwar through cyberviruses. Some already call it the World Wide War in which various actors, such as states and non-state actors, such as hackers, are equally involved. Commercial state or inter-governmental agreements like SOPA, PRISM, PIPA or ACTA are just a few international governmental initiatives to regain the control

---

2 Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7(3) ETHICS & BEHAVIOR 207-219 (1997). Available at http://www.nyu.edu/projects/nissenbaum/papers/toward_an_approach.pdf.
over the borderless dataflow. They aim to control the access to data. Although some governments attain to protect our data in the Internet, these inter-governmental agreements can lead to massive misuse and abuse of private data that can affect many others fundamental freedoms and basic human rights. The challenge will be to assess how human rights can be fully guaranteed under these arrangements and agreements. The complete absence of effective data protection will have repercussions and consequences both in leveraging human right realization and in preventing people from enjoying human rights.

II. Universal Human Rights in Cyberspace

To mention but a few fundamental freedoms and privacy human rights that are dealt with in this context are, for example, free expression of belief, political opinion, art and written texts; the free and equal access to information; and the protection of privacy issues such as family relations, friendships or health issues. Furthermore, human rights in cyberspace is about the protection and security to be free from harassment and persecution on internet for a based on one’s own political, ethical or gender identity as well for hers or his private professional, educational or health data without his or her consent. It is about protecting one’s own intellectual property and creativity, i.e., art, movies, pictures, literature, scientific results, as well as having access at any time to fair and open trials—to name but a few.

The often proclaimed “Right to Internet” which aims to allow individuals have access to internet at any time, and the “Right to be Forgotten” which assures that, one’s own private data remains private and can be deleted at any time, are already part of the overall human rights standards concerning access to information, the right to privacy and data protection (as in the EU Fundamental Rights Charta) and participation. Yet, how to realize these rights and turn them into active legislation has to be seen. Case law will most likely take quite some time to establish interpretations of these rights, although the Research Division of the European Court of Human Rights has already in 2011 published a groundbreaking documents on the potential, the Case-law concerning data protection and retention issues relevant for the internet could mean in future decisions taken by the court. In this document, the freedom of expression, intellectual property and issues of cybercrime are seen the major deficits that yet have to be further defined and interpreted through case law.3 Further

3 Council of Europe, ECtHR, Research Division, Internet: Case-Law of the European Court of Human Rights, (Strasbourg, June 2011). Available at http://www.echr.coe.int. (last visited December, 2013).
below, I will give two examples of recent cases ruled by the court in 2012 and 2013 under these provisions.

The fact that, basic human rights principles and norms are universal has been reconfirmed in 1993 during the World Conference for Human Rights in Vienna, Austria. It is therefore no longer an issue of international debates whether freedom rights exist or not, but rather how to implement and enforce them into national legislation. During the conference, all UN member states confirmed that, all human rights derive from the dignity and worth inherent in the human person, and that the human person is the central subject of human rights and fundamental freedoms, and consequently should be the principal beneficiary and should participate actively in the realization of these rights and freedoms.

According to this statement, human rights are rights inherent to all human beings, regardless of nationality, place of residence, sex, national or ethnic origin, color, religion, language, or any other status. We are equally entitled to the protection and promotion of these human rights without discrimination. They are interrelated, interdependent and indivisible. Human rights embrace sets of different values such as solidarity, confidentiality, fairness or friendship as well as principles, norms and standards such as the right to fair trial, the freedom of expression, or the right to adequate housing, access to water or access to information. Human rights are often written down and guaranteed by law treaties, customary international law, general principles and other sources of international law. They include obligations and duties of governments, companies, individuals or other legal entities (duty-bearers) to act in certain ways or to refrain from certain acts. Duty-bearers, such as governments, have to protect the human rights of right-holders, that is to say any person and citizen on this planet, regardless of his or her background. Human rights are often named as social, civil, economic, political or cultural and there is no hierarchy between them. Social human rights are, for example, the right to education, health, social security, family and marriage. Civil rights are those to participate, to assemble, to live in dignity, to enjoy fair and open trial, to be free from torture, and to enjoy physical integrity. Economic human rights are those to work, to adequate salary, to enjoy holidays, and to set up enterprises. Political rights are those to vote or be

---

4 UN Doc, GA A/CONF.157/24 (Part I), Report of the World Conference on Human Rights by the UN Secretary-General, (October 1993) Available at http://www.unhchr.ch/Huridocda/Huridoca.nsf/(Symbol)/A.CONF.157.24+(Part+I).En (last visited December, 2013).

5 WORLD CONFERENCE ON HUMAN RIGHTS (Vienna, Austria, June 14-25, 1993).

6 UN Doc. General Assembly Resolution 217 A (III), Preamble of the Universal Declaration of Human Rights, (December 18, 1948).
elected, to participate in decision making processes, and so on. Cultural rights are those to religious freedom and practice, as well as customs and traditions. Eventually, all these different categories of human rights cannot be exercised or enjoyed without one another. The right to housing or to work, the freedom of religion or the right to health can only be enjoyed or pressed for if the human rights to assemble, protest and participate allows us to make open claims for these rights, in case they are not executed or respected. This is the holistic approach to human rights under the principle of the so called Golden Rule of ‘do no harm to others as you would have them to do to you’.  

This means that, all these human rights ought to be balanced and estimated insofar as they do not harm the rights of others.

The human right to information, for example, applies to the extent that this information does not violate the dignity or privacy of others. For example, if very personal information about health or family would be accessible for everyone, it carries the risk that, this information violates the rights of the person concerned. Yet, protection of data should never justify censorship or random surveillance. It is here where the balance starts and it depends very much on who decides about the limits and borders of freedom to information. The more stakeholders involved, the more likely this balance and result might be accepted by most people.

For example, the right to enjoy scientific progress under the International Covenant on Economic, Social and Cultural Rights (ICESCR) from 1966 specifies in Art. 15 that ‘everyone enjoys the benefits of scientific progress and its applications’ on, for example, scientific research and medicine patents or copyrights on technology and art. These rights are valid offline as well as online, and it makes therefore no difference whether we illegally copy an artefact in a museum or in cyberspace; both acts are a violation of human rights. In Art. 13, for example, the human right to education is mentioned. It means that, education should be made accessible, offline as well as online, to train, educate and empower people in order to develop their human personality. They should be empowered to participate in decision making processes in their professional lives and to govern societies. This right also includes access to online teaching or to E-Governance. Art. 17 of the UN International Covenant on Civil and Political Rights (ICCPR) from 1966 states that, no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence,

---

7 Internet Encyclopedia of Philosophy, The Golden Rule (2010). Available at http://www.iep.utm.edu/goldrule/ (last visited December, 2013).
8 These human rights are expressed in mayor international treaties, such as the ICCPR and the ICESCR 1966.
or to unlawful attacks on his honor and reputation. This article is fundamental for the understanding of the protection of our freedom and privacy rights in cyberspace, because in this article, we read further that everyone has the right to the protection of the law against such interference or attacks. Most liberty and freedom rights are found in this covenant as well as in other international human rights treaties in Africa, Europe, the Arab World or the Americas; for example, Art. 3 establishes the non-discrimination principle, Art. 18 mandates freedom of religion, Art. 19 upholds the freedom of expression, Art. 20 mandates sanctions against inciting hatred and Articles 21 and 22 mandate freedom of association, and so on.

All these human rights, to name but a few, are internationally recognized and even though some countries have not ratified these covenants, most of these rights have turned into customary international human rights law. This means that, even if countries have not ratified certain international treaties, these human rights are generally valid and applicable, i.e., within national jurisdiction. They are customary and general, because the majority of people around the world aheres to them or includes aspects of them in their national legislation or legal procedures. Ultimately, they are all valid both online and offline and there is no difference whether they are violated in cyberspace or within physical space and borders. Yet, the open question remains: who can protect, implement and enforce human rights in cyberspace, if governmental mandates end at their state borders?

Following the controversies on cybersecurity, national sovereignty, and individual freedoms of users over the past decades, in 2011, the UN Special Rapporteur on Freedom of Expression, Frank la Rue from Guatemala, urged governments not to cut off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of Article 19, paragraph 3, of the ICCPR. He called upon all states to ensure that, internet access is maintained at all times, including during times of political unrest.9 And in 2012, the UN Human Rights Council in Geneva stated that, the same rights that people have offline must also be protected online and calls upon its member states to ensure freedom of expression and the access to internet, or, for example, the access to international cooperations that provides media information such as social networks, search engines, etc.10

9 UN Doc. A/HRC/17/27, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, (Frank La Rue, May 16, 2011), para. 23, 79.
10 UN Doc. A/HRC/20/L.13. Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, (June 29, 2012), para. 1.
In 2013, during a number of occasions and events on the international and national level, such as the NSA affair between the USA, Germany or Brazil, the issues of cyber espionage and misuse of private data came about. In consequence and response to these different developments and incidents, the UN Special Rapporteur La Rue once again urged the UN member states to ensure that, individuals are able to freely seek and receive information or express themselves whilst respecting, protecting and promoting their right to privacy. He highlighted the fact that, privacy and freedom of expression are interlinked and mutually dependent and therefore without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, cannot be assured that, their communications will not be subject to states’ security.\(^\text{11}\) The UN report received many responses, in particular by the civil society organization (CSO) network community. CSOs have long claimed that, human rights are not protected well enough in cyberspace. The Electronic Frontier Foundation (EFF), for example, claimed that, technologies can open a Pandora’s box of previously unimaginable state surveillance intrusions and metadata can reveal sensitive information that can be easily accessed, stored, mined and exploited.\(^\text{12}\)

Hence, so far there is no regional or international human rights regime such as UN, ASEAN, EU, OSCE, OAS or AU, ready to deal with the consequences and effects of global flow of data, intellectual property, secret information or private data, even though all these regimes have the topic on their agendas. Although citizens that use internet within the borders of regional organizations such as the EU enjoy some protection, these measures are not valid globally. The USA or China have long urged for joint binding agreements to deal with the borderless data flow in order to either protect or to restrict it. In technical terms that is a fight with windmills that cannot be won by state institutions nor by international inter-governmental regimes alone. The reason why it takes more than just a few governments in international regimes, such as the UN to solve the problems is that, it takes effective institutions to enforce common rules. Without the wider cyber community, like technical companies, internet providers, or search engines and so on, effective enforcement mechanism will less likely be established. Because the cyberspace is not restricted to states or to any

\(^{11}\) UN Doc. A/HRC/23/40, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, (Frank La Rue, April 17, 2013), para. 79.

\(^{12}\) Electronic Frontier Foundation, Internet Surveillance and Free Speech: The United Nations Makes the Connection, (June 4, 2013). Available at https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection (last visited December, 2013).
geographical or physical borders, it is thus not bound to any state or inter-state agreement and not to be controlled by state institutions alone.

The international human rights regime, for example, is entirely based on states’ (often non-binding) willingness and capacity to promote and protect human rights and is therefore a valid but weak institutional set up to govern cyberspace. Moreover, because this international regime depends on the joint agreements and regulations set by governments, including democratic and non-democratic ones, such as Russia, USA, Germany or China, the results are often compromises that, lack of strong monitoring and enforcement mechanisms based on international human rights law. More so, other stakeholders are often excluded from this process, i.e., internet providers, let alone the global network community or the billions of individual users, namely us. The International Internet Governance Forum (IGF), one of the main forums to tackle these issues, is yet also based on national institutions and their agencies and delegates. It is not truly transnational, although it aims to solve transnational violations of human rights and privacy.

Still, there is no international cyber law to combat cyber-attacks or the dissemination of private data and secret files. And if this culminates into a so called cyber-war, there has to be one party that declares the war to another party. Who are these parties? A state government against whom? And as every war ends, among which parties will there be a “peace contract” if no government or sovereign agent is involved and the combatants hide behind anonymous masks? Therefore, governmental rhetoric about leaks in the cyber world often use organic terms, such as cyber-attack, i.e., by virus, infections etc., which suggests that, the Internet is “alive” and therefore requires preventive, defensive measures, similar to global diseases and threat to health. But in the case of cyberwar, the ‘enemy’ is the individual internet users, who ‘abuse common rules’ of good conduct. Nonetheless, state governments, such as the US or British government have reacted in and often irrationally and precipitant way to the threat. This was demonstrated by the scandal around PRISM and the whistleblower, Edward Snowden, in 2013 or as the consequence of secret files leaked by WikiLeaks. None of these cases seems to be resolved, let alone in a way that would mean more data protection, privacy and freedom for all internet users on a global level. The often overhasty reaction by government, when governmental or secret data files get leaked shows the shortcomings of the current legislative bodies that are in place domestically and internationally. Interestingly enough, during these scandals, confidential secret service data has been made public by individual agents that, in return,
are made responsible for ‘espionage’ against states—an antagonism which exemplifies the lack of definition and clarification in these aspects.

Yet, efforts to ‘tame’ cyberspace and to give it overall rules and regulations to which we should all adhere to, is as old as the cyberspace and internet itself. In 1996, Jon Perry Barlow published the ‘Declaration of Independence of Cyberspace’. In this declaration, he indicated the situations and controversies that, today’s internet users worldwide are worried about. The Declaration sets out, in sixteen short paragraphs, a rebuttal to government of the Internet by any outside force, specifically state governments. He argues that, no government has yet the consent of the internet users to apply arbitrary laws and restrictions to the internet, and if they try to do so, as with the data protection laws within the EU or USA or the various inter-state agreements, servers will be changed and data will continue to be published through whistleblowers, hackers and “leakers” without the owner’s consent. The internet is a world outside any country’s borders. Barlow assured, twenty years ago, that the Internet community and thus the global user community has to develop its own social contracts to determine how to handle its problems based on the Golden Rule, which again is also the foundation for realizing human rights. The rule can be interpreted in such a way that if one does not want to have its own private data, pictures, letters, images or intellectual property and ideas to be publically disposed without one’s consent, then one should also not dare to publish someone else’s data without that person’s consent. Whether such social contract for the cyberspace will ever be realized or not, the idea behind that is individual responsibility and adherence to human rights, which the global community, us, has long agreed to. Another protagonist who aims to set common rules for the internet is Jeff Jarvis. He came up with another claim for internet freedoms and manifested that every citizen of this world needs to enjoy the right to connect, to speak freely, to assemble and to enjoy his or her privacy. Eventually, this can only be guaranteed with open and free access to public information and public good/spheres through internet.

The need for basic human rights is not disputed in this world anymore, not among cultures or among nations. Everybody agrees that freedom, justice, privacy and security are important. However, among the 2.5 billion internet users, not everyone will have the same ideas about their realization

---

13 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, (February 8, 1996). *Available at* https://projects.eff.org/~barlow/Declaration-Final.html (last visited December, 2013).
14 Jeff Jarvis, *A Bill of Rights in Cyberspace*, (March 27, 2010). *Available at* http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/ (last visited December, 2013).
and implementation in cyberspace. Thus, there is the claim that according to these general freedom principles and norms, a social contract for cyberspace could be established. This contract would need to be enforced by all internet users, regardless whether they are private or public, companies or governments and so on. This cyber human rights regime would be based on individual responsibility and behavior and on personal disguise and sanctions against those who violate these norms. Needless to say, companies’ business practices and government relationships can result in abuses of the human rights of freedom of expression, development, health, assembly and privacy. These human rights are often called ‘Digital Rights’ if they are exercised within cyberspace or through internet. Digital Rights, are embedded in freedom rights such as those stated in the UDHR or the ICCPRs that allow the access and use of ICTs such as computers and digital media, i.e., to information, to work, to communication, to health, to participation, to expression, to development (SDGs), to assemble, etc.\footnote{Office of the High Commissioner for Human Rights, Human Rights Indicators: A Guide to Measurement and Implementation, (Geneva 2013). Available at https://unp.un.org/Details.aspx?pid=23745 (last visited December, 2013). For the definition of digital rights see: BUSINESS AND HUMAN RIGHTS RESOURCE CENTER, RANKING DIGITAL RIGHTS PROJECT. Available at http://www.business-humanrights.org/Documents/Ranking_Digital_Rights (last visited December, 2013).}

On December 10, 2013, the International Human Rights Day, and 65 years after the UDHR was proclaimed by the UN in 1948 over 500 writers and Noble Prize Winners from over 81 countries, have signed an open petition urging the UN to draft an international bill on digital rights. They argue that, the dramatic increase of spyware on private data is undermining democracy online and offline and makes human rights null and void and privacy an illusion, so they fear.\footnote{The Guardian, International Bill of Digital Rights: Call from 500 Writers around the World, (December 10, 2013). Available at http://www.theguardian.com/world/2013/dec/10/international-bill-digital-rights-petition-text (last visited December, 2013).} Reactions to their open call were internationally perceived and the petition comes at a time during which different UN bodies are working on better digital rights protection. The massive support from the user community to develop such a concept is expected to have some impact on the progress of global protection mechanism and an international binding document.

### III. Cyber-Governance Efforts

Although international governmental organizations (IGOs), such as the UN (IGF), the Organization for American States, the African Union or the European Union or the International Telecommunication Union (ITU) aim
to set international standards for the use of cyberspace and internet to be respected and enforced by national governments, they have thus far failed to do so. The reason for this is that, states’ powers and enforcement mechanisms often end at state borders because their mandate to protect human rights is entirely based on state sovereignty and governments. IGOs and international courts often have only limited measures and means to protect human rights, let alone enforce them. What is thus needed is a new definition of Internet or cyber sovereignty. Thus sovereignty would be based on similar criteria as that of national or domestic sovereignty, namely to control and executive effectively and independently common norms and standards in a given space (formally: territory). A combination of rotating governance bodies and through active participation of various stakeholders, such control (or: governance) can be effectively executed. Charges, penalties or even imprisonment in case of misconduct and misuse of cyberspace need to be executed in a similar way as international courts, such as the European Court for Justice (ECJ), the International court of Justice (ICJ) and the International Criminal Court (ICC) already do.

In the debate and effort to set up a cyberspace governance regime, human rights norms and standards (such as the human rights to privacy, security, health, free expression, movement and enterprise) give guidance to the various number of different actors that are involved in the design of the cyberspace regime and how to possibly regulate it. If ever established, the cyberspace governing body will be one of multiple stakeholders and actors including national, international as well as private actors, such as representatives of companies, social networks, NGOs and individuals.

The big challenge thus for cyber governance is how to enhance users’ trust in the Internet and how to legitimize actors and provides that act and offer services, free or non-free of charge? The is on the one side, the institutional and agency legitimacy which concerns service providers, governments or private companies such as Microsoft, Google or Renren. There is on the other side, the actors and stakeholders legitimacy focus legitimacy. Their interaction and participation in the larger decision making process has to be regulated in the most transparent way possible accountability mechanism, such as common international human rights norms and standards should be enshrined in something that would qualify as a cyber constitution’ which includes monitoring, decision making measures and justiciability of these rights that is to say a Rule of Law in Cyberspace, i.e., through a global Cyber Court. There is no more and no less legitimacy, or belief and trust in the Internet than offline, thus the same mechanism that apply offline to increase trust and liability need to be applied online.
Internet users in societies in which the rule of law and human rights are not complied will less likely trust the Internet than users that live in societies in which human rights are compliance. But, people who live in societies with low law or human rights compliance will trust more in online agencies, companies or services that are based in societies in which the rule of law is adhered to. Thus by using services outside their country or state they live in, they legitimate Internet services, companies by repetitavily using their services and enjoy positive and non abuse responses by them, i.e., when they order consumer goods through online services abroad which actually deliver after people have pre-paid. Positive experience with norm compliance through external stakeholders which increase the legitimacy and trust in these services.

IV. A THREAT TO JUSTICE AND ‘RULE OF LAW’ IN CYBERSPACE

Emails, websites, networks, mobile phones, or the World Wide Web in general are not per se a safe place to put private data, but it has the potential to be so if these devices and their users that ‘move’ in cyberspace can trust in a rule of law abiding cyber regime. Although cyberspace is not an actor and therefore it cannot guarantee our freedom, uses, actors, state authorities, international organizations and companies can. Now that we live in a state of ‘post privacy’, this is more then ever important. We live in a world in which everyone of us has a long data trail somewhere in the internet and cyberspace that allows for retroactive actions by anyone at any time on a global scale, by national security agencies and local authorities, by providers or by ourselves.17

Cybersecurity is therefore best guaranteed if all actors and providers adhere to the same principles and if neutral multi-stakeholder based global enforcement mechanism can safeguard the Rule of Law. Human security, for example, is a people-centered view of security that is necessary for national, regional and global stability. It is about securing “freedom from want” and “freedom from fear” for all persons and therefore to assure human rights for all as the best path to tackle the problem of global or local insecurity.18 Political security is concerned with whether people live in a society that honors their fundamental freedoms. This level of security is more likely to be achieved if internet users can participate in decision

17 Jacob Appelbaum, Elevate Open Everything, ELEVATE FESTIVAL OPENING SPEECH (October 25, 2013). Available at http://2013.elevate.at/festival/ueber-das-festival/newsmagazin/detail/news/jacob-appelbaum-elevate-open-everything/ (last visited December, 2013).
18 Chapter 2: New Dimension of Human Security, HUMAN DEVELOPMENT REPORTS 24 (1994), Available at http://hdr.undp.org/en/reports/global/hdr1994/chapters/ (last visited December, 2013).
making and legislative processes of their country according to international human rights law standards, and if these laws later are complied with, for example the Rule of Law in any country or in cyberspace.  

Yet, Cybersecurity is the collection of tools, policies, the different security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment and users’ assets at any time at any place in this wide space. This includes, for example, connecting computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment—under the same standards, rules and consequences commonly agreed to. In the context of Rule of Law cybersecurity, strives to ensure the attainment and maintenance of the security properties of users’ assets, data and information against relevant security risks in the cyber environment. The general security objectives are comprised of the integrity of information and data authenticity and non-repudiation, and aim to secure data in a confidential manner.

In an essay on the Critical Theory of Cyberspace, Michael Froomkin highlights that, the Internet is a neutral tool in cyber security that can improve the quality of deliberative communities through effective participation and legitimacy of rules and standards, and consequently, the quality of political/societal systems or regimes. Therefore, protecting and securing this data for use that does not harm deliberative communication is one of the top priorities of the emerging cyber regime. Bearing in mind that, the number of internet users in 2000 was around 360 million users and today is around 3 billion, the urgency for setting up common norms and standards for internet to be used both by private and public actors and sectors, is high.

Froomkin and others have long argued that, due to the fact that, communication between these users has risen dramatically over the past decades, deliberation theories might apply to explain what may happen next.

19 Thomaz Guedes da Costa, Political Security, an Uncertain Concept with Expanding Concerns, GLOBALIZATION AND ENVIRONMENTAL CHALLENGES: RECONCEPTUALIZING SECURITY IN THE 21ST CENTURY 562 (Hans Günter Brauch ed., Berlin: Springer 2008). Available at http://link.springer.com/chapter/10.1007%2F978-3-540-75977-5_42# (last visited December, 2013).

20 INTERNATIONAL TELECOMMUNICATION UNION, DEFINITION OF CYBERSECURITY Available at http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. Also vid. Tim Maurer, Cyber Norm Emergence at the United Nations—An Analysis of the UN’s Activities Regarding Cyber-Security?, 8 (Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School 2011). Available at http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf (last visited December, 2013).

21 Michael Froomkin, Habermas @ Discourse. Net: Toward a Critical Theory of Cyberspace, 116 HARVARD LAW REVIEW 749-873 (2003).
Namely, due to the fact that, people communicate more for professional, business or private reasons through the Internet, they also exchange more ideas and opinions and thus create common norms and standards according to which they decide or govern their local environment. These are opportunities for Rule of Law. Consequently, global norms become local and vice versa. This is also true for human rights standards as for many other standards. Standards, norms or rules that work effectively by solving peoples daily problems stand great chances to become global rules. Today, more people than ever have a common understanding today of privacy or freedom of expression or access to information and therefore share the same ideas and principles about what to express and how to protect and secure their private data. For example, the common wish to express religious ideas or political opinions without harming or insulting others or being insulted in one’s own religious belief is a more common understanding among internet users today, than it was thirty years ago.

Nevertheless, according to the Freedom in the Net Index issued in 2013, most countries in the world censor Internet Freedom, some more, some less. There are various ways to do so. Governmental agencies, Internet police or hackers-for-hire, use different methods to disturb, filter or censor the exercise of freedom rights. The Index cites that, at least in 29 out of 60 states, blocking and filtering of information and platforms in the internet is a common practice. The tendency is rising. Although not all countries in the world are covered in this index, the main industrial ones are and this indicates how virulent censorship is. Cyberattacks on dissidents and human rights advocates, or paid pro-government bloggers, i.e., in China, Bahrain or in Russia are a daily annoyance.

Apart from self-censorship, the most common way to censor Internet users is blocking and taking down web sites under governmental surveillance or deleting critical websites and social networks. Sometimes, security agencies cause the slowing down of the speed of Internet, so people cannot use it for quick messages or search, for example, for protests, meeting points for demonstrations, urgent actions etc. Thus, the freedom rights are under massive pressure and constant surveillance. This all needs to be globally regulated.

Over the past years, different stakeholders, actors and agencies, such as

22 Sanja Kelly, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, & Ashley Greco-Stoner, eds., Freedom on the Net 2013. A Global Assessment of Internet and Digital Media, (Freedom House 2013). Available at http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf (last visited December, 2013).
representatives of search engines, communication platforms or social networks, to name but a few: Google, Skype, Microsoft Bing, Facebook, Twitter, Yahoo, Linkedin, Sina Weibo, Renren, Yandex or Yamli, have grouped themselves in different fora and networks. Search engines and social networks, for example, all have in common that they can allocate and collect data from each internet user, store it and later sell it or provide it for external users, such as private companies or national security agencies. The multi-stakeholder approach includes these companies and private actors as well representatives of international organizations such as the UN or the EU and national governments. They come together through informal and formal fora and build partnerships for consultation. The IGF and the World Summit on the Information Society (WSIS) has over 170 representatives of UN member states, which are all convening this forum for a multi-stakeholder policy dialogue. During their annual meetings, they attain to develop a shared understanding about the protection of data in cyberspace but they nevertheless play different roles and have different purposes and aims in these fora and networks. Governmental representatives can make decisions, implement and enforce them. Others, like the consultance from private companies and NGOs, can only serve as advisors and experts in these fora. Their partnerships are voluntary, with participation driven by the perceived benefits they may see emerging from the process. They are increasingly being used to challenge and lobby for change in policy processes. They have already played a role on previous governmental agreements to protect copyrights or other data in cyberspace, such as ‘IP Protection Act’ Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) in 2008, or when passing the ‘Stop online privacy act’ (SOPA) in 2011 as well as during the 2012 attempt to set up an inter-governmental ‘Anti-Counterfeiting Trade Agreement’ (ACTA) on a global level. Copyright is an exclusive right, it has the potential to restrict freedom of expression, i.e., scientific knowledge on medicine, technologies, art or literature, by others than the holder or author of the copyright.

Most of these recent efforts to protect copyrights and thus human rights where not successful because it became evident that, governments alone cannot solve the problem of data protection. They need to join the multi-

---

23 Internet Governance Forum. Available at http://www.intgovforum.org/ (last visited December, 2013).
24 Ellen M. Wesselingh, The Magic Show of Balancing the Enforcement of Copyright and Freedom of Expression, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON ICT LAW 2013, (August 15, 2013), (unpublished article).
stakeholder approach that includes actors from the non-formal and private sector such as technical corporations, search engines, internet users, civil organizations, and so on. Therefore in 2011, the Council of Europe in Strasbourg expressed its concerns when highlighting that, any Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, interdependence, and interrelations in accordance with international human rights law. They must also ensure full respect for democracy and the rule of law and should promote sustainable development.\(^{25}\) Therefore, in recent international meetings, we find a mix of actors and stakeholders involved in international, regional or national, for example IGOs, states, CSOs, technical actors that represent providers, communication services or search engines such as Microsoft, Apple, Google, Firefox, Yahoo, Xando, Weibo, Skype, Clouds, Dropbox etc. or other private business actors such as online business and companies, start-ups, different App provides, Amazon, DHL, or network actors like Mxit, Wretch, Facebook, Nexopia, Google+, Badoo, XING, Hi5, Orkut, Renren, Linkedin, Skype, and so on. The list could be continued. Implicitly, the Internet user is involved in all these categories and can have multiple functions, for example, when being a user of Renren, a customer of DHL, and working for IBM. Therefore her or his data can be collected by multiple technical providers, engines or companies during every phase of one’s own life. How little we know about how our data is processed, used or misused shows the judgment by the European Court of Justice of the European Union in October 2015. The Court declared that, the EU Commission’s ‘U.S. Safe Harbour Decision’ is invalid. Because most international service provides and social media networks are based in the US, in the EU, almost 5,000 companies relied on this Safe Harbor policy to operate businesses among the regions. It had allowed companies to self certify to provide “adequate protection” for the data of European users to comply with the European data protection directive, and with fundamental European rights such as the right to privacy under Article 8 of the Fundamental Rights Charta. This is now no longer valid and data of European users have to be better protected, and thus the European Commission has to amend and revisit the agreement to set common rules and enforcement mechanism that guarantee that, privacy matters are better protected in the future. The Court decision is only the beginning of what a

\(^{25}\) Council of Europe, *Declaration by the Committee of Ministers on Internet Governance Principles*, (September 21, 2011). *Also vid. Wolfang Kleinwächter, Ed., Human Rights and Internet Governance*, 7 (Berlin: Internet and Society Co:llaboratory e.V 2012). *Available at* http://dl.collaboratory.de/mind/mind_04berlin.pdf (last visited December, 2013).
new interpretation of ‘privacy’ and ways and means on how to safeguard what is meant by it.\textsuperscript{26}

Global cyberspace norms will more likely be adhered to by all internet-users if they have been part of designing them and agreeing upon them. This will enhance the legitimacy and authority of institutions, organizations, companies, agencies and practices in cyberspace.\textsuperscript{27} Frequent and widespread national data surveillance programs instead jeopardize civic trust and confidence in the Internet. They are conducted by national security agencies, secret services or private companies. Governments and national authorities using national intelligence or spyware viruses, or private corporations using business intelligence, can modify cookies on private computers to deduct data for their own purposes. Every Internet users leaves long data trails through social networks, i.e., on Skype and Facebook, after online shopping, when using governmental information services, or while sending SMS and other private messages through Email. We leave data trails when applying for new IDs online, using credit cards and so on. The amount of data is massive, hardly anyone has an oversight over it and therefore the abuse and misuse of these data is so alarming. We are no longer the owner of our own private data, and that is what leads to misconducts in cyberspace. It is massively used and processed by other stakeholders, both private and public ones.\textsuperscript{28} No single government has control over all this data, not even the most democratic societies, and this is why this data-trail also poses a threat to democracy and good governance. The fact that we cannot be assured protection leads to mistrust in companies or national authorities and thus decreases legitimacy of governments and other authorities.

Security issues are often connected to warfare and also cyberwarfare. The term cyberspace is a creation by military services and this foundation

\textsuperscript{26} COURT OF JUSTICE OF THE EUROPEAN UNION, DECISION NO C362/14 (October 6, 2015). Available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

\textsuperscript{27} William E. Hornsby Jr, \textit{The Ethical Boundaries of Selling Legal Services in Cyberspace}, NATIONAL LAW JOURNAL (1996). Available at http://www.kuesterlaw.com/netethics/abawill.htm (last visited December, 2013); \textit{Also vid.} Joe Peppard, & Anna Rylander, \textit{Products and Service in Cyberspace}, 25 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 335-345 (2005). Available at https://dspace.lib.cranfield.ac.uk/bitstream/1826/2687/1/Products%20and%20Services%20in%20cyberspace%20-%202005.pdf (last visited December, 2013).

\textsuperscript{28} Forrest Hare, \textit{Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?}, 3 THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE CRYPTOLOGY AND INFORMATION SECURITY SERIES (Christian Czosseck, & Kenneth Geers eds., Amsterdam: IOS Press 2009). Available at http://www.ccedcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf (last visited December, 2013). Electronic Frontier Foundation. Available at https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection (last visited December, 2013).
makes it sometimes difficult to apply civil rights and judiciary let alone a Rule of Law concept on cyberspace. The term expresses the combination of technical warfare instruments in cyberspace and was curbed in 1993. This type of cyber warfare involves the actions by a state, i.e., national military or international organizations (i.e., NATO) to attack another nation’s computers or information networks through, for example, computer viruses. In response to the dramatic rise of expenditures for cyberwarfare and cyber control by all countries around the world, the UN Security Council Working Group Report 2013 urges all UN member states to make careful risk assessment in cyberspace, i.e., control and vigilante cyberattacks through hackers. These attacks can dramatically affect national infrastructure and destroy a whole country, for example, through ICT-enabled industrial control systems of nuclear power plants. Furthermore, if governments and other actors were to invest more in confidence-building measures in the cyber domain, i.e., transparency, participation, consultation with ASEAN, AU, Arab League, OSCE, the NATO or the EU, in adopting cybersecurity policies, that would help to regain trust of internet-users. Otherwise, so the concern, cyber surveillance becomes a dangerous weapon against citizens, companies, and countries without control. In this context, it is national security agencies or the military which harms and violates human rights in cyberspace. For example, after 9/11 anti-terror internet surveillance measures in Europe, the USA, China, Russia, Saudi Arabia, Kenya and way over 100 countries worldwide have increased dramatically. In India, after the 2008 terror attack in Mumbai, the government passed the Information Technology Rules in 2011 which states that, ‘anyone who finds certain web content objectionable now has the right to have that site shut down.’

---

29 John Arquilla, & David Ronfeldt, *Cyberwar is Coming!*, 12 COMPARATIVE STRATEGY 141-165 (1993).
30 NATO Cooperative Cyber Defense Center of Excellence, (Tallinn, Estonia). Available at https://www.cccdcoe.org/ (last visited December, 2013). Also vid. Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace*, (to be published in the end of 2013).
31 Tim Maurer, *Cyber Norm Emergence at the United Nations—An Analysis of the UN’s Activities Regarding Cyber-Security*, 15 (Massachusetts: Belfer Center for Science and International Affairs Harvard Kennedy School 2011). Available at http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.
32 Detlev Wolter, *The UN Takes a Big Step Forward on Cybersecurity*, (September 2013). Available at http://www.armscontrol.org/act/2013 09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.
33 Radio Netherlands Worldwide, *Declarations of Gerard Oonk, Director of the Dutch NGO, (The India Committee of the Netherlands, May 5, 2011). Available at http://www.rnw.nl/english/article/stricter-indian-internet-laws-threaten-human-rights (last visited December, 2013).*
CONCLUSION

There is no need or desire to establish a separate set of human rights standards for cyberspace or for the Internet. Human Rights apply offline as well as online. The difference between these two worlds is the fact that, in the offline world, human rights are often enshrined in national constitutions or international frameworks that have either constitutional courts and parliament to monitor them or international monitoring bodies or courts that can enforce them. The online world, however, is thus far lacking of any such decision-making and enforcement mechanisms. Further, the magnitude and past of new technologies that allows for more and quicker data distribution, collection and procession can no longer be managed or governed by national governments nor by international organizations alone. The role and influence of private actors and companies as well as CSOs in cyberspaces is too obvious to be ignored. Therefore, one approach to safeguard and develop a regime that is rule of law based in cyberspace ought to be multi-stakeholder based and adhered to by cyber-users as well as by companies or governments. A global Cyber Court is one point of discussion, rotating governance regimes in which private and public or governmental actors sit side by side, decide and enforce and share responsibilities are other suggestions. The new cyber-regime stands chances to be more transparent and accountable beyond national security or autocratic restrictions, because it is non-territorial and has its own user-driven dynamic. Whether it is automatically more democratic and rule of law based remains nevertheless to be seen.