Good cyber governance must establish a human rights-based approach for (1) more accountability, (2) more transparency, and (3) more participation by stakeholders through the use of cyber tools, such as the Internet and mobile devices. Moreover, good cyber governance fosters human rights and protects them through technology. Cyberspace, however, is a borderless public space in which individuals, regardless of their citizenship, nationality, ethnicity, political orientation, or gender communicate and interact. Individuals use cyberspace and the Internet to conduct business, make policies, and organize their private lives. Yet this space does not have any common rules or standards, a governance apparatus, or enforcement or control mechanisms that would protect and foster people’s activities. Universal human rights norms and standards 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. Internet communication is often anonymous and used and shared...
GOOD CYBER GOVERNANCE

with the public worldwide, which usually remains 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 global, public community numbers around 2.7 billion Internet users. 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 to safeguard human rights for all Internet citizens.

For the purpose of this article, I will therefore argue that (1) cyber governance does not need new human rights norms or standards, but rather new governing and monitoring regimes and enforcement mechanisms that guarantee and safeguard the human rights of all people who use cyberspace; (2) we need to identify all private, public, governmental, and international actors who carry responsibilities in either violating or fostering human rights in the Internet; and (3) all users need to establish mechanisms that enhance trust in institutions (e.g., governments), companies (e.g., Internet providers, servers), and organizations (e.g., Facebook, YouTube).

Cyber Governance and Human Rights. On one hand, the Internet and cyberspace can foster and enhance individuals’ inclusive participation and access to politics and business, which they otherwise would not have. On the other hand, it can also exclude those who are Internet-illiterate or have difficulty accessing the Internet (e.g., children, aging people, and people without Internet-access). By sharing private information in cyberspace, billions of Internet users have already created virtual twin-identities in this new space, without ever having a chance to delete that information. Personal relationships and friendships through social networks such as Renren and Facebook can be seemingly anonymous and yet provide a vast amount of personal data; thus, it is a space for public privacy.1 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.2 Ultimately, what is missing in cyberspace is a quasi-government or governance regime that governs the needs and claims of its citizens through monitoring and enforcement bodies: a good cyber governance regime.

Although international governmental organizations (IGOs), such as the United Nations (UN), the Organization for American States (OAS), the
African Union (AU), and the European Union (EU) aim to set international standards and legally-binding treaties for the use of cyberspace and Internet to be respected and enforced by national governments, they generally fail to do so. The reason is that each state’s powers and enforcement power often end at state borders because their mandate to protect human rights is entirely based on state sovereignty and governments. Also, IGOs and international courts often have limited measures and means to protect human rights, let alone enforce them.

Because cyberspace has no physical or national borders, the ways and means to govern this new borderless regime are not yet defined. Nevertheless, in the debate and effort to set up a cyberspace governance regime, human rights norms and standards -- such as the right to privacy, security, health, free expression, movement, and enterprise -- provide guidance to the various different actors that are involved in the regulatory design of the cyberspace regime. If established, the cyberspace governing body will consist of multiple stakeholders and actors. This includes national, international, as well as private actors such as representatives of companies, social networks, NGOs, and individuals. The World Internet Governance Forum under the UN has initiated such a concept. Other fundamental freedoms and privacy human rights that are dealt with in this context are: freedom of expression, religion, political opinion, art, and written texts; free and equal access to information; and the protection of privacy issues such as family relations, friendships, and health issues. Furthermore, human rights in cyberspace is based upon secure protection from harassment and persecution on the Internet based on one’s own political, ethical, or gender identity along with undisclosed professional, educational or health data. Cyber human rights should protect an individual’s intellectual property and creativity in areas such as art, movies, pictures, literature, scientific results, etc. with access at any time to fair and open trials.

Good cyber governance has to be conducted over a domain of an individual’s public privacy, which includes public and private data. It must reconcile the freedom of information and expression on the Internet with the security and privacy of individuals in cyberspace. According to international standards and definitions, privacy is a personal space in which we develop our personality in a confident and free way, exercise our skills and capacities, maintain our health, and enjoy social relationships with family and friends. Hence, privacy in cyberspace means using the Internet as a service tool for private purposes without fearing that third parties, such as governments or companies (e.g., national security agencies, Google+, Microsoft) are accessing, selling, or publicly posting our data for national security or business purposes without our consent. Eventually, maintaining public privacy faces the challenge of how to balance our personal, professional, and private interests using the Internet as a free and open access communication tool, while creating standards and rules that may inhibit some level of privacy.

The debates and discussions around Internet freedom and privacy rights
GOOD CYBER GOVERNANCE

are fundamentally important in the areas of data protection, cybersecurity, cyber surveillance, and cyberwar through computer viruses. Some call it the "World Wide War" in which various state and non-state actors such as individual hackers are equally involved. Commercial-state or inter-governmental agreements, such as the Stop Online Piracy Act (SOPA), the NSA's surveillance program, PRISM, or the Anti-Counterfeiting Trade Agreement (ACTA), are just a few governmental initiatives to regain the control over the borderless dataflow. The challenge will be to assess how human rights can be fully guaranteed under these arrangements and agreements.

The often proclaimed 'right to Internet', which aims to allow individual access to the Internet at any time, and the right to be forgotten to ensure that one's own personal data remains private and can be deleted at any time, are already part of overall human rights standards concerning access to information, the right to privacy, and data protection (as in the EU Fundamental Rights Charter) and participation. The EU Court of Justice passed a landmark decision in May 2014 that buttresses privacy and the right of users to have their data removed or forgotten from the Internet. The ruling targets search engines and data providers such as Google, YouTube, and Facebook. Unfortunately, it only applies to the EU territorial space.

A global solution has yet to come. The Research Division of the European Court of Human Rights has already made some headway in 2011 by publishing a groundbreaking document on potential case law concerning data protection and retention issues relevant for the Internet. However, other international or domestic courts might take some time in interpreting the legal rights laid down by the EU Court of Justice.

Human rights are often inscribed and enforced by 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. Human rights are often described as social, civil, economic, political, or cultural rights, and there is no hierarchy among them. These different categories of human rights cannot be exercised or enjoyed without one another. The human right to information, for example, applies to the extent that this information does not violate the dignity or privacy of others. This is the holistic approach to human rights under the principle of the Golden Rule: "Do no harm to others that which you would not want done to you." Along these lines, a cyber human rights regime ought to be balanced and estimated insofar as they do not infringe on the rights of others.

That being said, protection of data should never justify censorship or random surveillance of individuals. Finding the balance depends very much on who decides the limits and borders of freedom of information. The more stakeholders involved, the more likely the resulting balance will be accepted. Ultimately, the UN Human Rights Council reminded us in 2012 that human rights are all valid both online and offline, and there is no
difference whether they are violated in cyberspace or physical space within borders. Yet the open question remains: who is the duty bearer? That is to say, who can protect, implement, and enforce human rights in cyberspace, if government authorities end at their state borders?

In 2013, the issues of cyber espionage and misuse of private data came about through the NSA affair between the United States, Germany, and Brazil. The former NSA contractor, Edward Snowden, revealed the U.S. government’s warrantless and limitless surveillance of U.S. citizens and Internet users around the world. The United States is now charging Snowden under the U.S. Espionage Act, but Snowden remains in exile in Russia while the U.S. government works on extradition. Snowden’s revelations continue to strongly impact the debate about privacy and its insufficient legal development and heavily violated laws. Even though the UN, the EU, and many nations extensively fine-tuned their laws and regulations on data protection in 2013, the main issue remains unresolved: how can privacy and freedom rights be safeguarded in cyberspace, if at all? Individually, many users started to adapt and become more cautious. Consequently, self-censorship by users could not be avoided and many sensitive communications no longer take place online. Facebook users have become alarmed at posting private pictures online, and millions of users no longer send their e-mails unencrypted. The need for technical tools such as encryption and deciphering technology are highly demanded. In Europe alone, the number of encrypted data transferred rose in 2014 from 1.5% to 6.0%. Yet overall Snowden’s revelations demonstrated that the problems of global surveillance – conducted by most NSAs in this world – need global answers, not just national or regional ones, let alone technical ones. The many national laws passed over the past year regarding data protection can only create more time, but not deliver the solution. Meanwhile, private, govern-

Snowden’s revelations demonstrated that the problems of global surveillance – conducted by most NSAs in this world – need global answers, not just national or regional ones, let alone technical ones.

U.S. government works on extradition. Snowden’s revelations continue to strongly impact the debate about privacy and its insufficient legal development and heavily violated laws. Even though the UN, the EU, and many nations extensively fine-tuned their laws and regulations on data protection in 2013, the main issue remains unresolved: how can privacy and freedom rights be safeguarded in cyberspace, if at all? Individually, many users started to adapt and become more cautious. Consequently, self-censorship by users could not be avoided and many sensitive communications no longer take place online. Facebook users have become alarmed at posting private pictures online, and millions of users no longer send their e-mails unencrypted. The need for technical tools such as encryption and deciphering technology are highly demanded. In Europe alone, the number of encrypted data transferred rose in 2014 from 1.5% to 6.0%. Yet overall Snowden’s revelations demonstrated that the problems of global surveillance – conducted by most NSAs in this world – need global answers, not just national or regional ones, let alone technical ones. The many national laws passed over the past year regarding data protection can only create more time, but not deliver the solution. Meanwhile, private, govern-

In response to these and other revelations, the UN Special Rapporteur on Freedom of Expression Frank de la Rue highlighted the fact that privacy and freedom of expression are interlinked and mutually dependent. Therefore, without adequate legislation and legal standards to ensure the privacy, security, and anonymity of communications,
GOOD CYBER GOVERNANCE

Journalists, human rights defenders, and whistleblowers, it cannot be assured that their communications will not be subject to states’ security uses. Efforts to tame cyberspace and establish overall rules and regulations to which we should all adhere is as old as the cyberspace and Internet itself. In 1996, Jon Perry Barlow published the “Declaration of Independence of Cyberspace,” indicating the situations and controversies that today’s Internet users worldwide are worried about. Barlow recognized 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 is the foundation for realizing human rights. Whether or not such social contracts for cyberspace will ever be realized, the idea behind them is individual responsibility and adherence to human rights, which we, as members of the global community (whether private or public), have long agreed to. So-called ‘digital rights’ are already embedded in freedom rights, such as those stated in the Universal Declaration on Human Rights (UDHR) or the International Covenant on Civil and Political Rights (ICCPR). These rights allow the access and use of information and communications technology, like computers and digital media, to enhance any of the aforementioned human rights and the overall human right to information. Consequently on December 10, 2013, the International Human Rights Day celebrated 65 years after the UDHR was proclaimed by the UN, over 500 writers and Noble Prize winners signed a petition urging the UN to draft an international bill on digital rights. The massive support from the user community to develop such a concept is expected to impact the development of global Internet governance principles.

Internet Governance Principles and the Multi-stakeholder Approach. In April 2014 in Sao Paulo, Brazil, various international organizations and stakeholders promoted the concept of Internet governance principles based on the multi-stakeholder approach. It promotes and protects the use of cyberspace and the Internet as a “platform for social, economic and human development and a catalyst to exercise human rights of all people of the world.” This approach requires the inclusive participation of all relevant actors, institutions, and organizations that deal with cyber governance. This can be a set of different private and public actors, such as Google, Yahoo, Facebook, the International Telecommunication Union (ITU), and governmental representatives and experts. This multi-stakeholder approach – if applied thoroughly – has the advantage that all relevant actors can participate and be heard on an equal basis. They not only vote or decide on subject matters together, but they also commit themselves to the successful implementation of the agreed subject matters. Ideally, they set their own standards and rules, defining possible repercussions or penalties for non-compliance by the involved stakeholders. Enforcement still relies heavily on cooperation with state actors, such as national security agencies, but can also be conducted by private actors through means of public ‘cyber-pressure’, utilizing naming
and shaming tactics which may threaten the legitimacy of the respective company, state agency or otherwise. It will not fully replace state agencies -- and it never will -- but it leads more to individual and corporate responsibility. All actors involved jointly monitor, safeguard and enforce the jointly agreed rules and regulations. The 2005 World Summit on the Information Society’s Tunis Agenda indicates some of the criteria for the multi-stakeholder approach. One example is whether member states and Cyber Security Organizations (CSOs) can call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, through adoption of legislation, the implementation of collaborative frameworks, best practices, and self-regulatory and technological measures by business and users. They attach great importance to the multi-stakeholder implementation of decisions, which is explicitly mentioned in the Agenda.16

Regimes and organizations governed only by governmental stakeholders will lose legitimacy and thus effectiveness over the long run because they do not include citizens, companies, and organizations that struggle with applying human rights to cyberspace. During the 2012 UN governmental-run ITU world summit, authoritarian regimes often outnumbered democratic ones. As a result, they undercut the flexibility of the “multi-stakeholder” approach. Votes during these types of meetings disadvantage “democratic” governments, because democratic regimes are accountable to their electorate, whereas authoritarian ones often represent the interests of a small group of elites only, but not general citizens and Internet users in their country.17

Furthermore, good cyber governance requires free, open, and easy access for all citizens globally, although less than 30% of world population has regular access to the Internet. Recent statistics show that countries with high levels of social capital and technical infrastructures use E-Governance to run business or public affairs mainly through the Internet, unlike countries with fewer infrastructures.18 In particular, E-Democracy that aims to have Internet-based general elections requires equal, safe and free access for all citizens under each respective political regime. The aim of inclusive participation via Internet can result in common agreements, norms, rules, and laws to govern communities. Countries that have high E-Democracy scores are also democratically mature in general.19 Yet there is no evidence found that E-Democracy leverages democratic behavior in countries that generally score low in democracy or are governed in an autocratic manner. Because E-Democracy is just one way to build on already existing good governance principles such as accountability and responsiveness, transparency, and Internet citizen participation, there is no automatic causality between Internet access and democracy. But access to Internet, which enhances access to information and civic participation, can be a tool or catalyst to trigger cultural changes that eventually lead to more democratic ways to govern a society.

The core question remains, whether or not people can develop trust and confidence in these Internet tools that in return leverage the legitimacy of
institutions or organizations that provide them — may they be public or private. In order to draw a correlation, we take a look at the general definition of democracy: the rule of the people for the people, which also describes the concept of rule of law as the basis for any democratic regime today. It becomes evident that cyber–technology, search engines, network providers, etc., can be used as tools or catalysts, but do not automatically lead to a democratic culture or country. Nonetheless, everyone who moves in cyberspace has the responsibility to protect and respect private data and freedom of information. We need common rules and standards, as well as strong decision-making, enforcement, and compliance mechanisms to realize good cyber governance. Internet users, providers, companies, and governments alike should be held responsible for both violating rights and protecting them.

Human Rights and Rule of Law.
Governmental authorities and democratic institutions are instrumental to safeguarding human rights in cyberspace. National and international courts also play a crucial role as part of this cyber regime to protect human rights. In a 2012 case concerning Turkey, the European Court of Human Rights (ECHR) reinforced the right of individuals to access the Internet by ruling against wholesale blocking of online content, asserting that the Internet has now become one of the principal means of exercising the right to freedom of expression and information. In October 2013, the ECHR ruled that an Estonian news portal, Delfi, was responsible for offensive anonymous posts against a ferry company. Previously, Estonia’s Supreme Court ruled that the website owner was responsible for the comments, not the people who made them. The judges in Strasbourg backed that stance in 2013. This means that service providers or website owners will be held accountable when their users or visitors post inappropriate language on their websites that violates the dignity and privacy of others. This has subsequently led to more surveillance and responsibility of owners on what is posted on their websites.

Legitimacy of any institution, company, or organization is achieved through the level of civic engagement or interaction in setting up, adhering to, or accepting common rules and standards. It increases or decreases by the level of Internet users’ trust in or engagement with these entities. The more these entities comply with its commands and human rights, the higher their legitimacy will be. Therefore, these entities will enjoy a greater degree of legitimacy when applying good governance principles in businesses, governments, and CSOs, both online and offline.

In the case of cyberspace, globalization and constructivist approaches help us understand why some argue that human rights norms diffusion impacts the way we think about national jurisdiction, state borders, and the nation-state. The global cyber governance regime is legitimate and sovereign if we interact on different levels. The International Court of Justice (ICJ) has argued that territorial sovereignty also implies obligations to protect human rights in cyberspace. For example, if technical companies or servers violate
human rights, they would be subject to national human rights laws, because even cyberspace requires the existence of some physical architecture. In response to the debate on whether Internet can weaken or strengthen sovereignty and legitimacy of state institutions, UN Special Rapporteur de la Rule of Law recommended states review national laws regulating surveillance and update and strengthen laws and legal standards. Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundation of a democratic society. Legislation must stipulate that state surveillance of private communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority.

**Legislation must** stipulate that state surveillance of private communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority.

**Good Cyber Governance.** Ultimately, human rights-oriented cyber governance is a new trend in which global Internet users aim to uphold their basic human rights through good cyber-governance principles. Yet there is no global rule of law culture in cyberspace as of yet, let alone any monitoring or enforcement mechanism based on the multi-stakeholder approach that would safeguard the rights of Internet users. Equal and universal legal standards are missing; thus, the claim for rule of law is one to be considered. International jurisdiction, customary and international human rights law, and the shifting role of duty bearer and rights holder towards more individual responsibility are all part of the recent development towards an open and fair cyber governance regime.

While there is no lack of human rights standards or laws, the measures and mechanisms that allow us to comply and adhere to these standards are national, not global. This is where change has to take place. Therefore, the global cyber regime has to develop innovative ways and mechanisms to monitor and enforce global human rights standards that go beyond existing national measures. There might be different ways to do so without excluding existing legal or political mechanisms.

One suggestion that has been proposed in this article is the multi-stakeholder approach. The multi-stakeholder community of organizations, governments, and experts ought to frame existing common global guidelines and laws for the needs and purposes of Internet users. This might more likely guarantee the inclusion of the public Internet users and the protection of our privacy; namely, our civic and social
human rights. A non-legally binding UN Resolution from December 2013 or the Internet governance principles promoted at NETMundial in Sao Paolo in 2014 indicate that governments emphasize preventing illegal surveillance and interception of private communications, and the illegal collection of personal data. These highly intrusive acts violate the right to privacy and freedom of expression and may threaten the foundations of a democratic society. With UN resolution 192, member states recall their own obligations to ensure that measures taken to counterterrorism or other security threats comply with international human rights law. Therefore, all governments of the world, in theory, aim to put an end to violations of these rights, and they are called to establish multi-stakeholder mechanisms with independent oversight, capable of ensuring transparency and accountability of state surveillance and interception of private communications and collection of personal data. It is vital to produce this new rule of law in cyberspace.

NOTES

3 Internet Governance Forum http://www.intgovforum.org/cms/
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, 17 April 2013, para.79.
17 Multi-stakeholder approach for cyber-security, read more at http://www.project-syndicate.org COMMENTARY/joseph-s--ney-contrasts-multilateral-
and--multi-stakeholder--approaches-to-governing-cyberspace#3tH1ru7slfTo2Qsf.99
20 ECHR, Case Yildirim v.Turkey, 18 December 2012, para.54.
21 ECHR, Case Delfi As v. Estonia,10 October 2013.