Towards an Internet Free of Censorship II

Perspectives in Latin America

Agustina Del Campo
Compiler

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información

CELE

UP
Universidad de Palermo

Towards an Internet Free of Censorship II

Perspectives in Latin America

Agustina Del Campo
COMPILER

Facultad de Derecho
Centro de Estudios en Libertad de
Expresión y Acceso a la Información

CELE

UP
Universidad
de Palermo

Contents

Foreword

The development of the internet brings about new opportunities, challenges and problems that require creative solutions, capable of promoting further development, investment, sustainable growth, while fairly and squarely guaranteeing the rights of users. Regulation is among the State sponsored solutions to solving some of the new issues brought about by the development of technology and it must have a pragmatic problem solving approach while respectful of the fundamental rights of people.

Over the past two years internet regulation in Latin America has flourished and increased exponentially, diversifying the agendas of our lawmakers, policy makers and judges. One of the persistent challenges that they face is that issues grow increasingly complex as technology continues to develop, mutate and change, rendering long fought policy consensus sometimes obsolete, inadequate, or incomplete. Another important factor affecting internet policy development is the gobal nature of the internet. Since issues are common to the global landscape of the internet, local developments are imbedded in regional and global development processes. India's debate and regulation on zero rating, for example, affected discussions and debates on the issue worldwide. As other countries "test" different solutions we, the global community, benefit from trial and error experience, witnessing their benefits, challenges and shortcomings. One of the most paradigmatic cases nowadays is Europe's right to be forgotten, which has spilled over to non-European debates on privacy, data protection and freedom of expression.

In the midst of this ever-changing internet and its context, CELE intends to contribute technical inputs to the larger policy debates, studying and critically evaluating comparative experiences, analyzing the impact of certain policies on human rights, and, wherever possible, proposing means or tools to understand and think about regulation in a human rights respectful manner. Since 2010 at CELE we have been working on internet regulation and human rights, particularly freedom of expression and Access to information. In 2012 we published our first Towards an Internet Free of Censorship, a

compilation of articles written by renowned scholars and practitioners from Latin America and the United States. The objective was to identify the main issues under prospective regulation, offer different approaches towards them and contribute concrete recommendations for public policy in Latin America.

This new compilation of articles addresses some of the most salient issues within the Latin American legislative and regulatory agenda towards the internet. These are complex and thorny issues that have generated intense debate among scholars, legislators, practitioners, engineers, companies and users.

The first article, authored by Carolina Aguerre, analyzes internet governance and the different local models developed in Latin America to assess their efficiency and impact. The second article, by Daniel Alvarez Valenzuela, offers an introduction to cyber security, highlighting the need to incorporate a human rights perspective towards its development. The third and fourth articles address zero-rating. Luca Belli explains the deep connection between access to the internet and zero rating policies, and Arturo Carrillo proposes an analysis of zero rating under the Inter-American system's three part test: legality, necessity and proportionality. Last but not least, the fifth and sixth articles offer two different approaches to the "right to be forgotten". Daphne Keller analyzes the European Directive and its (in) application to the Latin American context and Nelson Remolina reviews and criticizes the jurisprudence on the issue from the data protection perspective.

The articles compiled gather different views and solutions for complex issues. The overall objective of the publication is precisely to contribute to the understanding of the different aspects and complexities of each issue so as to inform and nurture public debate, identify potential virtues and flaws among the different approaches, and collaborate towards the creation of sound public policies, necessary and proportionate to the needs they address, while respectful of human rights.

This book was developed and is being published with the support of the Ford Foundation. CELE wishes to acknowledge and thank all contributing authors, the translators and the team that worked on putting it together. We sincerely hope it contributes towards an improved discussion of internet policy and regulation on these and other related topics.

Agustina Del Campo

Chapter One

Internet Governance Networks at National Level. Experience of Recent Cases in Latin America

Carolina Aguerre[1]

Summary

This paper addresses the Internet governance mechanisms emerged in the past years in various countries of Latin America, such as Argentina, Colombia, Costa Rica, Mexico, Uruguay and Venezuela, taking the Brazilian case as the example. The literature on Internet governance is focused on conceptualising the relevance of the national dimension. These new spaces are considered as *policy networks* in transition towards national governance networks based on which a specific field of action is outlined. The paper addresses national cases, seeking to understand their variations, common aspects and possible consequences of the agreements that define Internet policies.

Introduction

Up until recently, Internet governance was a marginal topic in most of the political agendas of Latin America. Debates were limited to some specialised government agencies, a group of scholars and a few NGOs. But by

[1] Carolina Aguerre is professor of New Technologies at the Department of Social Sciences of the University of San Andrés and researcher at the Centre of Technology and Society (CETYS) of the same institution. She is also researcher at the University of Pennsylvania's Internet Policy Observatory. She holds a Ph.D. in Social Science from the University of Buenos Aires and a Master's Degree in Communication, Culture and Society from the Goldsmiths College, University of London. Her research lines are focused on Internet governance policies and development, including the deployment of new critical Internet technologies and infrastructure. She worked as executive director of LACTLD, the Latin American and Caribbean ccTLDs organisation, member of the IGF's MAG and of the LACIGF's Programme Committee. This article is an English translation of the Spanish original.

mid-2013, Snowden's revelations about mass surveillance on the Internet drastically changed the debate on the matter. At present, these matters are discussed both in the mass media as well as at some events, such as the *Netmundial* meeting in Sao Paulo in April 2014, which managed to gather the attention of State secretaries and ministers.

It is important to analyse the *Netmundial* meeting and the role of Brazil, since it is directly related to the purpose of this paper about the development of national mechanisms of Internet governance. This conference would not have been possible in that country without the support and expertise of the Internet Steering Committee (CGI in Spanish) and its multi-stakeholder approach of Internet governance. During 2013, the Brazilian stance as a global leader in Internet governance became an indisputable fact. No other state was able to express in such a compelling manner its discontent towards the ubiquitous surveillance scheme developed by the US National Security Agency (NSA)[2], or coordinate a high-level joint action by April 2014 with various players involved in the current setting of Internet governance. The purpose was to address the issue of open and secure Internet that ensures privacy and freedom of expression. The role of Brazil -understood as the Government but also as the various stakeholders, including the civil society, the Academia and the business sector of the country- as one of the leaders of the international debate on Internet governance policies, is neither surprising nor new if we consider not only its geopolitical dimension and several diplomatic strategies (including the "soft power"), but also the country's own background on Internet policies developed in the last two decades.

Brazil's leadership responds to the country's approach towards Internet governance in the internal front, based on multiple stakeholders who are part of the CGI, created in 1995, which has become a role model in the country and abroad, and also to the country's model of Internet resource management[3]. Among other results, this mechanism has allowed the country to facilitate coordinated responses from the Government and other players involved (civil society, business sector and universities) in the light of an external threat to Internet governance, such as the actions perpetuated by the NSA. In turn, it enables the country to coordinate processes such as the *Marco Civil* of Internet (Civil Rights Framework for the Internet), established in 2009 to promote a basic platform of principles for the use and governance

[2] United States National Security Agency (NSA). The NSA used a programme called PRISM to monitor data of millions of citizens and governments all over the world.

[3] These are the domain names, IP addresses, the IXP coordination, among others.

of Internet. According to the Marco Civil rules, which were completed in 2016, the CGI was appointed as the agency responsible for monitoring the implementation of this law[4].

However, since late 2012, several initiatives came up in Latin America and the Caribbean, taking into account the policies and governance of Internet as the main working line, just like the CGI. Besides Brazil, more recent developments of national mechanisms are found in the following countries: Argentina, Colombia, Costa Rica, Mexico, Paraguay, Peru, Dominican Republic, Uruguay y Venezuela. The emergence of Internet governance on the political agendas of various countries of Latin America raises several questions that this paper intends to answer: Which are the institutional elements? Which players are represented and how? What goals do they pursue and what have been their results? To what extent are other institutional models replicated? How do these initiatives integrate with other international and regional forums for discussion?

A fundamental premise of this work is that these mechanisms were built on the basis of *policy networks*, defined as "more or less stable patterns of social relations between mutually dependent actors, which form around policy programmes"[5]. The image of a *policy network* is that of a space for stakeholders' frequent exchange, leading to stable relations among them. According to some authors, this encourages the mutual coordination of interests around specific policy domains[6].However, over time, these policy networks of Internet increasingly turn into "governance networks" which, at institutional level, emerge as a result of specific incentives and tend to get formalised[7].

In turn, Peters[8] identifies four governance mechanisms, which he labels as "shadows" to describe the authority behind each of the governance networks

[4] The CGI's growing prominence has been challenged by President Temer's caretaker administration and by the telecommunication carriers, reinforcing the importance acquired by this agency in relation to the Internet policies and development in the country, while it threatens other economic and political interests that are questioned by a more decentralized and open approach as is the Internet.

[5] Kikert, 1997, p. 6 (*cited on:* Blanco, I., Lowndes, V. and Pratchett, L., *Re-Organising Babylon: on the Meaning of Policy Networks and Network Governance and their Democratic Consequences*, paper prepared for the "Governance Networks: Democracy, Policy Innovation and Global Regulation", Conference, Roskilde, Roskilde University, 2-4 December, 2009, p. 6).

[6] Adam, S., and H. Kriesi, "The Network Approach", en P. A. Sabatier (ed.), *Theories of The Policy Process*, Boulder, Colorado: Westview Press, 2007.

[7] Blanco, Lowndes and Pratchett, L, *supra* note 5.

[8] Peters, B. Guy, *Governing in the Shadows*, SFB-Governance Lecture Series, No. 3, DFG Research Center (SFB) 700, Berlin, 2010. Available at: http://bit.ly/2ejlPum

currently emerging. These are the "hierarchies", understood as the state bureaucratic level; the "markets", a mechanism based on the power of the big organisations or market forces (such as drug-trafficking); the "society", defined as the social networks coming from the civil society, and a fourth mechanism identified as the "knowledge" of experts (related to the concept of "epistemic communities"[9]).

The work is structured in three parts. The first part characterises Internet governance as well as the fundamentals and principles underpinning the national processes in this area. The second part elaborates on six national cases (Argentina, Colombia, Costa Rica, Mexico, Uruguay and Venezuela), taking into account the Brazilian experience with the CGI. This last case has been thoroughly analysed, and will be used as reference framework since it has been the first national process of Internet governance and policies since 1995. Finally, the last part addresses a compared analysis and offers recommendations.

I. Characterising Internet Governance

Internet governance is an elusive concept, which has been characterised as an "inkblot on the Rorschach test"[10], since the various stakeholders express their motivations and expectations when describing it. While some consensus exists after the World Summit on the Information Society (WSIS) and the Tunisia Agenda (2005), the issue still remains ambiguous and controversial: "The development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet". This definition of Internet governance is related to the definition of regime in international relations as "a set of implicit or explicit principles, norms, rules and decision-making procedures around

[9] According to Haas (Haas, P. M., "Introduction: Epistemic Communities and International Policy Coordination", in *International Organization*, 46(1), 1992), an epistemic community is a network of professionals with recognised expertise and competence in a particular domain or issue-area. Although epistemic communities may consist of a variety of disciplines and backgrounds, they have a shared set of normative and principled beliefs, notions of validity and causality and a common policy enterprise.

[10] Drake, William J., "Reframing Internet Governance Discourse: Fifteen Baseline Propositions", p. 1. Paper based on presentations at the *Workshop on Internet Governance*, International Telecommunication Union, Geneva, February 2004; and the *United Nations ICT Task Force Global Forum on Internet Governance*, New York City, March 2004, available at: http://bit.ly/2fQlfW6

which actors' expectations converge in international relations"[11], which in turn follows the institutionalist shift adopted by that discipline.

The WSIS' definition of Internet governance has exerted a remarkable influence on the framework of international policies, but entails a normative, and descriptive rather than analytical nature. It does not account for the emerging process that has been characterised with the development of this technology on the part of specific communities, where such development and the uses of technology determine or, at least, condition these roles, principles and norms. This second approach of governance seems to be more related to the socio-technical perspective.

However, beyond definitions, the research studies on Internet governance have focused on the global side of the issue, and on the conformation of the international regime, deemed as the "dominant agreements"[12]. It is true that Internet is a borderless technology, but its global side overshadows the various orientations of the national dynamics and the diverse capacities deployed by the actors in their territories for more than two decades since the growth of Internet. The complexity of Internet requires a deep understanding of how it works and of the sophisticated governance strategies on the part of the stakeholders involved. This argument involves strategy and policy experts in the subject-matter, whose decisions are based on scientific and technical knowledge, for instance, from the technocratic perspective[13] and/or the governance of experts[14].

Besides approaching the issue of Internet from the viewpoint of the stakeholders and international agreements, another possibility is to do so by recognising the degree of imbrication between the technical and political aspects of this technology[15]. The classical socio-technical arguments such as Bijker's[16] claim

[11] Krasner, Stephen, *International Regimes*, Palo Alto, Stanford University, 1983. Own translation.

[12] Keohane, Robert and Nye, Joseph S., *Power and Interdependence: World Politics in Transition*, Boston, Little, Brown and Company, 1989.

[13] Centeno, Miguel Angel and Wolfson, Leandro, "Redefiniendo la tecnocracia", in: *Desarrollo Económico*, No. 37(146), 1997, pp. 215-240.

[14] Hall, Peter A., "Politics as a Process Structured in Space and Time", annual meeting of the American Political Science Association, Washington D.C., 2010.

[15] Drake, *supra* note 10; Solum, Lawrence B., "Models of Internet Governance", in: Illinois Public Law Research Paper Nº 07-25, Illinois, 3rd September, 2008, p. 48-91, available at: http://bit.ly/2eBliPK; DeNardis, Laura, *The Global War for Internet Governance*, New Haven, Yale University Press, 2014.

[16] Bijker, W. E., "Sociohistorical technology studies", en S. Jasanoff, G. E. Marsh, J. C. Petersen, & T. Pinch (Eds.), *Handbook of Science and Technology Studies*, Sage Thousand Oaks, 1995.

that the technical decisions are immersed in the social and institutional context where they were created and embedded. In this line, the WSIS (2003-2005) openly questioned the institutional legitimacy of the first governance agreements, which were decontextualized and distant from the interests of stakeholders from countries which were not involved in the origins of this technology. It also emphasised the policies derived from the decisions made at forums such as the Internet Corporation for Assigned Names and Numbers (ICANN) and other technical meetings. The WSIS put on the table the institutional design and the roles assigned to the various players of Internet governance, including the recognition of a multi-stakeholder governance as a fundamental principle of all processes. According to the characterisation made by Jupille and Snidal[17], the WSIS opened the door for the debates on the "use", "selection", "reformulation" and "change" of the existing institutional agreements. The WSIS also expanded the debate on the Internet governance agenda, transcending technical and institutional matters of Internet to include issues related to human rights and the development dimension. For this reason, the Internet governance agenda at present is quite diverse and requires the involvement of various experts and sectors to encompass this whole spectrum of topics.

The need to delimit the scope and the focus of national policies -even when they still are at an incipient stage- had already emerged during the Internet boom with the delegation of top-level domain names and IP address blocks in the second half of the 80s and early 90s. The development of local capabilities in relation to Internet as well as the stable mechanisms of national coordination and participation at international forums also defined the responsibilities of national actors from the public, private and scientific fields.

It must be noted that the inclusion of developing countries in the mechanisms of Internet governance was considered by the Working Group of Internet Governance (WGIG) and by others, of vital importance to ensure the progress and legitimacy of the process[18]. Besides, these authors emphasise the further creation of national mechanisms for participation as a precondition for relevant involvement at international fora. The WGIG also offers a significant

[17] Jupille, J. and Snidal, D., "The Choice of International Institutions: Cooperation, Alternatives and Strategies", in: *American Political Science Association annual meeting,* Washington, D.C., September, 2005.

[18] Siganga, Waudo, "The Case for National Internet Governance Mechanisms", in: Drake, W.J. (ed.), *Reforming Internet Governance: Perspectives from the Working Group of Internet Governance (WGIG)*, New York, The United Nations Information and Communication Technologies Task Force, 2005; Afonso, C.A., *Gobernanza de Internet: un análisis en el contexto de la CMSI*, Montevideo, ITeM, 2005; Drake, *supra* note 10.

approach for this work, highlighting four recommendations on Internet governance mechanisms: forum function, global public policy and oversight, the institutional coordination, and regional and national coordination.

Kaul, Grunberg and Stern[19] identify three gaps which pose challenges to the implementation of public policies aimed at providing global public goods. These gaps, which have prompted concerns related to the legitimacy and representativeness of the Internet governance processes in the last decade, are the following: a) A jurisdictional gap observed in the discrepancy between the global boundaries of today's major policy concerns and the essentially national boundaries of policy-making; b) A participatory gap which results from the fact that despite the growing institutionalisation of the involvement of non-governmental actors in international cooperation, they still face representation and legitimacy problems in many international forums, particularly when they are from less developed countries. According to the authors, the advantage of including these actors would be that by giving them greater participation, the Governments could have greater support for decision-making and could promote pluralism and diversity. This argument favours the multi-stakeholder participation processes of a large part of the Internet governance processes, and c) an incentive gap to control the effects of the countries' actions on the global public goods because moral suasion is not enough. Up until recently, and in particular due to the impact from Internet "scandals" in the last years, few national stakeholders perceived the issue as a need or a problem, since global forums and the spaces for international policy-making were not among their priorities. The national mechanisms addressed below consist of examples which may be useful to close these gaps.

At national level, up until not long ago, few countries had mechanisms for the development of Internet policies. This does not mean the absence of a long-running background of incipient involvement in the matter and the regulation on several aspects (related to content and infrastructure mainly). But the spaces for the development of Internet policies were less defined.

II. Internet Governance: national cases in Latin America

The case studies selected are addressed below. Each case sets the context for the Internet background in the country from its origins, proving for many of them, especially Brazil, Costa Rica, Mexico and Uruguay, that the

[19] Kaul, I., Grunberg, I., & Stern, M. A., *Global public goods: international cooperation in the 21st century*. Oxford University Press, 1991.

pioneers who have introduced and operated this technology are involved in the new, emerging mechanisms.

II.A. Argentina

As many of the countries of Latin America and Europe, Argentina started performing activities related to IT networks when Internet was introduced in research and academic institutions. In terms of the adoption of Internet protocols, by 1991 Argentina was already connected to the largest international networks, including Internet among others[20]. However, the Internet growth started to gain momentum when the international communications market was opened in 1997. Up until then, although the telecommunications market opened in 1990, the domestic market was characterised by an oligopoly and a monopoly through the TELINTAR group, composed of TELECOM and Telefónica for international communications.

The efforts from the so-called "Internet pioneers" to achieve connectivity into international communications at an affordable price entailed a tough battle but highly influential to define what might be considered the "spirit of Internet" of these new and emerging stakeholders. They included actors from the academic field, such as the Computing Department of the School of Exact and Natural Sciences of the University of Buenos Aires, the RETINA academic network, and the actors related to the emerging business sector, which were different from telecommunication providers and grouped under CABASE -the chamber of the incipient sector- in 1989.

As for relations with international processes, it was only when the WSIS gathered in 2003 that government actors showed a more proactive attitude towards the global Internet regime. The Internet political agenda focused on aspects of deployment and adoption of new technologies, including poverty and the socio-economic gap rather than the political aspects of the international regime. However, this began to change after the meeting in Tunisia. Argentina sent there a large delegation to the WSIS and gained a high regional profile at the conference. But this meeting had little impact on institutional mechanisms and on domestic policies, except for raising the need to follow up these matters on the part of some Government sectors, particularly within the Foreign Affairs Ministry. The actors involved in the various layers of Internet policies in the country still based their actions on

[20] Other known networks competing with Internet at that time included BITNET, UUCP and Usenet.

informal coordination mechanisms after many years of joint work.

In the past five years, changes have emerged from a particular view about the role of the State in many policy areas of the country, especially in the sectors related to public goods and services where the State participates not only through regulation but also as a communication service provider. Some of the examples that illustrate this situation include the National Plan *Argentina Conectada* (Argentina Connected) of 2010, when public investment was made for the deployment of an optical fibre network that expanded the country's main networks. Another example is ARSAT, a company created by the State in 2006 to develop satellite communication services. With the digitalisation of the spectrum and the implementation of the *Argentina Conectada Plan*, ARSAT became the telecommunications provider. The last example derives from the role of the Digital Argentina Act passed by Congress in December 2014 and partially revoked by the new Administration in December 2015, and from the creation of the Ministry of Communications, following the Colombian experience in the matter, which will be addressed below. This ministry assumes the various communication functions discharged by several bodies, and the same Decree that created it (267/15) also gave way to the new regulatory entity -the National Communications Entity (ENACOM). Despite the differences between a project such as Argentina Digital, its enforcement and regulatory body called AFTIC, and the recent creation of a Ministry of Communications and ENACOM, the State shows an attitude of growing intervention and interest in the matter, confirmed in April 2014 when the Secretariat of Communications called on the short experience of the Argentine Commission on Internet Policies (CAPI)[21] . However, it is still premature to deepen into an analysis in this line and the implications for Internet and governance, considering not enough time has yet passed and the announced Convergence Act that is expected to legally frame the process.

More specifically, in the case of Internet governance in the country, with the change of Government in late 2015, a Ministry of Modernisation was created to address the subject-matter by its various bodies. For its part, the Secretariat of Innovation and Public Administration created the National

[21] This Commission was created by means of a resolution (Res. SECOOM 13/2014) and was composed by government agencies with the primary purpose of improving coordination within the State, and although the attempt was made to start a multi-participatory governance process, the Digital Argentina Act ended up blocking the attempt.

Office for Internet Policy and Development[22], whose purpose is to represent the national State in international forums on the matter, and design and develop Internet governance policies at national level. In this manner, the subject was installed in the national public agenda and got institutionalised within the State, but following a classical consolidation process which was part of a bureaucratic context. Just like with the new Ministry of Communications and the regulatory entity (ENACOM), it is still too soon to consider the effects of this Secretariat and the National Office on the national governance mechanisms with other non-governmental actors.

Finally, the Argentine case also includes an incipient national forum on Internet governance with the creation of the first Argentine Dialogue for Internet Governance held in October 27, 2015. This mechanism was consolidated based on the participation of various stakeholders -civil society, government, technical and business community- within the framework of electronic debates and meetings to discuss heated regulatory and policy issues related to Internet and new technologies. The emergence of informal relations resulting from these forums for discussion among stakeholders, who also participated in international processes and meetings within the framework of ICANN, Internet Governance Forum (IGF), Latin American and Caribbean Internet Governance Forum (LACIGF), LACNIC and WSIS, encouraged the group to organise a national forum, following the experiences of other regional spaces, remarkably the *Grupo Iniciativa* in Mexico, which will be discussed below, and has already organised two Mexican Dialogues on Internet Governance.

The institutional entity assumed by the organising group of the Dialogue in Argentina is a multi-sector committee with the involvement of all stakeholders in the traditional sense of Internet governance, composed by nine people from the various sectors[23]. The organising group opened a call for participants to create an agenda-setting committee for the first event. For that, an open meeting was organised to define the main topics, including a period for public comments based on a Web form to finally come to a definitive agenda. Stakeholders from all sectors were present at the Dialogue, constituting the first experience which would be replicated in 2016, but this

[22] The under-secretariats that report to the Ministry of Modernisation were created upon the Administrative Decision 232/2016 of March 29, 2016. Available at: http://bit.ly/1pKRENB

[23] One of the members representing the academic sector in the discussion is the author of this paper.

time with a more formalised format and under the name "IGF Argentina"[24]. One of the main consequences of this Dialogue was to materialise the issue on the public agenda, which was resumed by many of the participants who, after the elections, assumed government offices that are currently addressing these topics, as is the case with the Ministry of Modernisation.

In summary, since April 2014 and Argentina's participation in *Netmundial*, Internet governance in Argentina has become a clearer priority for the State through various mechanisms (many of them of short duration). The other stakeholders who have historically performed a *de facto* Internet governance for being resource, technology and standards operators in the country are still in the process of consolidating their actions, and the first edition of the Dialogue in 2015 constitutes a clear signal for the definition of a *policy network*. The most remarkable aspect in terms of more recent institutional mechanisms in the country relates to the interpretation made by the State of the need to create greater coordination and promote knowledge to intervene more effectively in this environment.

II.B. Costa Rica

Costa Rica presents a tradition of networking initiatives, and was the first Central-American country to be connected to the Internet in 1993. These efforts were the result of scientific endeavours and of two organisations involved in the development of Internet and telecommunication infrastructures in the country -RACSA and ICE. In institutional terms, those endeavours began at the University of Costa Rica, which participated jointly with other Central American universities in the development of a regional network[25]. Additionally, Costa Rica was the first country in the region to develop an exclusive IP backbone in 1993, and one of the few countries in Latin America whose telecommunication systems remained under the State's orbit (ICE was a state-owned monopoly until 2008). This last characteristic together with the development of its own technology, within the framework of university research centres, allowed for an Internet deployment independent from the

[24] At the time of completing this work in July 2016, the organising group of the Dialogue called a preparatory meeting on July 19 for the IGF Argentina to set up a programme committee selected by members of the various sectors.

[25] Siles González, Ignacio, *Por un sueño en.re.dado. Una historia de internet en Costa Rica (1990-2005)*, Montes de Oca, UCR, Institute for Social Research, 2008.

interests of the large international groups[26]. Even when the public telecommunications monopoly ended in the country, the government sector was still present in Internet matters, as we will see later in relation to the development of specific national mechanisms for the development of Internet policies.

In 2012, Costa Rica hosted the ICANN 43 meeting. Former President Laura Chinchilla's opening address aimed not only at improving the Internet characteristics in her country, but also at enhancing the characteristics of the global digital environment. That same year, the Internet Governance Council of Costa Rica (CCI in Spanish) was created and organised by "nic.cr". This body (".cr" domain administrator) is part of the National Academy of Sciences of that country and, both organisations have had a long history of being involved in Internet development in Costa Rica. The CCI was convened under the organisational umbrella of the ".cr" to create a platform for the discussion of the most relevant aspects of Internet development in that country. Some of the topics addressed include a national broad-band plan, a Universal Access Fund and the development of the first IXP established in 2014. Its formal objectives are to participate in policy recommendations for the "nic.cr" and the deployment of Internet to meet the country's development goals.

As for the CCI composition, while it is a multi-stakeholder body, with representatives from government agencies, scientific institutions, NGOs and businesses, most of its members are government and state entities. In this manner, while the principle of multi-stakeholders is the basis of its operational practices, the CCI is government-oriented.

Although the CCI does not produce any formal documents, nor does it establish nation-wide stances on a particular issue -as is clearly the case of the Comitê Gestor de Internet do Brasil, "CGI.br"-, it is a platform for the discussion and validation of initiatives, especially led by the ".cr" in the technical aspects. As for the working modality, most meetings are held in online format in the various working groups which are part of the CCI: national Internet policies, Internet security, educational network, cybercrime, infrastructure and promotion of the ".cr" domain, although face-to-face meetings are held every six months.

The "nic.cr" had previously analysed the initiative carried out by the national domain registries of Mexico (".mx") and the "CGI.br", and its operating arm, the "nic.br", before calling on the CCI. The latter is not as formal

[26] Téramond, Guy F., "Interconexión de Costa Rica a las grandes redes de investigación Bitnet e internet", on *Ideario de la ciencia y la tecnología: hacia el nuevo milenio*, San José, Ministry of Science and Technology, 1994. Available at: http://bit.ly/2fDHbz2

as the Brazilian experience and, unlike the Mexican experience -which will be later analysed-, participation is subject to institutions, and not to people. According to a SUTEL (regulator) representative, who participated in this initiative, had there been more formal mechanisms in place, tensions would have existed with those bodies that are not currently part of it. The potential to open up to new players is a relevant dimension, since players that are not currently part of this body may question its legitimacy.

In relation to its mission and objectives, there are various opinions depending on whether actors come from the government sector or not. As to the former, the CCI represents an informal space for learning, sharing experiences and receiving input for policy-making processes. For the other actors, it constitutes a space of governance.

The experience of the CCI in Costa Rica exemplifies an effort to formalise a policy network for the production of concrete results in the technical aspects of Internet governance, that have already produced concrete results, as is the case with the ".cr" domains, the launch of the first IXP in 2014 and the development of cybersecurity training modules. Despite this body's non-binding nature, the government's participation in this initiative constitutes a validation of other mechanisms for the development of Internet policies and governance in that country.

II.C. Colombia

Just like in other countries in the region, the origins of Internet in Colombia relate to the academic sector. In 1991, Jon Postel -then Manager of the Internet Assigned Numbers Authority (IANA)- passed the administration of the Colombian domain onto the University of Los Andes. Also, just like in other countries in the region, the 90s marked the beginning of the liberalisation of the telecommunications market, until then operated by one single government player and its national telecommunications company, TELECOM.

But, unlike other regional cases, Colombia has a converging vision of communications, even prior to the digital era, as the Ministry of Communications was already created in 1953, grouping the post, telecommunications and giro transfer services. Since then, and more specifically with the development of Internet in the country, whose boom was in 1998 and 1999, the Ministry began to intervene in order to favour the adoption of Internet among citizens. This Ministry finally changed its name in 2009 under Law No. 1341, and is now called Ministry of Information and Communication Technologies. The purpose of this law is to create a regulatory framework

for the sector's development, open ICTs to everyone, boost competition and reinforce users' rights.

A characteristic aspect of the origins of Internet in Colombia was the long process between 2002 and 2009, when the Ministry of Communications, and then the MINTIC, began to regulate the country code registry until the domain operation was finally transferred from the University of Los Andes to CO Internet SAS, under the Ministry's guidance. This event, just like other regional cases where there was a fight for Internet resources, entailed important consequences for the establishment of a national governance process, due to the awareness and special interest awakened on the matter, thus outlining a specific theme and political field.

The fifth edition of LACIGF held in Bogotá, in 2011, led to the first interactions among a diverse group of actors involved in the matter in the country. The actors that were part of that informal dialogue were motivated to exchange their views prior to an event, or in relation to a specific topic of relevance. The "*Mesa Colombiana para la Gobernanza de Internet*" (Colombian Round Table for Internet Governance) group was made up of multiple players with representatives from the civil society, the government, academics, the technical community and the private sector at the sixth LACIGF in Córdoba. Since then, the group held regular informal meetings until the first forum on Internet governance was carried out in Colombia, in November 2014, at the Xavierian University of Bogotá, and the second one in September 2015 at the Tequendama Hotel in the same city.

The *Mesa Colombiana de Gobernanza de Internet* is an open space that welcomes more players. It has a stable secretariat and list of participants, representing the academic, private (five), government (two) and the civil society (six) sectors. However, while the academic sector has a space destined to its representatives, the involvement of this player is lagging behind due to the lack of own incentives, even though participants *do* attend the meetings. The presence of Internet pioneer players in this table is remarkable. They represent several sectors, evoking the metaphor of a policy network on its way to consolidate a governance network. In line with its operational format, the Colombian round table has five central themes (Internet for poverty reduction, neutrality, Internet governance, cybersecurity and cyber defence, and freedom of expression) that make up its agenda, though current matters are also analysed. The group also has multi-platform coordination and dialogue mechanisms (mailing lists, teleconferences, etherpad) apart from the on-site bimonthly meetings, for which the corresponding minutes are drafted. This area-by-area working modality, jointly with the possibility

of constant interaction and the production of specific documents related to the various topics assessed by the Table, is one of the most relevant deliverables of this initiative.

Due to the openness, the possibility for multistakeholders to be equally involved and the development of the work agenda, the experience of the Colombian Round Table is in line with several principles outlined under the WSIS and the IGF frameworks, as well as the working methodologies seen in other organisations, such as ICANN or the Internet Engineering Task Force (IETF). The coordination with other regional spaces –as was the case at the beginning of this process within the framework of LACIGF, and with the international arena- occurs as a result of the participation of these players in those instances.

II.D. Mexico

By the early 90s, the Internet network infrastructure in Mexico was one of the best regional scenarios, where three academic networks provided service to users in three of the highest populated areas in the country. These efforts had the initial support of the government, but later on were increased and then started competing for funding[27]. At that time, there were several actors involved in the basic Internet infrastructure: first, the ".mx", that was transferred by Jon Postel to ITESM[28] in 1989, second, the UNAM network[29], which administered a B-type block of IP addresses[30], and third, the National Technological Network. The Internet Society (ISOC) Mexico Chapter worked within the context of UNAM, and there was an implicit agreement of division of technical and political tasks between these two important university institutions -the ITESM and the UNAM.

By 1995, with the increased popularity of Internet thanks to the emergence of the World Wide Web, it was essential to join efforts in this direction. In this way, the ITESM became the *country code Top Level Domain* (ccTLD) and the national Internet address registry in Mexico (NIR).

[27] Gayosso, Blanca, "Cómo se conectó México a la Internet. La experiencia de la UNAM", on *Revista Digital Universitaria*, No. 4(3), Ciudad de México, , 2003. Available at: http://bit.ly/1x9AieR

[28] Monterrey Institute of Technology and Higher Education.

[29] National Autonomous University of Mexico.

[30] This is a block of 65,356 hosts, a very high number for a time when Internet had not yet been massively deployed to citizens.

The early years filled with rivalry over the coordination of Internet resources and basic infrastructure left an important legacy to the Internet pioneers of both universities. They learnt they had to work in line with the international action frameworks for this growing scheme, both to understand the rules but also change and create new institutions and strengthen their domestic position.

While these Internet engineers and pioneers in Mexico rolled out new institutional mechanisms to operate with these new technologies, the regulatory telecommunications authorities focused their efforts towards other areas. The emergence of Telmex as a private company resulted from this government action and brought about the massive development of a fibre optic network, which put Mexico at the forefront in terms of Internet access quality compared to other regional countries. Between 1995 and 2006, the Federal Telecommunications Commission (COFETEL) consolidated its role as a regulatory entity, although its field of action was quite limited despite the reform made in 2006. The delayed process of reforms in telecommunications ended when President Enrique Peña Nieto took over in late 2012, giving rise to several lines of action. One of the first measures was the creation of the National Digital Strategy Agency, with the purpose of coordinating Internet matters from the Executive Branch, including aspects of Internet governance and digital communication, and the creation of the Federal Telecommunications Institute (IFT), that finally proposed the organisation of the sector. Before continuing with the impact of the presidential strategy since 2012, it is essential to highlight the parliamentary initiative of 2009, that sought to levy a 3% tax on Internet services. This initiative was stopped by a virtual demonstration on Twitter and other social media platforms under the motto #InternetNecesario, as people also took to the streets in the main cities. This accelerated the involvement of the civil society and other players in relation to the importance of participating in the discussion on Internet public policies.

The creation of the National Digital Strategy Agency was highly influential as it proposed five central objectives for the development of the strategy: government transformation, digital economy, quality education, universal and effective health, and public security, which can be realised in an enabling environment where Internet governance is included in the country.

This strategy turned out to be a fundamental triggering point for other historical Internet actors to develop the so-called *Grupo Iniciativa*, as the ones we have already mentioned ("nic.mx", ISOC Mexico Chapter, UNAM), as well as the Mexican Internet Association (AMIPCI). These groups and others were already informal, with weak coordination mechanisms. However, in practice, they were a reliable policy network with years of experience. This network

had no official or legal structure and started operations in 2013 within the framework of informal discussions among the various sectors grouped in an e-mail listing. Initially, the ".xm", in its function of organiser, contacted two representatives from five sectors (the Academia, the government, the technical community, businesses and the civil society) to form the group, and adopted the following principles related to the organisational aspects: equitable participation, balanced representation, self-motivated instead of formal leadership, on the basis of the topics of discussion and agreed-upon decisions[31].

In 2013, the group decided to hold a meeting to show the fluent and interactive nature of the work done by *Grupo Iniciativa,* which was called "*Diálogos Mexicanos para la Gobernanza de Internet*" (Mexican dialogue for Internet governance), an event with similar characteristics to a national IGF. The programme was developed based on surveys carried out in the Internet community in Mexico, and included a variety of topics ranging from human rights, to e-commerce to online participation. The turnout at the event was very high, with over 150 on-site participants and 3,000 devices that were connected to the online platform for remote follow-up. In February 2015, a second edition with similar turnout and adherence was held. But beyond *Diálogos*, the group maintains its presence and identity based on the coordination and discussion of the current issues within the members of the mailing list.[32]

The Group is inspired in the general working principles of the technical Internet community and its mechanisms (IETF, ICANN) for discussions based on consensus, openness, equality and the approach of the Tunis Agenda towards an Internet governance based on the respect and the promotion of human rights.

This initiative was particularly relevant during the LACIGF held in Mexico City in 2015, since it worked as a national liaison body in the setting of the regional agenda. It will also have to define its role at the Internet Governance Forum 2016 in Guadalajara by year-end, which will prove this mechanism's effectiveness as a bridge between the national and international governance, and as a policy network to coordinate the various national players.

II.D. Uruguay and Venezuela: incipient experiences

As anticipated at the very beginning, there are other national initiatives in the region, which are still emerging. One is Venezuela, which held several editions of

31 Interview conducted on July 16, 2014 to Manuel Haces, prospective manager with Network Information Center Mexico (NIC.MX) at the 7th edition of LACIGF, El Salvador.

32 The e-mail used for the group is grupodeiniciativa@nic.mx

the Venezuelan Dialogue for Internet Governance between 2014 and 2015. The main driver for the organiser of these meetings, which was the ISOC Chapter in that country, was the possibility to have a multistakeholder space for dialogue. Considering the Venezuelan political context and the role of the government in the country's public arena, it was not easy for the organisers to create a space for dialogue on complex and controversial topics, as is in general the agenda for Internet governance. In spite of the controversies and disputes on the various subjects addressed in the programme, including claims and questionings among actors on issues related to network neutrality, human rights in Internet and access policies, the event managed to lay the foundations for legitimacy to continue working and organise a second forum. The second edition was jointly hosted by the Association of Internet Users (*Internauta Venezuela*) and the ISOC Venezuela Chapter, and was entitled "II Meeting on Internet Governance for Social Development and the Transformation of the State", held at the CANTV auditorium. The second edition of the event reported a higher turnout and greater government involvement in the various panels.

This forum has some points in common with other regional and international events of similar characteristics, remarkably the LACIGF or the IGF, upon which organisers have based their guiding principles. One of the most outstanding results from these forums is that the government of Venezuela, through the National Telecommunications Commission (CONATEL) is -at the time when this paper is published- developing a process to set up a multistakeholder model driven by the government.

The case of Uruguay has some points in common with the Venezuelan experience, since the initiative stems from that country's ISOC Chapter with the objective to develop the first Internet Governance Forum, held in May 2016, under the motto "Internet in Uruguay: a dialogue amongst us all". Until now, it has been proposed only as a space for convergence of stakeholders for the organisation of forums. While this was an idea that the government of that country -through the Agency for the Government Development of Electronic Management and the Society of Information and Knowledge (AGESIC)[33]- sought to materialise within the national context, it also knew it was not the most appropriate actor to lead the initiative to avoid a governmental bias in the process. Just like in Costa Rica, the historical presence of the State in the country's communications has been, and still is, led by the sector's structure around a national monopolistic entity (ANTEL). Organisers held an open call

[33] It is a decentralised agency that has been developing the country's digital agenda for almost a decade, participating in the international spaces related to Internet governance.

to all entities and individuals interested in joining the initiative to develop the event's agenda. The participation of different organisations related to the *Casa de Internet de América Latina y el Caribe*, based in Montevideo, in drafting this agenda influenced the initiative, and brought about the experience of other national forums and, regional and international meetings, generating mechanisms of isomorphism with other experiences. The forum had over one hundred and fifty on-site participants and twice that number in remote devices. Ultimately, this case shows the progress made in the consolidation of a policy network on Internet in that country.

II. Comparative analysis

While the mechanisms applied stem from different sources, a series of critical events[34] actually defined the initial kick-off. Some of these events resulted from external factors, as is the case of Argentina and Colombia, and others had an internal triggering factor, as Mexico and Costa Rica. In the case of Argentina, the *Netmundial* meeting underscored the State's need to act in coordination and to generate mechanisms of dialogue with other actors to carry the process forward. In Costa Rica, the momentum of Internet governance on the presidential agenda was used as an opportunity to develop the CCI. In Colombia, the need to coordinate and understand the position of local players in view of a regional event, such as LACIGF was a key factor for the Governance round table to take off. In Mexico, the drive of a new administration and the creation of a specialised agency of new technologies, motivated other players involved in the technical and commercial development of Internet to develop a multistakeholder mechanism. The cases of Venezuela and Uruguay show the clear support from the Internet Society, through its Chapter mechanisms, to the development of these initiatives.

In relation to the scope and the objectives of these initiatives, the cases analysed vary a great deal. Except for the CGI experience, all initiatives mentioned in this document constitute very recent mechanisms. As was already proven by the case of the CGI itself, the process of consolidating a multi-party initiative requires time and commitment to a project that consolidates itself as a space of voluntary cooperation, and that attempts to go beyond a policy

[34] Understood as the decisions which produce a legacy that perpetuates in time, in a context where contingency and historical incidents prevail (Capoccia, Giovanni and Kelemen, R. Daniel, "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals", on *Historical Institutionalism World Politics*, Vol. 59, Nº 3, Cambridge University Press, April 2007, p. 341-369. Available at: http://bit.ly/2fSoFb0).

network to become a governance network. Shifting from a policy network to a governance network depends on the characteristics of each context, and is not always necessary. In some cases, if there is hostility or ignorance towards issues related to Internet governance, a policy network will not suffice and a mechanism of governance network will have to be consolidated. If any of these experiences are consolidated in the mid-term, as the experience in Costa Rica, Colombia and Mexico seems to show, their institutional capacity could be strengthened to develop a governance network.

In parallel, these processes are reluctant to formalities that may slow down operating times, or that may generate bureaucratic barriers, which are typical of the advance in the Internet agenda and of the original mechanisms adopted by Internet engineers around the IETF. In turn, none has the power to issue recommendations or proposals of binding nature, not even the CGI up until very recently. In many of these cases, the processes appear as recommendations, and the formal capacity resulting from these spaces is of consultative nature.

The main strength of these mechanisms resides primarily in the legitimacy-building of a process, for which it is essential to build dialogues to inform policy makers and exchange various and confronting perspectives. It also resides in the agenda-setting capacity. But it is critical to have the results derived from these exchanges and discussions documented or have them in some other format (audio-visual, for instance), so that a legacy and a memory can be built on mechanisms which would otherwise appear as ephemeral or isolated. It is also important to mention that these spaces do not bear the same meaning for all the actors involved. Beyond the interest, vocation for service and public interest expressed by many participants as their motivation to engage in these spaces, a distinctive connotation and impact is found depending on each sector and situation.

For players involved in these initiatives, the formalisation of these spaces has brought about some substantial advantages. Firstly, they have access to information and knowledge in a more stable and organised way that enables them -in cases as that of the "nic.cr" as organiser of the CCI Costa Rica- to validate their development strategies or consolidate multi-player and national strategies in view of international events, as has been the case of the *Grupo Iniciativa* in Mexico and the Colombian experience. Secondly, clearer parameters are set for the agenda and the line of action, which would otherwise disappear if a formal mechanism (as would be in a policy network) was not in place. However, in countries with a short history of governance networks formally established with non-government actors, as is the case

for a large part of Latin America, the chances that these mechanisms acquire any additional function other than consultative processes, is a possibility rejected by government representatives involved in these initiatives, and by other actors (although in the latter, varying positions are found) [35].

It is also worthy of note that there are variations both in the composition of the stakeholders involved in these initiatives as well as in their level of participation. The Argentine case is still incipient and the change of Administration, whose agenda includes Internet governance, is expected to increase its representation and participation in the incipient Secretariat/ Programme Committee of Argentina's IGF. In the case of the *Grupo Iniciativa* of Mexico, while in the group's early days the idea was to have two representatives per sector, today the group of government actors has more representatives than the rest, in part due to the inclusion of the governance agenda in more government entities, a trend that is also observed in the rest of the national cases that were analysed. It is important to note that in the case of the CGI, used as a framework of reference, the most equitable participation process with the greatest representation of non-government players occurred in 2003, when -under Decree 4829- a by-laws reform amended the participation of leaders from various sectors, and created "nic.br", the body that manages Brazil's Internet resources.

The experiences analysed in the national cases also vary in terms of the level of adaptation/adoption to the global rules of the Internet governance game. The Brazilian CGI, which was established before many other regional and international mechanisms and institutions, is a system that represents several of the principles and mechanisms that are currently deployed in ICANN, IGF and in the Action Plan of the Information Society in Latin America and the Caribbean (ELAC). The CCI as well as the *Grupo Iniciativa*, the *Mesa Colombiana*, and the emerging examples in Venezuela and Uruguay show great adherence to the principles and practices associated with the working process within the framework of the ELAC and LACIGF in the region, as well as the IGF at a global level.

Conclusions and recommendations

This paper addresses the national Internet governance mechanisms in the fledging processes of institutionalisation, covering the main developments that have shaped the strategies of emerging players organised around

[35] The literature on governance networks shows very critical positions against certain mechanisms, which are not transparent and may even challenge state authorities.

Internet governance, in configurations sometimes similar to a policy network (Argentina, Mexico, Uruguay, Venezuela), and in other cases, similar to governance networks (Colombia, Costa Rica). Clearly, the "CGI.br" is included in this second category.

Following Peters' classification of "governing in the shadows", understood as the authority that gives sense to a certain agreement, the social capital of Internet pioneers in these countries consolidated governance mechanisms that were initially based on the knowledge of experts. Those configurations are especially present today in the cases of Mexico and Costa Rica, and to a lesser extent, in Argentina, Uruguay and Venezuela. It is particularly relevant to dig into emerging institutional processes for Internet policies and governance in the region at this historical point in time, since, from an institutional perspective, the origins set up mechanisms that consolidated the initial options later on. As observed with the introduction of Internet in these countries, many of these actors are still involved in the recent national mechanisms of Internet policy and governance. It is still too early to assess the legacy of these initiatives, beyond the emergence of national forums on Internet governance, that constitute a visible point for discussion and agenda-setting.

The concept of policy network and its evolution towards a governance network still confronts the traditional idea that policies are unilaterally defined by the State. As was already pointed, these processes' contributions to policies on this matter are still emerging. It is also a complex issue to assess since Internet itself is a technology difficult to regulate through traditional instruments, and therefore, much of the progress made by these mechanisms are procedural and intangible. The gaps in participation and the subsidiarity levels highlighted at the beginning of this paper as relevant to the provision of global public goods, are aspects being addressed by the national processes, even when there is still a deficit in the capacity of involvement and incidence on the agendas, and in regional mechanisms, such as LACIGF or ELAC, as well as the IGF. A greater need exists to address domestic matters, which are frequently imposed by the agendas of governments and their regulatory and legislative processes, rather than matters which may appear less visible in the agenda or which may require greater follow-up and coordination efforts in the mid-term, as is the case of regional and global instances. In this line, a recommendation for these mechanisms would be to move forward with these initiatives in two fronts: for one, focus on the Internet issues in the country, characterising the topics with the value of specific and local knowledge, and providing the corresponding prioritisation; for the other, deploy a follow-up mechanism that is more active in regional and/or international spaces where In-

ternet governance topics are developed, and where actors such as the academia and the civil society have incidence capacity. This regional and international dimension is essential, since an important part of the issues related to Internet from a governance stance is not only restricted to jurisdictions and territories, thus, feedback is fundamental to enhance both experiences.

Another recommendation to strengthen the relevance of these spaces is the development of more permanent work mechanisms, instead of only focusing on the organisation of the national IGF (or its equivalent), in order to obtain public results. This is because joint efforts make the work and the achievements more visible than holding one annual event. It is important to say that these mechanisms behave as transversal work spaces, as is the case of the Costa Rica CCI (which does not even organise an Internet governance forum in the country), the Brazilian CGI (that only began organising the national forum in the last years), the *Mesa Colombiana* or the *Grupo Iniciativa*. In the most recent cases, as that of Argentina, Uruguay or Venezuela, the objective of these spaces is still focused on consolidating processes for the creation of a multi-sector forum.

An additional element that may be considered as a "good practice" of several of these experiences is the use of online collaboration tools, both at the level of discussions as well as of documents and proposals (it is quite remarkable in the cases of Costa Rica, Mexico and Colombia). In this way, the work becomes more transversal and, in turn, an "institutional memory" is created for players who may join in the future.

As to the academic contribution to these spaces, it is interesting to highlight that this is conceptualised as "civil society" in the IGF, while in other spaces with greater presence of engineers, it may be associated to the "technical community". However, the role of the academia and of academics in these national spaces and mechanisms has a brighter visibility, and may become a player with a more defined identity than that of other regional and international spaces. These academic contributions may be related to the capacity to produce primary information, research and arguments supported on empirical evidence and/or a disciplinary body.

Last, the excessive formalisation with consequences on the rigidity of some of these mechanisms should not be mistaken with a synonym of a more consolidated national process. The experience of the Brazilian CGI is that of a corporate model, with clear rules and guidelines, and with a history of over 20 years of existence, jointly with a funding system associated to Internet resources, which should not necessarily be replicated as a model in other national contexts, where the Internet governance policy network is not yet sufficiently developed. In these cases, it will be necessary to consolidate experiences that,

even though they may be not too formal, they have continuity in time and produce some tangible results -whether as national forums or documents- to capture more players from various sectors, and to enable a more balanced development of public policies and regulations around the Internet.

Other references

Hemmati, Minu, *Multi-stakeholder Processes for Governance and Sustainability: Beyond Deadlock and Conflict*, London, Earthscan Publications Ltd., 2002. Available at: http://bit.ly/2fCGxVU

Kenis, Patrick and Schneider, Volker, "Policy Networks and Policy Analysis: Scrutinizing a New Analytical Toolbox", in: B. Marin and R. Mayntz (eds.), *Policy Networks: Empirical Evidence and Theoretical Considerations*, Fránfort, Campus Verlag, January 1991. Available at: http://bit.ly/2ffbgru

Kooiman, Jan, "Governance. A Social-Political Perspective", in: Grote, J. and Gbikpi, B. (eds.), *Participatory Governance: Political and Societal Implications*, Opladen, Leske + Budrich, 2002, p. 71-96.

Lucero, Everton, *Governança da internet: aspectos da formação de um regime global e oportunidades para a ação diplomática*, Brasilia, Fundação Alexandre de Gusmão, 2011.

Mariscal, Judith, Rivera, Eugenio and United Nations, *Regulación y competencia en las telecomunicaciones mexicanas*, Mexico, F.D., United Nations, ECLAC, International Trade and Industry Unit, 2007.

Núñez, Mauricio Guido, *Tutela de los nombres de dominio en Internet*, 2004, available at: http://bit.ly/2fZy13Z

Olson, Mancur, *The logic of collective action: Public goods and the theory of groups*, Cambridge, Massachusetts, Harvard University Press, January 1971. Available at: http://bit.ly/1EG6zOe

Quarterman, John, "Networks in Argentina", *Matrix News*, Vol. 5, Nº 8, Texas, Matrix Information and Directory Services Inc., 1991.

Rhodes, R.A.W., "The New Governance: Governing without Government", in *Political Studies*, Vol. 44, Nº 4, 1996, pp. 652-667.

Chapter Two

Cybersecurity and Human Rights in Latin America

Daniel Álvarez Valenzuela[1] y Francisco Vera Hott[2]

Introduction

Since the end of the 2000s, several events have vertiginously placed cybersecurity at the forefront: denial-of-service attacks in Estonia, cyberattacks in Georgia, the consolidation of organised cybercrime in certain countries, mass leaks of information from businesses and States, use of malware and tapping of digital communications by governments to persecute activists, among many other events. All of this has been amplified by Edward Snowden's revelations on the activities related to mass communication surveillance performed by intelligence agencies from countries such as the United States, England, New Zealand, among others.

These events bring about a growing technical sophistication of the means that are being used, going from social hacking modalities, like *phishing*, to advanced and persistent threats, with complex malicious applications, some of which are specifically programmed to steal strategic military or commercial information, to others that may illegally code the content of a computer, turning it inaccessible for

[1] Daniel Álvarez Valenzuela is a lawyer. He holds a Bachelor's Degree in Legal and Social Sciences and an LLM in Information Technology Law from the University of Chile. He is currently attending a Ph.D. course at the same university. He is professor of Privacy and Technology in pre-graduate and post-graduate courses at the School of Law of the University of Chile. He is also Research Coordinator at the Centro de Estudios en Derecho Informático. Founder and general editor of the Revista Chilena de Derecho y Tecnología (Chilean Law and Technology Journal). He is founder of Derechos Digitales NGO. His email is dalvarez@uchile.cl.

[2] Francisco Vera Hott is a lawyer. He holds a Bachelor's Degree in Legal and Social Sciences from the University of Chile. He is Fulbright grantee and Thomas Buergenthal Scholar 2016-2017. He is currently completing post-graduate studies at the George Washington University. His email is francisco@verahott.com. This article is an English translation of the Spanish original.

its legitimate owner, who will later have to pay the IT criminals to recover access to his/her own information. All of these developments share a common feature -cybersecurity has now become the main concern for multiple stakeholders, both public and private, many of whom are making great efforts to understand the risk posed by cyberspace and the decisions they must adopt to confront it.

The aim of this paper is to make a critical review of certain concepts which are essential for discussion. For this purpose, cybersecurity will be presented as a contended concept, presenting the main arguments around it and drafting the minimum standards that should be met, from a human rights standpoint, and providing examples within the Latin American context.

I. Specificities on the concept of cybersecurity

For some years now, the term cybersecurity has been increasingly gaining terrain in the public and private sphere, even transcending the field of specific skills of IT professionals. Today we witness how cybersecurity has been responsible for the adoption of measures by governments, international organisations, universities, businesses, civil society organisations and even individuals -in their respective fields- in order to address a phenomenon that apparently is here to stay.

The diversity of stakeholders involved in the debate on cybersecurity -hackers, IT professionals, private sector executives, public officials, security and defence officials, journalists and human rights activists- accounts for the fact that each actor makes use of the concepts related to "cyberspace" (usually with the prefix "cyber" before the terms) based on his/her focus of attention and personal interests, as consensus exists over a material meaning of the expression "cybersecurity", let alone its legal, political and -strangely- technical dimensions. But before addressing cybersecurity, it is essential to review the ideas and concepts underlying the terms "cyberspace" and "security", which are part of the new environment that surrounds us. For this purpose, we will briefly analyse both concepts, including the specific paradigms of our approach, which are related to security, national security, human security and information security.

I.A. Cyberspace

The concept of cyberspace -a term combining the word "cybernetics" and "space"[3]- was first introduced on the book *Burning Chrome*, written by

[3] Singer, Peter and Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014.

science fiction author William Gibson, who later resorted to the term extensively in his novel *Neuromancer*. On the latter, the writer refers to cyberspace as a 3-D environment of pure information exchanged via computers, where people are generators and users of that information[4].

Today, most concepts related to cyberspace hinge around the idea of a space, environment or domain of information, which can be appreciated in the collection of definitions published by *New America* in late 2014[5]. At various levels, all of them define cyberspace as a dimension different from the physical one, where human interaction takes place based on the exchange of information[6].

Cyberspace is made up of three clearly distinguishable layers. The first one is the physical infrastructure (cables, computers, satellites), which enables cyberspace to operate as such. The second layer is the logical infrastructure (network protocols, computer programmes), which creates the language that enables machine-man interaction, and the third layer is made of the content y/o the human interactions (texts, audios, videos, etc.)[7]. Each of these layers is subject to different regulations which may systemically converge or not, making the analysis of cyberspace as a whole more complex.

While today Internet resides at the core of the cyberspace concept, it does not exhaust it but constitutes one of its most important manifestations. Cyberspace is something bigger than Internet; it is the digital information environment even when it is not part of the network of networks[8], which also includes the human interactions that occur there and the interactions of computer systems that are not connected to the Internet[9].

---

[4] Craigen, Dan, Diakun-Thibault, Nadia and Purse, Randy, "Defining Cybersecurity", *Technology Innovation Management Review*, Ottawa, Carleton University, 2014. Available at: http://bit.ly/2fzXhNF

[5] Maurer, Tim and Morgus, Robert, "Compilation of Existing Cybersecurity and Information Security Related Definitions", *New America Report*, Washington DC, October 2014, p. 18-24. Available at: http://bit.ly/2eB5ZGJ

[6] Concepts similar to cyberspace may be found, but focused on certain particular aspects, such as information security or information technology. Without detriment to any differences, all concepts make reference to this new reality defined by the use and processing of digital information.

[7] Benkler, Yochai, "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access", on: *Federal Communications Law Journal*, Nº. 52, Washington DC, 1999.

[8] Singer, Peter and Friedman, Allan, *supra* note 3, p. 14.

[9] A clear example of the aforementioned is the case of Stuxnet, a malicious programme that attacked a nuclear power plant that was not connected to any computer network, which shows the possibility for attacks in cyberspace without the need to use the Internet.

All in all, the concept of environment, domain or territory underlying the term cyberspace, necessarily imbue it with a political burden, as a place where power disputes occur within and over cyberspace, and are expressed in the definition of concepts such as cybersecurity. In this sense, each concept of cyberspace and, particularly, of cybersecurity, brings about a specific political agenda, as we will see later on.

I.B. Security

Security is a much older and contended concept, discussed in several fronts and disciplines that date back -in contemporary times- to the end of the Cold War[10] and, indeed, it is not possible to address it comprehensively in this paper, but we will focus on the concepts that may seem relevant to define cybersecurity, strictly ruling out legal notions, such as legal security, and those that are more psychologically or privately oriented, which aim at the sense of security rather that the political or social dimension of interest to us. Nonetheless, even when it is hard to find a univocal definition for security[11], some of the most relevant security paradigms may be identified in order to build the concept of cybersecurity, namely: national security, multidimensional and human security and information security.

The traditional security paradigm is that of "national security", which in turn results from the idea of sovereignty[12]. This concept, whose modern form is observed in the works of Hobbes and Bodin, was enshrined in the Treaty of Westphalia in 1648[13], which contains the ideas of territorial integrity, political stability, military agreements and economic activities.

The paradigm of national security holds States as the protagonists, and the prevalence of their sovereignty as the assumption of living in society. This is the assumption of any political activity, so the main goal is the prevalence of the State's sovereign power. Thus, the government must protect the State and its citizens from all kinds of crises and threats, using its various tools to generate and project power. This paradigm was explicitly adopted by many

[10] Baldwin, David, "The concept of security", on *Review of International Studies*, Nº. 23, Cambridge, Cambridge University, 1997, p. 9.

[11] Several dictionaries define security as "the state of being secure", and the term "secure" is defined as "safe, protected against danger or risk", which only offers a functional framework to the concept, but does not answer the question about which type of danger or risk is to be prevented or minimised.

[12] "Sovereignty", *Stanford Encyclopedia of Philosophy*, Stanford University, 2016.

[13] Treaty of Westphalia.

countries after the end of the Second World War, in the light of a nuclear threat and within the context of the Cold War. The doctrine of national security was developed based on this paradigm. In the American context, it has also been known as "hemispheric security"[14], and it was used, under the concept of internal enemy, to justify the violent seizure of power and the emergence of dictatorships all over the world, particularly in Latin America[15]. The concept was also used by many of those dictatorships as the rationale for very serious human rights abuses, which affected many people. All in all, the concept of national security has evolved since the 1990s to become part of new paradigms, such as multidimensional security and human security.

Within the American context, the concept of "multidimensional security" arises by the end of the Cold War, with the emergence of a new regional outlook characterised with common instability factors, which go beyond the state and military spheres, and comprise a range of matters including poverty, terrorism, organised crime, arms trafficking and natural disasters[16]. The use of the multidimensional security paradigm was ratified by the Organisation of American States (OAS) in October 2003, within the framework of the Special Conference on Security, where the "Declaration on Security in the Americas" was adopted. A new concept of hemispheric security was developed, including both traditional and emerging threats, and stating that human rights and fundamental freedoms are essential to the stability, peace and development for the States of the Americas[17].

The "human security" paradigm, for its part, marks a shift in the concept of security, putting the human being at the centre. Its origins also date back to the end of the Second World War and the proclamation of the Universal Declaration of Human Rights in 1948[18]. The very first paragraph of the Declaration's preamble states that "the recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world", placing human beings, and not the State, at the centre of security challenges and, specifying that the State security does not necessarily coincide with people's security.

[14] Rojas, Francisco and Soto, Daniel, "Estándares Internacionales y Seguridad Pública", in *Derecho Público Magazine*, Vol. 77, Santiago, University of Chile, 2012. Available at: http://bit.ly/2eAWkA9

[15] *¿Qué es seguridad humana?*, San José, Costa Rica, Inter-American Institute on Human Rights. Available at: http://bit.ly/2af7dde

[16] Rojas, Francisco and Soto, Daniel, *supra* note 14, p. 444.

[17] *Ibíd*. (*quoting:* Declaration on Security in the Americas, Organisation of American States, 2003).

[18] Universal Declaration of Human Rights, Paris, December 10, 1948.

The high point of this concept is the United Nations Development Programme's (UNDP) *Report on Human Development*, in 1994, where human security is defined under two main aspects: "It means, first, safety from such chronic threats as hunger, disease and repression. And second, it means protection from sudden and hurtful disruptions in the patterns of daily life -whether in homes, in jobs or in communities"[19]. Hence, human security is defined as the people's freedom from fear, want or misery and the freedom to lead worthwhile lives[20].

From a technical standpoint, the concept of information security can be summarised in the preservation of a system's confidentiality, integrity and availability of information[21]. Confidentiality aims at maintaining data private, only to be accessed by its recipients. Integrity means that the system and its data are not altered or removed without the owner's authorisation or will. For its part, availability is the possibility of using the system for the purpose it was originally designed[22]. All in all, the concept of information security does not exhaust in the three aforementioned elements. Other academic contexts refer to it as the confidentiality, integrity and authenticity triad, while in the field of information security management, a distinction is made as to the interaction among technologies, processes and people.

Finally, the development of more complex IT networks and, particularly, the development and ubiquity of Internet have raised the need to integrate new properties into the concept of information security, such as resilience[23], which enables systems to resist and overcome threats against their security instead of becoming unavailable. This is consistent with a key aspect of information security management, goes beyond the mere prevention of attacks or incidents, and tends to identify and properly manage associated risks. As any specialist would point out, there is no state of absolute security in IT, only the possibility to minimise and manage those cases where security is jeopardised.

---

[19] *Report on Human Development*, United Nations Development Programme, New York, 1994.

[20] Inter-American Institute on Human Rights, *supra* note 15.

[21] The exact origin of this definition is not clear, even when the supporting operating concepts go back to numerous military treaties from ancient times, as that of "*de bello Gallico*" (the Gallic Wars), and is currently included in various technical standards in the subject, as the ISO 27000 standard series.

[22] Singer, Peter and Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014, p. 35.

[23] *Ibíd*., p. 36.

I.C. Cybersecurity

After analysing the concepts of cyberspace and security, it is important to address the concept of cybersecurity, which combines both elements and defines the idea of security in this new setting. There is not a widely-shared conception of cybersecurity, as this term is much more contended than "cyberspace". To date, according to the *New America* research[24], more than forty-five different concepts exist in this regard.

Cybersecurity should be understood as a concept different from information security, since it is far from being technical or aimed at specialists, and makes reference to the interaction of cyberspace with the various security conceptions, including in some cases, the use of cyberspace as a means or tool to pose threats to national security, multidimensional security in some aspects or even, human security.

According to the most modern definitions, cyberspace is another setting where States and organised players can build and exercise power. Therefore, the concept of cybersecurity may expand to represent the power dispute in cyberspace. Such dispute also comprises the concept of cybersecurity and the way in which States fight to impose their concepts of security and systems of values in cyberspace. In the words of the Minister of Foreign Affairs of Estonia, Marina Kaljurand, "cyber" is not a technology but a political notion anchored in the convergence of various technologies, where cyberspace works as a social scenario, financial market and political battlefield[25].

I.C.I. Importance of a risk management approach and lack of a shared concept

Since it is impossible to fully prevent the occurrence of cyberattacks, specialists have reached a high level of consensus on the importance of a risk management and minimisation approach. In this sense, it is critical to include this approach into the cybersecurity concept, since it implies a rational and proportioned analysis of the subject-matter, and promotes the use of the right technical tools to manage risk within cyberspace. Besides, considering risk management and, consequently, the constant possibility of

[24] Maurer, Tim and Morgus, Robert, "Compilation of Existing Cybersecurity and Information Security Related Definitions", *New America Report*, Washington DC, 2014, pp. 25-32

[25] The International Institute for Strategic Studies, "Evolution of the Cyber Domain: The Implications for National and Global Security", 2015, pp. 15-16.

suffering IT attacks or incidents, incorporates not only a preventive notion in relation to the occurrence of incidents, but also a "resilience" or recovery capacity against them. On the other hand, overlooking the risk management perspective (or a similar one) in the definition of cybersecurity paves the way for the adoption of unsuitable or disproportioned public policies or measures.

II. Internationally relevant cybersecurity aspects

Cybersecurity notions and concepts are expressed and gain relevance in several fields of action, for instance, in relation to the States' behavioural rules in cyberspace, international Internet regulation, the mechanisms to fight cybercrime and the role of surveillance in that environment. We will refer to each of these settings individually.

II.A. Inter-State behavioural rules and cyberspace militarisation

Cyberspace has become the field where States engage in economic, diplomatic and military relations. This circumstance has raised several questions as to the existence and application of behavioural rules for state-players in cyberspace, particularly in those cases where conflicts involving States and other international stakeholders take place in this setting. In particular, cyberspace conflicts (also known as "cyberconflicts"[26]) are sparking big debates regarding the application and construction of international law in these situations.

In principle, broad consensus exists that international law may be fully applicable in cyberspace, since the actions regulated under international treaties are not limited to a specific environment, but rather refer to actions *per se* and their consequences. In addition, some actions in cyberspace may impact the physical world, for instance, the case of the malicious programme known as *Stuxnet* which disabled the facilities of an Iranian nuclear power plant, producing similar effects to those of a physical or kinetic attack.

In this way, international instruments on human rights and armed conflicts may be applicable in cyberspace. However, the debate resides on the scope of such application: the extent to which it is possible to apply the existing international treaties and the cases for which no definite solutions exist; it also relies on the definition of minimum behavioural rules to be followed by

[26] This concept has been basically elaborated on "Evolution of the Cyber Domain: The Implications for National and Global Security", The International Institute for Strategic Studies (IISS), 2015.

States in cyberspace, which may constitute a body of international common law with the purpose of being applied in cyberspace.

The most relevant effort to answer these questions may be found in the so-called "Tallinn Manual"[27], a NATO-sponsored academic initiative, which compiles the analysis made by several international law experts in relation to the application of various international law standards in the field of cyberspace, particularly focusing on the *jus ad bellum* rules governing the States' behaviour in cases of armed conflicts. Although we will not analyse the content of this manual in detail -whose second version is soon to be updated and published- it is important to make some basic clarifications on the state of the art of this discussion, in relation to three circumstances: i) espionage in cyberspace; ii) the use of cyberattacks with no physical consequences, and iii) the use of cyberattacks with physical consequences.

First, espionage or secret theft is not expressly ruled under International Law, without detriment to constituting a common and long-running practice among States. Due to the aforementioned, espionage activities conducted by agencies such as the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ) or other similar institutions, are not penalised and are generally addressed by the affected States through political or diplomatic measures. However, as we will further analyse, when espionage and surveillance practices are targeted against people, the provisions of international treaties on human rights may be applicable, in particular, rights related to privacy and freedom of expression.

In the first place, a case that deserves special attention is that of mass surveillance of Internet communications and activities. The disclosures made by the US intelligence analyst, Edward Snowden, since June 2013, revealed a series of operations conducted by the NSA and its allies within the framework of the intelligence community known as *five eyes*[28]. The seriousness of Snowden's disclosures lies on the large scope of the surveillance operations disclosed, including the extensive data records on telephone calls within the United States, the secret and unparalleled access to users' data of various social media platforms as Google, Yahoo or Facebook, or the capacity to tap and store Internet traffic of a whole country, among other disclosures.

[27] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013. Available at: http://bit.ly/2eJIfDV

[28] A detailed list on Edward Snowden's disclosures may be found on the website of the English newspaper *The Guardian*, entitled "The NSA files", available at: http://bit.ly/2cmqvxE

In the second place, the use of cyberattacks without physical consequences, as the one launched in Estonia in 2007, consisting of scattered denial of service (DDoS) attacks against the networks of the country's financial and government sectors, is one of the most difficult problems to solve in the sphere of international law, which considers the hypothesis of an armed conflict characterised by the destruction of physical facilities or the loss of human lives, which is not easy to confirm in these cases.

Considering that the rules of international law are not enough, various initiatives, including the "Tallinn Manual", confidence-building measures adopted by international bodies such as the Organisation for Security and Cooperation in Europe (OSCE), the OAS, the UNASUR's South-American Defence Council, or the UN Group of Experts' reports, aim at the creation of basic behavioural standards to be followed by States in cyberspace, ranging from the publication of their points of contact and definitions and the prohibition to attack critical infrastructures in each country, to the imposition of support actions in case of attacks and the prohibition to launch attacks through intermediaries or *proxies*.

In the third place, in relation to cyberattacks with physical consequences, these may be linked to the concept of self-defence and armed attack under the United Nations Charter Article 51[29]. To date, however, there is no record of cyberattacks that may be considered as armed attacks with serious consequences for a country's infrastructure or that may have claimed the lives of humans. The above-mentioned cases would be the only instance where the concept of cyberwar would apply.

Nevertheless, from an international law perspective and due to the difficulty to frame a cyberattack as an armed attack, we agree with the statements made by professor Thomas Rid[30], who declares that an offensive act has to meet certain criteria in order to qualify as an act of war. Any act of war has to have the potential to be lethal; it has to be instrumental; and it has to be political (malicious IT code), that is potentially lethal, something which does not match any conflict occurred in cyberspace until now, and which will apparently not occur.

II.B. Internet Governance and Cyber-security

Although Internet is not cyber-space -as was already explained- today it represents its most evident expression, whose international regulation sets

[29] United Nations Charter, San Francisco, United Nations Organisation, 1945.

[30] Rid, Thomas, "Cyberwar will not take place", on *Journal of Strategic Studies*, vol. 35, N° 1, 2012.

up an interesting system where States, international organisations, technical organisations and other stakeholders, such as private companies, academics and civil society interact in a complex context of technical and political forums and spaces with diverse binding capacities, all grouped under the so-called Internet governance.

This governance system poses a big challenge to the adoption of cyber-security decisions, whose debates are held in forums which have traditionally discussed security matters under the paradigm of inter-state multilateralism, while Internet governance discussions also involve the active and deliberate participation of other non-state players, which conform the so-called *multis-takeholder* paradigm. The compared experience raises the need for joint work among States, the private sector, the Academia and the civil society. In line with this, the *multistakeholder* paradigm does not only represent an alternative, but a necessity, given that most of the Internet infrastructure (i.e., part of cyber-space) is in private hands or managed by private technical organisations.

Thus, the relation between Internet governance and cyber-security presents multiple and interesting challenges. For one, the integration of spaces for discussion on security and Internet governance in order to address the issue of cyber-security from a broader perspective, including Internet technical and regulatory aspects. For another, the importance of ensuring the inclusion into those spaces of *multistakeholder* governance principles, that allow for Internet governance and a wider and informed debate that takes into account the stances of the various parties involved.

II.C. Cyber-crime and Cyber-security

One of the problems of cyber-security that entails the most direct impact on people is cyber-crime. However, as in cyber-security and cyber-war, the concept of cyber-crime is also subject of further discussion and explanation.

To start with, there are several crimes related to the use of digital technologies, ranging from actions that go against cyber-space, such as unauthorised access to IT systems, information theft, destruction and sabotage of IT systems, publication of sensitive or non-consented information, IT fraud, data kidnapping or *ransomware*, to crimes that use cyber-space as the primary means to commit the act, such as fraud through the Internet, production and dissemination of child pornography, the infringement of intellectual property rights; to those crimes where cyber-space may have a role, such as the use of communication media for kidnapping, or sending e-mails in cases of blackmailing. Regarding the first two categories (crimes against cyber-

space and crimes where the main means to commit the act is cyber-space), the United Nations Organisation[31] proposed a broad concept including both categories, and a restricted conception, which makes a distinction between IT crimes (or cyber-crimes in strict sense) and computer-related crimes.

For its part, cyber-security in a wide and undetermined sense (cyber-space and security combined in various expressions), may involve virtually any type of crime based on digital media. For the purpose of this work, it is interesting to establish the extent to which the legal classification of cyber-crime may contribute to cyber-security, and to do so we will use the technical approach to cyber-security -already analysed (IT security)- that relates it to the preservation of data confidentiality, integrity and availability.

In this line, while the legal classification of crimes against cyber-space (first category) is closely related to the protection of information security, the legal classification of crimes related to cyber-space (second and third categories) is not directly linked to information security, but to the protection of several legal elements, such as assets, sexual dignity or freedom, or to the possibility of granting authorisation for law enforcement agencies to take forensic or surveillance measures that may affect information security, which does not only have an impact on public security, but also on the human right to privacy, as we shall see.

In this way, crimes included in the first category may be assumed to directly contribute to cyber-security in a technical sense, while the other two categories have a more complex relationship with the concept. This does not mean that crimes included in the second and third categories do not have social relevance (in fact, they are generally more serious) or that measures should be adopted, but rather that their cause and rationale go beyond the sphere of information security.

Beyond the relationship between cyber-crimes and cyber-security, the problems associated with the two concepts encompass the global nature of cyber-space, in a context where criminal laws are essentially territorial. In order to overcome this problem and to facilitate the international pursuit of cyber-crimes, the Convention on Cybercrime of the Council of Europe[32] was signed in 2001 in Budapest, Hungary, establishing a series of measures to be adopted by each country, both for the legal classification of specific

[31] Lara, Juan Carlos, Martínez, Manuel and Viollier, Pablo, "Hacia una regulación de los delitos informáticos basada en la evidencia", on *Revista Chilena de Derecho y Tecnología*, Vol. 3, No. 1, Centre for IT Law Studies, Santiago, University of Chile, 2014, pp. 103 and ss. Available at: http://bit.ly/2fQ81ZD

[32] Convention on Cybercrime, adopted on November 23, 2001, in Budapest.

crimes and for the adoption of international cooperation measures. By early 2016, almost fifty States signed the Convention, as Panama and the Dominican Republic were the only signatory countries in Latin America and the Caribbean, and in May 2016, the Chilean government submitted a bill for its approval and subsequent ratification before the National Congress.

III. Cyber-security from a human rights perspective

III.A. Validity of human rights in cyber-space

Without a doubt, international law is applicable to cyber-space in full force of all rules and with no distinctions whatsoever. This results from the text of the Universal Declaration of Human Rights[33], which enshrines the principles of universality and indivisibility of human rights, without distinction of any kind, as stated in the Declaration's preamble and first and second articles. The aforementioned was ratified by several United Nations General Assembly declarations, especially that of June 29, 2012, which underscores the promotion, protection and enjoyment of human rights on the Internet[34], and that of January 21, 2014, which sets forth the right to privacy in the digital era[35].

III.B. Human rights involved

Based on the above-mentioned, there are no specific human rights protected in cyberspace, but rather all of them are recognized and protected in this sphere, with no exception. However, some rights are particularly relevant in cyberspace for being strictly related to information in its various perspectives and expressions. These are the right to privacy[36], freedom of expression and information[37], together with the right to security and liberty[38]

[33] Universal Declaration of Human Rights, Paris, December 10, 1948.

[34] United Nations General Assembly, Resolution A/HRC/20/L.13, 29th June, 2012.

[35] United Nations General Assembly, Resolution A/RES/68/167, 21st January, 2014.

[36] Art. 12 Universal Declaration of Human Rights, art. 11 American Convention on Human Rights.

[37] Art. 19 Universal Declaration of Human Rights, art. 13 American Convention on Human Rights.

[38] Art. 3 Universal Declaration of Human Rights, art. 7 American Convention on Human Rights.

and no discrimination[39].

The interaction of human rights and the various concepts and topics about cyber-security is complex and not always clear, since the concepts on cyber-security and human rights are related at various levels. On the one hand, they supplement each other in a virtuous cycle as long as cyber-security remains functional to the protection of privacy, access to information or freedom of expression and personal security, among other rights.

This is the case with the technical concept of information security, where confidentiality is directly linked to the rights to privacy and personal security, and integrity and availability are related with the rights of freedom of expression and access to information. This relationship is not so straightforward when the conception of cyber-security generically refers to risk management for cyber-space, which may be inspired in concepts of national or multidimensional security, or in the concept proposed by the SCO on information security, which, in the name of cyber-security, may involve the control of information at levels incompatible with freedom of expression.

III.B.I. Concept of cyber-security from a human rights perspective

In order to propose a cyber-security concept from a human rights perspective, it is important to consider some factors already mentioned:

First, human rights are universal and inalienable, so the concept of cyber-security can by no means imply the absence of recognition to, or a waiver of any of these rights.

Second, human rights are indivisible, so no human right should be considered separately or secondary to any other right. In this sense, the interpretative criteria of human rights should maximise the rights and not consider any right as secondary to another.

Finally, it is preferable to consider a virtuous relationship with human rights instead of a contradictory one, in order to embrace concepts and remain functional to the previously mentioned attributes of universality, indivisibility and inalienability.

In this way, and considering cases where a virtuous relationship between human rights and cyber-security does exist, besides a level of clarity and accuracy to distinguish when cyber-security is being considered -as was already observed in the case of cyber-crimes-, it is desirable to use the tech-

[39] Art. 7 Universal Declaration of Human Rights, Arts. 1 and 24 American Convention on Human Rights.

nical concept of information security as the basis for the conceptualisation proposed in this paper.

All in all, this is not a new approach, and builds on the debate raised at the core of Freedom Online Coalition, an international coalition of countries which strive for the promotion of freedom on the Internet as their main objective. A working group called "An Internet free and secure" was formed within this coalition, with the purpose of building a new definition of cyber-security[40], putting it at the same level as human rights to be included into public policy-making. In this way, the group drafted the following preamble and definition:

> Preamble: International human rights law and international humanitarian law shall apply online as well as offline. Cyber-security must protect technological innovation and the exercise of human rights.
> Definition: Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline.

While it is an appropriate concept in general, which builds on the essence of the technical definition of information security and expressly makes reference to human rights, it does not define a risk management approach but similar -though not analogous- technical concepts. Besides, the point on technological innovation is not really necessary for the purposes of the definition, nor is it at the same level as human rights. As a matter of fact, when the concept was developed, the working group did not address the reason for including technological innovation, but rather the final objective, which is to enhance the security of persons (to articulate the technical concept, under the ISO 27000 standard) and the means used for that purpose: policy, technology and education.

Apart from the unnecessary inclusion of technological innovation as an element to be protected, and the absence of a risk management approach, this concept of cybersecurity may evolve in time towards the inclusion of human security elements at its core, aiming not only at a classical concept of personal security, but one that, based on justice, will contribute to peoples' freedom from fear, want or misery, and freedom to live in dignity. Ultima-

[40] Donahoe, Eileen and Maurer, Tim, *"Why Do We Need a New Definition for Cybersecurity?"*, Freedom Online Coalition, 2016. Available at: http://bit.ly/2fXTme3

tely, human rights should be taken as the foundation, and then should be developed as a goal. Therefore, the future of the concept of cybersecurity from a human rights perspective does not only aim at protecting certain attributes of information that are functional to them, but also at ensuring that cyberspace remains a fertile soil for the development of people, allowing mankind to reach new standards of freedom and dignity.

IV. Cybersecurity and human rights in Latin America

Latin America is a region with several distinctive features, such as the prevalence of Spanish and Portuguese languages, mostly presidential systems of government, many countries with a history of authoritarianism, with dictatorships tied to the national security doctrine, and that currently shows very high rates of economic and social inequality. Within this context, it is interesting to compare cases where cybersecurity approaches are in conflict with human rights. It is particularly interesting to analyse some cases where cybersecurity-related concepts, rules and practices, followed by the States of the region, have an impact on, and potential non-compliance of, international human rights obligations.

To that end, we shall briefly point to the efforts made by Latin American countries in terms of designing cybersecurity-related public policies, and then briefly address cases of potential impact on human rights in relation to the legal classification of IT crimes, use of malware and other cyber-attacks against people by States in the region, and legislative attempts to set up disproportionate surveillance regimes through data retention or geographical location disclosure measures.

IV.A. Development of cybersecurity policies and strategies in Latin America

The analysis of public policies around cybersecurity is not limited to legal texts, but also includes the consideration of other instruments such as cybersecurity policies or strategies, which are not limited to regulating certain behaviours, but to coordinating efforts among various sectors to reach strategic public-policy objectives.

Beyond debates about its definition, cybersecurity is a complex, systemic and multi-factorial concept, involving various aspects such as the security of public and private networks, critical infrastructures, crime prevention, edu-

cation, good practices, public-private partnerships, international relations, so on and so forth. Designing comprehensive public policies on this matter remains a big challenge for States, especially in view of the possible reductionism which may be faced when designing these strategies and policies.

In Latin America, the development of these tools has been rather scarce. The *2016 Cybersecurity Report* carried out by the Organisation of American States and the Inter-American Development Bank, presents a standardised and detailed study on the cybersecurity policies and strategies developed by Latin American and the Caribbean countries, considering maturity in five dimensions (startup, formative, established, strategic and dynamic) and employing the methodology of the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. Results fall short of encouraging. Out of the 32 countries analysed, 17 are in "startup stage", i.e., they show no progress in developing a strategy or, if the process has already begun, it was done without stakeholder consultation. Other 10 countries are in "formative level", i.e., they have articulated a strategy scheme with potential consultations to stakeholders, and only 3 countries have reached the "established level", meaning that an instrument has already been approved, consulted with stakeholders, and there is some data, risk and threat analyses made. The study shows that no country in the region has reached high maturity levels in terms of cybersecurity[41].

These figures more or less coincide with the numbers reported by the International Telecommunications Union (ITU)[42], which reveal that only Panama[43], Colombia[44], Brazil [45]and Uruguay[46] have national cybersecurity strategies or policies in place. However, according to the associated documents, the Uruguayan document is just a government decree, which rules the information security requirements for public agencies, so it does not qualify as a national cybersecurity strategy as such.

[41] Organisation of American States and Inter-American Development Bank, "Cybersecurity, Are We Ready in Latin America and the Caribbean?", on *2016 Cybersecurity Report.*.

[42] International Telecommunications Union's Repository on National Security Strategies.

[43] Government of Panama, *"National Strategy for CyberSecurity and the Protection of Critical Infrastructures"*, 2015**,** p. 35.

[44] Colombia has developed two tools on cybersecurity: Conpes 3701 document on *"National Planning Policy Guidelines for Cybersecurity and Defence"*, and the Conpes 3854 on *"Digital Security Policy"*.

[45] While Brazil does not have any cybersecurity strategy document similar to that of other countries, it has put in place a set of tools which resulted from coordinated efforts of political planning, which derived in the *Green book on Brazil's cybersecurity*, a security guideline for critical information infrastructures, a national defence strategy and a general information technology strategy, which includes security.

[46] Oriental Republic of Uruguay, CM 827, April 7, 2014.

For its part, Panama appears in the ENISA map[47] as the only Latin American country with a cybersecurity strategy, together with Jamaica[48] and Trinidad and Tobago[49] in the Caribbean, while Costa Rica, Peru and Paraguay are still preparing their strategies. Chile joins the list. Since 2015, it has been preparing a national cybersecurity policy[50] and, in February 2016, it submitted a policy draft to public consultation. Paraguay also published a policy draft in April 2016[51], with the purpose of receiving comments from citizens. The Argentine case is also worthy of note. The country has a programme for the protection of critical infrastructures and cybersecurity[52], whose actions are generally coordinated in other countries by means of a cybersecurity strategy.

IV.B. Concepts of cybersecurity in the region

The above described strategies and policies, both in terms of formal definitions and objectives, reveal some of the notions discussed before in this paper. For reasons of space and diversity, the cases of Argentina, Brazil, Chile and Colombia, which depict some of the points of discussion, will be analysed below.

Among the countries mentioned above, which have some degree of development for cyber-security strategies, it is not possible to find a formal and established definition of cyber-security in some of them, being Argentina the most paradigmatic case, since it has no formal definition for the term[53], as is concluded by the *Asociación de Derechos Civiles* in Argentina (Asociation for Civil Rights) in their research on the definition of cyber-security in said country. This happens despite the fact that the concept is repeatedly used in decrees and other official documents.

[47] European Union Agency for Network and Information Security, National Cyber Security Strategies.

[48] Government of Jamaica, National Cyber Security Strategy.

[49] Government of the Republic of Trinidad and Tobago, Inter-Ministerial Committee on Cybersecurity, National Cyber Security Strategy.

[50] Inter-Ministerial Committee on Cybersecurity from the Government of Chile, Glossary.

[51] Government of Paraguay, National Secretariat for Information and Communication Technologies (SENATICS), National Cybersecurity Plan.

[52] National Programme for Critical Information and Cybersecurity Infrastructures of the Argentine Republic.

[53] Asociación por los Derechos Civiles (ADC), Privacy Area, "*Descubriendo la agenda de ciberseguridad de América Latina: el caso de Argentina. Segunda entrega: Marco normativo"* (Discovering the cybsersecurity agenda of Latin America: the case of Argentina. Second Publication: Regulatory framework), Argentina, 2016, p.11. Available at: http://bit.ly/2fkM68z

Another country that does not have an accurate definition is Brazil, probably due to the fact that it does not have any main strategic instrument on cybersecurity. Nonetheless, it is possible to find an interesting definition collected from the *Green Book on IT Security*, which defines it as "the art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets, and critical infrastructure"[54]. This concept, which covers some of the aspects analysed, may be criticised for its failure to include a risk management approach, nor does it solve the conceptual tensions among the prevailing security paradigms.

Chile defines cybersecurity under the Supreme Decree No. 533/2015[55], which establishes the creation of an Inter-Ministerial Committee on Cybersecurity, and defines the concept as "the condition characterised by a minimum level of risk and threats to technological infrastructures, local information components and interactions over the cyberspace, as well as the set of technical policies destined to reaching such condition".

This concept, in line with the definition of cybersecurity proposed by several countries, solves basic aspects around the term, especially in the sense that the objective is to minimise and not to suppress risk, showing the perspective of need and proportionality of the measures at stake, which is compatible with a human rights approach. It also makes reference to the physical and logical infrastructures and the interactions within cyberspace, excluding the content of those interactions, thus protecting cyberspace as a platform or space to express and exchange information, but not the nature of the content, leaving aside discussions on this point, in particular, aspects related to control, censorship or surveillance of harmful content.

Last, it is important to consider the case of Colombia, which has recently submitted a new iteration on its cybersecurity policy-making paper. In 2011, the country prepared a document (Conpes 3701) on the "National Planning Policy Guidelines for Cybersecurity and Defence", defining cybersecurity as the "State's capacity to minimise the level of risk to which citizens are exposed in relation to cyber threats or incidents"[56]. This concept was criticised

[54] Presidency of the Republic, Institutional Security Cabinet, Executive Secretariat, Department of Information and Communication Security, *Livro verde segurança cibernética no Brasil*, 2010. Free translation of "*Segurança Cibernética: arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas*" (Portaria 45 SECDN, 2009).

[55] Government of Chile, Supreme Decree No. 533.

[56] National Council on Economic and Social Policy, Republic of Colombia, *"National Planning Policy Guidelines for Cybersecurity and Defence"*, 2011, p. 39.

due to lack of accuracy and the risks therein contained, specified as "cyber threats or incidents", since many situations might fit into this definition.

These criticisms were taken for the preparation of the new Conpes 3854, which presents a national policy on digital security, and a new definition of cybersecurity:

> It is the set of security resources, policies and concepts, security safeguards, guidelines, risk management methods, actions, research and development, training, suitable practices, insurance and technologies that may be used seeking availability, integrity, authentication, confidentiality and not rejection, in order to protect users and the organisation's assets in cyberspace[57].

Without detriment to the analysis of the full document and its implementation -which deserve thorough consideration-, the above-mentioned concept of cybersecurity, included in Conpes 3854, depicts the progress attained in the regional debate, which offers an interesting conception that covers the specific tools and objectives of cybersecurity, collecting elements of information security, such as the preservation of confidentiality, integrity and availability, plus authentication and no rejection and, putting the focus on the protection of information assets and users.

In this way, the concept proposed by Colombia contributes to better orienting public policy decisions on cybersecurity and, is also more functional and in line with the approach on human rights in cyber-space.

IV.C. Tension between cybersecurity and human rights in Latin America

Apart from the conceptual development of the term cybersecurity, the region has also been the stage for several cases where the application of public policies on behalf of cybersecurity was in tension with the international human rights law.

In some cases, the subject-matter is not the concept of cybersecurity, but the use of digital tools to illegitimately affect human rights, weakening people's information security in cyber-space without a clear certainty as to the need or proportion of their application.

[57] National Council on Economic and Social Policy, Republic of Colombia, *"National Planning Policy on Digital Security"*, 2016, p. 87.

Due to the impossibility of making a thorough analysis of each case, reference will be made to the categories that best illustrate the tension previously described: the legal classification of cyber-crimes affecting the exercise of human rights and the use of digital surveillance tools, which represent a potential breach of the human right to privacy.

IV.D. Legal classification of cyber-crimes and human rights

In the last five years, efforts have been made -successfully in some cases- in various Latin American countries, such as Argentina, Brazil, Chile, Peru, Paraguay and Mexico, to introduce laws which classify behaviours that represent a legitimate exercise of the right to freedom of expression, as criticising authorities publicly, creating parody accounts in social media, using certain IT tools, among others. Many of these criminal offences are not considered from a paradigm of protection of information confidentiality, integrity or availability in cyber-space, nor are they taken from a risk management approach, but rather refer to different kinds of considerations related to criminal policy matters.

In these cases, first, the challenge is to perform an analysis in order to classify certain crimes related to the use of cyber-space, based on evidence, criminal law and the international recommendations on the matter. Second, and in case the legal classification of these crimes becomes necessary, a human rights approach should be applied so that it remains within a framework of strict necessity and proportionality. Another relevant challenge is to prevent the use of the cyber-security concept as a white-card, which can justify any new legal classification in relation to cyber-space, and identify and consequently justify the legal asset protected in each case.

IV.E. Use of digital surveillance tools and human rights

As part of the discussions on cybersecurity, reference is usually made to cyber-space surveillance[58], in circumstances where there is an inverse relation since information confidentiality is negatively affected through these practices when performed in an unnecessary and disproportionate

[58] Several civil society organisations, as ADC Digital (in the already mentioned report) identify digital surveillance as one of the commonly used definitions of cyber-space -and the one which sparks greater criticism from the civil society. As was stated at the beginning of this paper, surveillance in cyber-space, especially since Snowden's revelations, is more related to the breach of cyber-security rather than to the concept's application.

manner against users. Some surveillance practices, such as mass data and metadata retention, collection and/or storage also affect the human rights to privacy and to secrecy of communications, since they constitute an arbitrary interference into people's private life.

In line with this, some States in the region have laws in place, which force Internet Service Providers to retain users' data, including location, connection hours and IP addresses used for browsing, while others have been related to several reports that reveal the use of malware with the purpose of surreptitiously surveiling specific persons.

In relation to legislation on data retention, countries such as Chile have an Internet connection data retention scheme for one year, available to the country's Prosecutor's Office, without the need to request any legal authorisation to access this data. Peru[59] and Mexico[60], on their part, have rules in place which establish location data retention for Internet users.

As to the use of malware, some reports issued by Citizen Lab from the University of Toronto[61] and by Derechos Digitales NGO[62], reveal that several States in the region (Chile, Ecuador, Paraguay, Venezuela, Mexico, Honduras, Colombia and Brazil) have acquired platforms from two companies (Hackin Team and Gamma Group), that are able to infiltrate malware into the digital devices of certain people to spy on the devices and the information captured by them.

The lack of transparency in the acquisition of these tools -primarily discovered through technical investigations and news leaks-, added to the little understanding as to whether or not their use is consistent with each country's domestic laws and the applicable human rights standards, pose a great challenge for the States in the region to have better transparency standards for the acquisition and use of data collection and processing tools.

All in all, the purpose of both practices (data retention and use of surveillance malware) serves police and intelligence objectives, and represents a big challenge ahead as to the convergence of cyber-security and human rights.

[59] Argote, Carlos, *"Vigilancia masiva en Perú: Ley Stalker",* Oficina Antivigilancia, 09/11/15. Available at: http://bit.ly/2eJxxwW

[60] Forbes Staff, "*¿De qué va la Ley de Geolocalización*?", in *Forbes*, Ciudad de México, 16/01/14. Available at: http://bit.ly/2fABRhb

[61] Related articles and reports available at: http://bit.ly/2fwmSVc

[62] Pérez de Acha, Gisela, "*Hacking Team: malware para la vigilancia en América Latina*", Derechos Digitales NGO, March 2016. Available at: http://bit.ly/1S0Tku6

V. Conclusions

Cybersecurity is a disputed concept and the debate on the matter is based on various technical and political assumptions, as no international consensus exists as to the concept's material content. As a matter of fact, there is even no consensus on the fact that the concept under discussion actually defines cybersecurity. Based on the root of the term, cybersecurity implies a kind of relationship between cyber-space and security and, this last concept also admits various viewpoints, which present the paradigms on national security, multidimensional security and human security at a high level, jointly with the technical notion of information security.

Considering the statement described above, the public debates on cybersecurity should not assume the existence of a shared concept on the matter, let alone extend cybersecurity to a national security paradigm, which is close to obsolescence. In this manner, beyond embracing or criticising the concept, it is necessary to clarify the values and conceptions expressed when using the term, recognising the existence of various looks in its regard and aiming at reaching a common understanding that recognises those looks. Also, it may be concluded that cybersecurity is an issue that comprises several domains, and up until now, few countries in Latin America have been able to address it comprehensively.

As was previously observed, cybersecurity -regardless of the definition adopted- is a question that should be addressed systemically, considering several dimensions, as the adoption of adequate technical standards, effective legal policies, cultural gaps, diplomacy and international standards, among others. In this way, addressing cybersecurity comprehensively is not just a technical, police, educational or diplomatic problem, but it includes all of those aspects and, to make it effective, it is important to engage as many stakeholders as possible and a management model that includes them into the corresponding processes.

Within the Latin American framework, the debate on cybersecurity has lacked (and still lacks, in some cases) a systemic view and rather focuses on specific problems and discourses, which tend towards a reductionist vision of the problem. However, the efforts made by countries such as Chile, Colombia, Jamaica and Paraguay, since 2015, have shown some progress in the design of policies, with a more inclusive vision of cybersecurity.

It still is important to analyse whether the implementation of these policies is consistent with the statements they claim, and whether they are capable of balancing and building on the full respect for human rights along the process.

V.A. Recommendations to guide the debate on cybersecurity towards human rights standards

Need to take ownership of a cybersecurity concept based on human rights and to promote the creation of strategies in that regard.

As was pointed above, at present, there is no concept of cybersecurity that raises broad consensus in the international community. This situation represents big opportunities to promote a concept on cybersecurity that includes a vision of human rights at its core.

In that sense, there are interesting proposals, as the one made by the Freedom Online Coalition, which may serve as a starting point, since they expressly establish the application of human rights in cyberspace, and restrict the elements of security to a technical conception of information security.

However, it is also possible to go beyond in the concept of cybersecurity to promote human rights through the use of paradigms as that of human security, which do not limit the conception of security to national or international stability, to the dimension of public security or to the preservation of certain information attributes.

The application of the human security paradigm to cyberspace offers the opportunity to include elements of social justice into the debate, which in this context, may be translated into an active agenda for non-discrimination, access, economic development and self-determination, as a manifestation of a person's freedom from fear, want or misery and freedom to lead worthwhile lives[63].

In this sense, the specific recommendation is that besides generating concepts of cybersecurity that consider a paradigm for risk management and for the protection of platforms and infrastructures, as was already mentioned, elements of human security should also be included to emphasise the possibilities of development presented by cyber-space and the need to expand the reach and confidence in that environment, adding a positive phase to a problem that tends to be tackled in a reactive way.

All in all, it is impossible to give a specific and detailed proposal on how cybersecurity should be defined, since this decision will depend on the political and social context where that definition is to be introduced, and on the particular interests of the stakeholders involved. It is advisable to find a convergence of the various perspectives for this concept and, in particular

[63] Inter-American Institute of Human Rights, *supra* note 15.

for civil society, include the human rights perspective into cyber-space in order to attain greater access and fewer barriers to this environment.

Implement cybersecurity governance solutions considering active roles for the multiple stakeholders.

Finally, as for the relationship between Internet governance and cybersecurity, there is a big challenge ahead in terms of the need to integrate those spaces where security matters are currently discussed with the more consolidated Internet governance forums. In this point, it is important to share with the governments in the region -many times more experienced in security debates than in Internet governance- the lessons and experiences learnt in Internet governance spaces, inviting them to participate in those discussions.

For non-governmental players, it is a big challenge to understand the spaces where security matters are traditionally discussed, identifying dominant debates and developing strategies to become part of those spaces in a constructive way.

Beyond the relationship between spaces where security and Internet governance are discussed, it is important to overcome the rigid conception about the roles to be adopted by the various players in the public debate, and implement innovative governance models for cybersecurity that include the multistakeholder paradigm and that can add the capacities of all their members in order to create a secure cyber-space.

The afore-mentioned is particularly true in terms of civil society, whose players are not always considered in these debates, and are of special importance to develop cybersecurity models that build on an unconditional respect to human rights.

Chapter Three

Net Neutrality, Zero-rating and The Marco Civil

Luca Belli[1]

Introduction

Over the past decade, net neutrality (NN) discussions have been proliferating all around the world, involving a variety of stakeholders both at the Brazilian level and within various international fora. NN is a non-discrimination principle aimed at preserving Internet openness and facilitating the full enjoyment of end-users rights and, for this reason, it has been enshrined in various national and international regulatory instruments. At the Brazilian level, NN is explicitly protected by Law 12.965/2014, better known as the Marco Civil da Internet MCI *i.e*. the Civil Rights Framework for the Internet, which is a federal law setting fundamental principles and rules framing Internet regulation in Brazil. The evolution of the NN debate has greatly influenced the elaboration of the MCI and the Presidential decree aimed at specifying some MCI provision. Notably, over the public consultations leading to the elaboration of the decree, zero rating (ZR) and their compati-

[1] Luca Belli, Ph.D. is Senior Researcher at the Center for Technology and Society (CTS) of Fundação Getulio Vargas Law School, Rio de Janeiro, where he leads the 'Internet Governance @ FGV' project. Luca is also associated researcher at the Centre de Droit Public Comparé of Paris 2 University. Before joining CTS, Luca worked for the Council of Europe Internet Governance Unit; served as a Network Neutrality Expert for the Council of Europe; worked as a consultant for the Internet Society and as a Ph.D. researcher at Université Panthéon Assas (Paris 2). He is also the founder and co-chair of the Dynamic Coalition on Network Neutrality of the United Nations Internet Governance Forum, as well as the co-founder and co-chair of the Dynamic Coalition on Community Connectivity and the Dynamic Coalition on Platform Responsibility. Luca's works on net neutrality have been used i.a. by the Council of Europe in order to elaborate the Recommendation of the Committee of Ministers on Network Neutrality. He is author of De la gouvernance à la régulation de l'Internet, edited by Berger-Levrault, Paris, and co-author of the Net Neutrality Compendium, edited by Springer. Luca is also co-editor of Medialaws.eu.

bility with NN were one of the most hotly debated topic. ZR is the practice of sponsoring access to specific applications that do not count against the user's monthly data caps and, between 2014 and 2016, the analyse of such practices has become intimately intertwined with virtually every NN debate. The purpose of this article is to contextualise NN and ZR, in order to explain the recent policy and regulatory development in Brazil and distil lessons that may be useful in other contexts.

First, the article examines the rationale for NN, providing an overview of the NN debates around the world and stressing the instrumental role of the NN principle in order to allow the full enjoyment of Internet users' fundamental rights. (Part I) After having analysed NN from a more general perspective, I briefly analyse ZR practices, highlighting the existence of various ZR models and scrutinising their (non-)compatibility with NN. (Part II) Particularly, I point out that a considerable number of ZR schemes aim at creating new consumers of predefined services rather than new Internet users, thus predefining the way in which individuals may use the Internet and limiting end-users' potential to create disruptive innovation. Such scenario de facto redefines Internet users as mere consumers rather than protecting their peculiar feature of being "prosumers" *i.e.* both consumers and producers of information, ideas and innovation.

Subsequently, I analyse the MCI and its core role as a principle-law promoting human rights, full exercise of citizenship and universal access and innovation, stressing that the MCI considers NN as one of the core principles that allow the achievement of such goals, orientating the discipline and use of the Internet in Brazil. (Part III) Besides being exemplifying the inclusion of NN alongside constitutional values, such as the protection of human rights and the promotion of innovation, the Brazilian case is very useful from a practical perspective, in order to explain that ZR practices risk to reduce severely Internet openness, *de facto* limiting individuals' use of Internet connection to a limited number of sponsored applications. In this regard, I argue that the combination of reduce data-caps and sponsored services has the potential to reduce the general-purpose nature of the Internet transforming it into a predefined-purpose network while fostering artificial scarcity. In fact, sponsoring specific applications only make sense when combined with limited data caps, thus representing an incentive for operators to keep monthly data allowance as reduced as possible, rather than promoting the use of an open Internet. Lastly, I provide some initial suggestions on what policy choices could avoid this phenomenon, namely the promotion of community networks that may sustainably expand Internet access, building

infrastructure from the edges, while empowering individuals and triggering positive progress amongst previously-unconnected communities.

I. The Net Neutrality Debate

The proliferation of NN debates has prompted a number of stakeholders to position themselves on the matter, stimulating the elaboration of both national and international NN policies.[2] Although different advocates have proposed various flavours of NN, the majority of stakeholders agree on the substance of NN, defining it as "the principle according to which Internet traffic is treated without unreasonable discrimination, restriction or interference regardless of its sender, recipient, type or content or terminal equipment."[3] The concrete implementation of such principle is however hotly debated and NN discussion have been proliferating at both international and national level, triggering controversies – and intense lobbying – with regard to what should be considered as "reasonable" traffic management as well as on the very necessity (or not) to regulate traffic management.

NN controversies focus on the degree of leeway that network operators should have in implementing Internet traffic management (ITM) techniques able to "discriminate" against specific content, applications and services that cross their electronic networks. Although this may seem as a purely technical issue, it has great social, juridical and economic implications. Indeed, the implementation of differentiated treatment through a variety of ITM techniques may unduly limit users' freedom of expression or competition, when such measures are not necessary and proportionate to the achievement of a legitimate aim.[4] Indeed, NN

[2] Belli, Luca and Foditsch, Nathalia "Network Neutrality: An Empirical Approach to Legal Interoperability" on Belli, L. and De Filippi, P. (eds), Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet, Part III, Springer International Publishing, November 6, 2015.

[3] See IGF, Policy Statement on Network Neutrality, Outcome of the 15th United Nations Internet Governance Forum, November, 2015.

[4] Belli, Luca and van Bergen, Matthijs, "Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet ", Council of Europe, Steering Committee on Media and Information Society CDMSI, 4 th meeting, Strasbourg, 3-6 December 2013, Misc19, available at: http://bit.ly/2fMPiKB; Federal Communications Commission (FCC), "Report and Order on Remand, Declaratory Ruling, and Order on the Matter of Protecting and Promoting the Open Internet", GN Docket No. 14-28, 2015; Council of Europe, Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, January 13, 2016, available at: http://bit.ly/2f8FlWS; Belli, Luca and Foditsch, Nathalia, *supra* note 2.

discussion have gained particular prominence due to the fact that ITM techniques can be used not only for legitimate purposes but also to disfavour competing services, unduly blocking or downgrading them, or favour commercial partners through prioritisation.[5] Such undue limitations are possible in the absence of NN policies and they have been proven in a variety of national contexts such as the US[6], Chile[7] or the EU[8], thus leading to the elaboration of NN frameworks.

It is important to note that ITM plays a key role in guaranteeing the smooth operation of electronic networks, for instance by preserving network security and integrity. However, operators may misuse ITM techniques to favour or disfavour specific services, based on purely commercial considerations. Indeed, the technological evolution of the past fifteen years has allowed operators to use ITM techniques to target specific applications, services or content, putting in place so-called application-specific measures. Such application-specific measures may be exploited to discriminate against services that are in direct competition to the services that sustained the telecoms industry for decades, such as voice and messaging,[9] or the applications that compete with the commercial partners of the operators. Indeed, while vertical integration can be beneficial from an industrial organisation perspective, it seems understandable that the vertical integration[10] of network operators

[5] Body of European Regulators for Electronic Communications (BEREC), "A view of traffic management and other practices resulting in restrictions to the open Internet in Europe", findings from BEREC's and the European Commission's joint investigation, BoR (12) 30, May 29, 2012. Available at: http://bit.ly/2fRLVCU

[6] Federal Communications Commission, *Madison River Communications, LLC and affiliated companies*, Acct. Nº FRN: 0004334082, Washington D.C., 2005. Available at: http://bit.ly/2f8Dul1; Federal Communications Commission, "Commission Orders Comcast to End Discriminatory Network Management Practices", FCC News Media Information 202/418-0500, August 1, 2008. Available at: http://bit.ly/2cpWlsb

[7] Tribunal de Defensa de la Libre Competencia (TDLC), *Voissnet vs CTC,* Judgment 45-2006, October 2006.

[8] *See* BEREC, *supra* note 5.

[9] Broadband Internet Technical Advisory Group (BITAG), "Port Blocking", a Broadband Internet Technical Advisory Group Technical Working Group Report, August 2013. Available at: http://bit.ly/2fQYnVb; *See also* BEREC, *supra* note 5.

[10] It should be noted that vertical integration phenomena do not exclusively concern network operators and have also been observed with regard to online platforms. (European Commission, "Antitrust: Commission sends statement of objections to Google on comparison shopping service; opens separate formal investigation on Android", press release, April, 2015. Available at: http://bit.ly/1FQxesN). Although this latter type of vertical integration has the potential to harm Internet openness and deserves the attention of regulators, it should be noted that NN policies do not focus on online platforms and rather focus on operators acting at the access layer. *See* BEREC, *supra* note 5; Belli and Foditsch, *supra* note 2.

together with Content and Application Providers (CAPs) offers concrete incentives to privilege the traffic of the commercial partners, via paid prioritisation,[11] and blocking or slowing down[12] the traffic of competing services. Therefore, although ITM can offer welfare-enhancing benefits to both users and operators, it can also be exploited for abusive purposes that solely benefit a narrow range of stakeholders *i.e.* operators and their commercial partners. Such undue discrimination may have nefarious consequences not only on free competition but also on users' freedom to seek, impart and receive information without interference, which is guaranteed by a variety of international law instruments and by the majority of existing national constitutions.[13]

Importantly, it must be noted that the NN debate does not represent a binary choice between no traffic management and free traffic management. In fact, even the most vocal supporters of non-discriminatory treatment of Internet traffic admit that NN has exceptions for reasonable traffic management, while even the strongest opponents of NN admit that operators should not engage in anti-competitive practices. While it is true – and openly agreed by NN advocates – that discriminatory traffic management is beneficial, when necessary and proportionate to the achievement of specific legitimate purposes,[14] the Gordian knot is the definition of the extent to which traffic management practices may be considered as legitimate, necessary and proportionate. In this regard, it must be noted that, although divergent views persist with regard to ITM, stakeholders generally agree that discriminatory traffic management can be considered as reasonable as long as it is necessary and proportionate for the achievement of some specific purposes. Particularly, ITM is generally deemed as reasonable for network-security and network-integrity purposes or to prioritise emergency services, in case of force majeure, or when protocol-specific[15] ITM becomes

[11] Paid prioritisation refers to the practice of giving preferential treatment to the data streams of the operators' commercial partners. This practice is presented by operators as a technique to deliver content with guaranteed quality of service. Paid prioritisation has been criticised due to its potential to create "Internet fast lanes" and "dirty roads", thus favouring commercial partners, while disfavouring services lacking the financial capacity necessary to pay for priority.

[12] This practice is also referred to as "throttling" and includes techniques specifically limiting the user upload or download rates of certain types of data flows. This technique has been deemed as controversial when not transparently disclosed and used to discriminate against competing services' data-streams.

[13] Belli, Luca and Foditsch, Nathalia, *supra* note 2.

14 *See* IGF, *supra* note 3; *See* BEREC, *supra* note 5.

[15] The term "protocol-specific" qualifies and ITM technique that targets or affects a class of applications running on a specific protocol, such as VoIP. Differently from application-

necessary to mitigate the effects of congestion[16] because protocol-agnostic ITM is not workable.[17] Moreover, the utilisation of Content Delivery Networks[18] (CDNs) is also generally considered as compatible with NN, because CDNs improve performance and ease congestion by adding capacity to electronic networks, rather than degrading other communications passing through the same routers.[19]

Besides being used to manage congestion phenomena, ITM measures may also be beneficial in dealing with malicious usages of the Internet such as spam, cyberattacks and illegal content and services. However, as noted above, while acquiring the capability to manage Internet traffic in more precise and efficient fashion, *e.g.* filtering out spam or prioritising latency-sensitive applications in case of congestion, several network operators have also acquired concrete incentives to discriminate against specific resources for purely commercial reasons. As such, ITM techniques may be used to guarantee the smooth

specific ITM, which target a specific application, protocol-specific ITM targets an entire class of applications exploiting the same protocol. The term "protocol-specific" is contrary to "protocol agnostic" that qualifies an ITM technique that does not target or affect a specific class of applications. *See* Bastian et al., "Comcast's Protocol-Agnostic Congestion Management System", RFC 6057, December, 2010. Available at: http://bit.ly/1BKFpF4

[16] It must be noted that the analysis of congestion phenomena is not as simple as it may appear. Notably, it is particularly difficult to objectively identify the real cause of network congestion. As noted by Frieden (2014), "the actual cause of […] congestion remains elusive. Content creators and distributors speculate whether retail ISPs have deliberately caused congestion, by refusing to further upgrade network capacity, or by allocating available capacity in ways that bolster the probability of congestion for the traffic of specific content types and sources. ISPs reject this scenario and cite to less nefarious circumstances such as weather, home-based holidays and the decision of content distributors, such as Netflix, to release an entire season's worth of program episodes". *See* Frieden, Rob, "Net Bias and the Treatment of 'Mission-Critical' Bits", TPRC Conference Paper, March 24, 2014. Available at: http://bit.ly/2eXhbRE

[17] When different stakeholders attending the IGF 2015 where asked to express their feedback on such characterisation of reasonable traffic management, 84% expressed a favourable or very favourable assessment..See IGF, Secretariat, "Idea Rating Sheet - Net Neutrality", Survey 645723, 2016. Available at: http://bit.ly/2f8Z3lh. Similar exceptions to non-discriminatory treatment can be found in the majority of existing NN frameworks.

[18] CDNs are network systems that intermediate between the source of an application provider and the operator with the purpose of speeding up the transmission of data. *See* Pallis, George and Vakali, Athena, "Insight and Perspectives for Content Delivery Networks", Communications of the ACM, Vol 49, Nº 1, January 2006. Available at: http://bit.ly/2fNh5us. They do so by locally hosting copies of select data (mirroring), and when an end user requests it, the CDN intercepts the request and sends the data from the local hosting point instead of the remote source. Hence, CDNs improve performance by reducing the total distance that data-packets have to travel to reach their destination.

[19] BEREC, *supra* note 5; FCC, *supra* note 4.

functioning of the Internet but also to (dis)favour specific data-packets, thus having the capability to distort the market and alter users' freedom to seek, impart and receive information without interference, in the total unawareness of end-users. In this regard, a variety of Internet companies have argued that network operators "have the incentive to discriminate and block Internet traffic, they have the tools to carry this out and they also have the ability to hide their actions by distributing the blame to other stakeholders."[20]

Therefore, discriminatory ITM can be used for anticompetitive purposes but can also undermine users' fundamental freedom of expression. According to International human rights law, states have a negative obligation of non-interference in individuals' possibility to freely seek, impart and receive information and ideas as well as a positive obligation to protect individuals from adverse effects that the actions of private companies or of other individuals may produce on their freedoms.[21] In this sense, the jurisprudence of the Inter-American Court of Human Rights (IACHR) as well as of the European Court of Human Rights (ECtHR) seems to be unequivocal as regards the relevance of non-discriminatory treatment of information and ideas. On the one hand, the IACHR has consistently argued that "equity must regulate the flow of information", while stressing that state have a positive obligation to "extend equity rules, to the greatest possible extent, to the participation in the public debate of different types of information, fostering informative pluralism".[22] On the other hand, the ECtHR has continuously stated that freedom of expression "applies not only to the content of information but also to the means of dissemination since any restriction imposed to the [means] necessarily interfere with the right to receive and impart information".[23] Such considerations have also been repeatedly ech-

[20] *See* Internet Association, "Comments of the Internet Association in response to the Federal Communications Commission's ("Commission" or "FCC"), May 15, 2014". Available at: http://bit.ly/1qYaLAF

[21] *See* UN Human Rights Committee, General Comment 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 2187th meeting, March 29, 2004; *See also* Council of Europe Commissioner for Human Rights, "Reports On the Rule Of Law and the Internet", December 2014; See European Court of Human Rights, *López Ostra v. Spain*, Judgment Nº 16798/90, §44-58, December 9, 1994; European Court of Human Rights, *Khurshid Mustafa and Tarzibachi v. Sweden*, Judgment Nº 23883/06, December 16, 2008.

[22] Inter-American Court of Human Rights, *Kimel v. Argentina*, Merits, Reparations and Costs, Series C Nº 177, May 2, 2008, para. 57; Inter-American Court of Human Rights, *Fontevecchia y D'Amico v. Argentina*. Merits, Reparations and Costs, Series C Nº 238, November 29, 2011, para. 45.

[23] European Court of Human Rights (ECHR), *Autronic AG v. Switzerland*, May 22, 1990,

oed by the Special Rapporteurs on Freedom of Expression that have taken a proactive approach to NN protection, jointly stressing that "[t]here should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application."[24] Accordingly, European governments have decided to explicitly protected NN as a human rights norm. Indeed, the 47 Council of Europe members have enshrined the protection of NN into a Recommendation of the Committee of Ministers[25], thus reiterating their commitment to NN, openly expressed since the 2010 Declaration on network neutrality.[26]

Such commitments are due to the observation that non-discriminatory access to and circulation of content, applications and services does not only facilitate free flow of information but can also be beneficial in reducing barriers to enter the market of creativity and innovation. In this regard, it must be noted that Internet users have the peculiar feature of being "prosumers" *i.e*. not only consumers of information but also producers of potentially disruptive innovation. For this reasons, stakeholders point out that NN is key in "preserving Internet openness; fostering the enjoyment of Internet users' human rights; promoting competition and equality of opportunity; safeguarding the generative peer-to-peer nature of the Internet; and spreading the benefits of the Internet to all people."[27] Indeed, in the online environment, the freedom to receive and impart ideas means freedom to access and share innovation, actively contributing to the evolution of the Internet. Hence, by reducing operators possibility to interfere with the users' freedom of expression, non-discriminatory treatment of Internet traffic has the potential to allow Internet users to be developers of innovation and to offer potentially disruptive new application and services, competing on level playing field with established market players. In this sense, it is particularly important to stress that Internet users are to be considered as prosumers and that NN policies precisely aim at facilitating such empowering feature. Therefore, it seems incorrect to argue that NN policies conflict with private

Judgement Nº 12726/87. Available at: http://bit.ly/2h4jNf6; ECHR, *Ahmet Yıldırım v. Turkey*, Judgment Nº 3111/10. Available at: http://bit.ly/2hoQneG

[24] Frank LaRue (UN), Dunja Mijatović (OSCE), Catalina Botero Marino (OAS), and Faith Pansy Tlakula (ACHPR), "Special Rapporteurs' Joint Declaration on Freedom of Expression and the Internet", June 1, 2011. Available at: http://bit.ly/1wnld8U

[25] CoE, *supra* nota 4.

[26] Council of Europe, Declaration of the Committee of Ministers on Network Neutrality. Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies, 2010. Available at: http://bit.ly/2hAl4dx

[27] *See* IGF, *supra* note 3.

sector interests, as claimed by some NN opponents. On the contrary, NN policies are usually supported by a wide spectrum of business actors. In fact, supporters of the NN principle include not only human rights advocates and academics, but also an ample range of CAPs and start-up innovators.[28] On the contrary, detractors of NN are generally telecoms operators with relevant market power and self-regulation partisans, such as libertarians as well as some academics, arguing that Internet access providers should be free to manage Internet traffic as they wish, and that NN regulation may reduce innovation at the network level and impede the implementation of new business models, such as pay-for-priority.[29]

Due to the evolution of Internet usage patterns[30] – particularly, the growth of video-on-demand and online gaming – operators have been asserting their willingness to utilise ITM to differentiate traffic[31] and propose pay-for-pri-

[28] Start-ups and established Internet companies have regularly demanded strong NN provisions in the various counties where NN policies have been discussed. As an instance, in EU start-ups established the "Start-ups for net neutrality" initiative that was also replicated in Brazil while, in India, nearly 700 start-up founders urged Prime Minister Modi to defend NN. *See* http://bit.ly/2g4EMCn

[29] Wu, Tim and Yoo, Christopher, "Keeping Internet neutral?: Tim Wu and Christopher Yoo Debate" on *Federal Communications Law Journal*, Vol. 59, N° 3, 2007. Available at: http://bit.ly/2gdkmWW

[30] While in the 1990s, Internet traffic was predominantly made of law-bandwidth and latency-tolerant email exchanges, in the 2000s the diffusion of video downloading and peer-to-peer applications started to generate a more bandwidth-intense usage of the Internet, while the diffusion of Voice over IP, video streaming and multi-player gaming generalised latency-sensitive applications whose quality declines with delay. *See* Ou, George, "Managing Broadband Networks: A Policymaker's Guide", The Information Technology and Innovation Foundation (ITIF), December 2008. Available at: http://bit.ly/1Fz48ui

[31] Traffic differentiation is based on the use of any ITM technique "that classifies and applies potentially different treatment to two or more traffic flows contending for resources on a network (a flow being a group of packets that share a common set of properties)." BITAG, "Differentiated Treatment of Internet Traffic", 2015, available at: http://bit.ly/2gFtWxN. Differentiation is based on the exploitation of multiple traffic classes that may have varying levels of priority and can be implemented using Differentiated Services (DiffServ), Integrated Services (IntServ) and/or Multiprotocol Label Switching. *See* Grossman, D., "New Terminology and Clarifications for Diffserv. Request for Comments: 3260", April, 2002. Available at: http://bit.ly/2hSsaKx; Baker F., Polk J. Polk and M. Dolly. M., "A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic". Request for Comments: 5865. Available at: http://bit.ly/2gNRA03; y Rosen, E. y col., "Multiprotocol Label Switching Architecture" Request for Comments: 3031, 2012. Available at: http://bit.ly/2gPz065. Differently from best-effort traffic, "intserv- or diffserv- enabled traffic relies on differential scheduling mechanisms at congested routers, with packets from different intserv or diffserv classes receiving different treatment." (*See* Floyd, S. and Allman, M., "RFC 5290: Comments on the Usefulness of Simple Best-Effort Traffic", July, 2008. Available at: http://bit.ly/2fqTt0B) Floyd, S. and Allman, M., "RFC 5290: Comments on the Usefulness of Simple Best-Effort Traffic", Network Working Group,

ority offerings, in order to support the investment[32] aimed at the expansion of network capacity.[33] Particularly, the recent growth in video streaming has required economic efforts to handle increasing traffic demands[34], thus prompting operators to propose the extensive use of ITM to charge different prices for different quality levels. In this sense, several operators have suggested the need for additional fees, beyond the existing Internet access fees, arguing that based on pay-for-priority schemes would provide extra revenue for network-enhancement investment. While it is true that NN policies impede that operators extract additional revenues from pay-for-priority offerings, it seems almost unrealistic to state that further revenues would automatically lead to more infrastructure investment – or to suppose that operators would invest more in infrastructure in the absence of NN provisions. In this regard, it seems relevant to note that, in spite of the fact that its net profit grew of 179%[35] in the first trimester of 2016, Telefônica Brasil openly supported the introduction of data caps within fixed networks in Brazil, arguing that data caps in fixed networks represent a needed measure to stimulate investments.[36]

Furthermore, while pondering the necessity of pay-for-priority models in order to finance network investments, it seems important to stress that end-users do remunerate operators for Internet access and legitimately expect the possibility to access and receive any content, application or service of their choice. In this sense, NN aims at avoiding that network operators impose two-sided pricing on the Internet, charging an extra fee to access specific content, applications or services. Such practice may indeed distort the market and potentially preclude access to those content and applications that do not enter into a commercial relation with operators.[37] Furthermore, it is essential to note

Internet Engineering Task Force, July 2008. Available at: http://bit.ly/2fqTt0B

[32] It is important to stress that operators are not the only economic actors bearing relevant costs and investments. As noted by Felten (2013), CAPs should not be considered as free-riding operators' infrastructure due to their significant recurring and transit costs as well as major investment to bring their traffic as close as possible to end-users. *See* Felten, Benoît, "There's No Economic Imperative to Reconsider an Open Internet", Diffraction Analysis, April 3, 2013. Available at: http://bit.ly/2ga5dGb

[33] Bello, Pablo and Jung, Juan, "Net Neutrality: Reflections on the Current Debate", Global Commission on Internet Governance (GCIG), Paper N° 13, published by the Centre for International Governance Innovation (CIGI) and Chatham House, May 2015. Available at: http://bit.ly/2g9YewV

[34] OECD, "The Development of Fixed Broadband Networks". OECD Digital Economy Papers., No. 239., OECD Publishing, 2014.

[35] *See* http://bit.ly/2evlnbv

[36] *See* http://vivo.tl/2eVKTGF

[37] Economides, Nicholas and Tåg, Joacim, "Network neutrality on the Internet: A two-

that the attractiveness of the Internet is a function of the user's possibility to freely access, create and share content, applications and services, which "are the *raison d'être* of the Internet [because] without e-mail, the Web, social media, VoIP and so on, the Internet would be (literally) useless."[38] Hence, basing discrimination amongst content, applications and services on commercial criteria risks jeopardising the very rational of the Internet, *i.e.* providing an open and general-purpose platform for communication and innovation. This latter point is of particular relevance not only in light of the fact non-discriminatory ITM is instrumental to allow any user to share innovation but, mainly, because the strong majority of business actors within the Internet ecosystem are not network operators but rather (commercial or non-profit) online services, stat-ups or regular enterprises having online presence. The majority of such business players would not have the financial capacity to afford prioritisation – or to be zero-rated, as we will point out in the next section – and for this reason, they have regularly sided with NN advocates, demanding strong safeguards against discriminatory ITM. In this sense, it is telling that, in a variety of countries, start-ups created *ad hoc* coalitions demanding strong NN provisions[39] while a wide range of Internet companies and tech giants have been openly advocating that "preserving the Internet's neutrality ensures that it remains an engine for economic growth, innovation, and democratic values."[40]

Many of the concerns that have been voiced over the past decade of NN debates are currently re-emerging with regard to ZR. Indeed, NN policies have been adopted with the goal of avoiding that operators' choices may jeopardise the full enjoyment of Internet users' rights, while limiting Internet openness. For this reason, ZR opponents largely coincide with NN advocates, while supporters of ZR usually coincide with detractors of NN. In the next section, we will provide a brief taxonomy of ZR models, based on Belli[41], scrutinising ZR compatibility with the NN rationale and stressing what could be some costs and benefits of such practices.

---

sided market analysis" on *Information Economics and Policy Journal*, Vol. 24, February 2012, p. 91–104. Available at: http://bit.ly/1NCEDyX

[38] Clark, David and Blumenthal, Marjory, "The End-to-End Argument and Application Design: The Role of Trust", on *Federal Communications Law Journal*, Vol. 63, Nº 2, Article 3, March 1, 2011. Available at: http://bit.ly/2fR3ODW.

[39] *See e.g.* Startups for Net Neutrality http://bit.ly/2fQwTx3; Startups por uma Internet Livre http://bit.ly/2fL7Jzi

[40] *See supra* note 20.

[41] Belli, Luca, "Net Neutrality, Zero Rating and the Minitelisation of the Internet", on *Journal of Cyber Policy*, Vol. 2, Londres, Routledge, 2016.

II. Zero Rating Models under a Net Neutrality Perspective

The term ZR generally describes business practices whereby operators or a third party sponsor the data consumption related to a limited set of applications or services, which may be accessed by a mobile network users, without incurring in charges related to data consumption. Hence, the data consumption of ZR services is not counted against users' data allowance. Sometimes, ZR services can be accessed with no need to have a data plan, although, usually, there are combined with a wide range of data plans. Such practices are usually based on the positive discrimination of specific applications and have been proposed in developing as well as developed countries, triggering a new wave of NN discussions. Several forms of ZR exist and can be categorised in: (i) application ZR, (ii) application sponsoring, (iii) ZR platforms and (iv) application-agnostic data sponsoring.[42] The same provider may engage in several ZR practice in several countries or within the same country. The ZR taxonomy will be briefly analysed below, stressing the compatibility or not of the various ZR types with the NN rationale. Subsequently, ZR will be considered from ta Brazilian perspective.

ZRs aim at achieving two objectives which can be seen as fundamental, from the perspective of both operators and big Internet companies, *i.e.* the attraction of subscribers from competitors' networks and the creation of new customers. On the one hand, price differentiation schemes such as ZR acquire an essential role to attract customers and restore growth of operators' profits, which are increasingly tending towards flatness in several regions of the world – particularly, in Western Europe.[43] As such, popular services such as dominant social networking sites are zero rated by operators in order to attract users and increase their subscribers' base. Such scenario is patent in Brazil, where operators zero rate only three dominant social networks Facebook, Twitter and WhatsApp and the popular music-streaming application Deezer. On the other hand, CAPs with sufficient financial capacity may be keen to sponsor data usage of their specific services thus paying to operators a sort of right to preferential access to subscribers or new subscribers, whose personal data will be subsequently collected and monetised. This latter model can be defined as application sponsoring and slightly differ from the application ZR model. In the application ZR model,

[42] *Id.* This taxonomy is further analysed..

[43] Ovum, "Telecoms, Media and Entertainment Outlook 2015", Ovum Telecoms and Media, 2015. Available at: http://bit.ly/1MDDHvC.

the operator bundles Internet access service and unlimited use[44] of a given application – or a specific class of applications, such as video streaming apps or instant messaging apps – and does not receive sponsoring fees from third parties. On the contrary, in the application-sponsoring model, the costs that operators attribute to the use of a given application are charged to the application provider, which undertakes the role of sponsor. Application sponsoring is particularly enticing from the operators' perspective because the costs are charged to the sponsor, while the proposed bundle of capped internet access and sponsored services is likely to attract new subscribers. Therefore, in both applications ZR and application sponsoring the user is not billed for accessing a specific service, the main difference between this models being the identity of the sponsor that bears the cost established by the operator to access the application.

The abovementioned forms of ZR may give rise to various problems, when analysed under the lenses of NN policies. As mentioned above, the rationale of NN is to prevent operators from discriminating against specific application for commercial reasons, thus avoiding operators' undue interferences with users' freedom to use the Internet as they wish, including sharing innovation on a level playing field. On the contrary, it seems obvious that the decision to sponsor or zero rate a specific application is taken on a purely commercial basis. Indeed, both application ZR and application sponsoring have the inner purpose to direct users' attention towards a service perceived as free, thus orientating user choice to the cheapest service rather than the best or most useful service. As stressed above, applications to be zero rated are selected by operators, based on the consideration that their popularity – which frequently equals to market dominance – may attract users, or due to the application provider financial capacity to subsidise users' access to its application. Although these may seem as a mere market practices, it is important to understand what could be the impact of such practices on the Internet ecosystem as a whole. The key question is indeed to understand whether they have the potential to distort the Internet ecosystem, subjecting applications' attractiveness to the financial capacity of the provider rather than to the usefulness, efficiency and creativity of a given service.

It seems understandable that the abovementioned practices may be beneficial for the application sponsor. In this regard, it may be noted that,

[44] It must be noted that, sometimes, access to ZR applications is not unlimited but rather limited through a specific cap. In this sense, for instance, operator TIM Brazil zero-rates WhatsApp while defining a specific cap of 50Mb per day.

when the online review Slate experimented the potential attractiveness of ZR, communicating to "some would-be listeners that [a given Slate] podcast wouldn't count against the data plans on their smartphones [the targeted] group was 61% more likely to press play."[45] However, although ZR it may look as beneficial to have free access to specific services, it should be noted that such practices have the potential to turn the Internet into a predefined-purpose network orientating the choice of the majority of users towards the consumption of sponsored applications, rather than empowering users with the possibility of being active producers of innovation.[46] In this regard, data analysed by the Alliance for Affordable Internet (A4AI) in various developing counties seem to show that ZR may ultimately distort freedom of choice, having a remarkable impact on how individuals decide to use the Internet. Indeed, although the majority of individuals taking part to the A4AI survey argued that they would prefer to have full Internet connection for a limited time or limited data volume rather than unlimited access to specific services,[47] ZR practice induces 72% of users not to keep on using ZR services. Particularly, A4AI points out that "35% of all zero-rating users continue to use the zero-rated service and a paid plan [and] 37% continue to use […] zero-rated service in combination with public WiFi" while "28% of all zero-rating users no longer use a zero-rating plan and are now paying customers."[48]

The adoption of ZR in developing countries has acquired particular relevance, in light of its proposed use to foster the adoption of online services in areas or countries where Internet penetration is particularly low, in order to bridge existing digital divides.[49] In this regard, some forms of ZR have

[45] Knutson, Ryan, "Will Free Data Become the Next Free Shipping?", *The Wall Street Journal*, October 24, 2014. Available at: http://on.wsj.com/1TYfgcc

[46] Belli, Luca, *supra* note 37

[47] Particularly, A4AI research stresses that "one-third of respondents said they would prefer access to all websites/apps, with a restriction on the amount of data that could be used. A minority of users (18%) preferred having unlimited data for accessing a limited number of sites (i.e., the way in which most zero-rated services are currently implemented). In sum, when faced with a restriction in exchange for "free" data, a majority (82%) of users prefer access to the full Internet, even if that access is limited in terms of time or by a data cap." *See* A4AI, "Digging into the Data: Is Zero Rating Really Bringing People Online?", 2016. Available at: http://bit.ly/1UCwNab

[48] *Ibid.*

[49] Digital divides between and within countries are due to a number of factors. First, connectivity may be hard to foster due physical barriers such as lack of infrastructure or geographical barriers – such as mountain chains or deserts – raising the cost of infrastructure deployment and making it scarcely profitable, particularly when the population of such

been presented as necessary and proportionate exceptions to NN,[50] allowing unconnected individuals to freely access selected online services rather than being completely disconnected. On the contrary, a number of critics have voiced the possibility that ZR practices be used to unduly influence and distort individuals' freedom of opinion, arguing that sponsoring a limited number of applications can limit individual's Internet experience to an artificial bubble. Such scenario has been concretely described by Mirani who suggested that access to a limited selection of applications de fact leads users to believe that zero-rated service "is the Internet,"[51] as it emerged from surveys conducted in various developing countries. In this sense, it is important to note that commercial practices having the potential to affect the usage patterns as well as the freedom of opinion of such a strong portion of users should be carefully scrutinised by regulators in order to understand the potential (social and economic) costs and benefits that they may determine.

Conspicuously, a first type of concerns to be considered is whether the concentration of users towards sponsored applications has the potential to affect negatively media pluralism and, consequently, individuals' possibility to form freely their own opinion. This risk was particularly evident in India, during the consultation of price discrimination mechanisms, organised by TRAI, the national telecom regulator. Notably, Facebook, which has been one of the most vocal stakeholders of the Indian consultation, lobbied for ZR exploiting its own zero-rated services in order to send notifications to its users, encouraging them to send prefilled emails labelled "I Support Free Basics [*i.e.* Facebook own ZR programme] in India"[52] to TRAI. Moreover, application-sponsoring and application-ZR practices may be considered as a differential treatment of Internet traffic, because specific traffic is subsidised to users while the rest is billed. Such differentiation is not necessary

areas is limited. Second, individuals' capacity to connect may be severely limited due to the population's illiteracy, which may foster incomprehension or even fear of technology. Lastly, populations' poverty is a significant obstacle when the cost of Internet access represents a substantial portion of the average monthly income. *See* International Telecommunication Union (ITU), "ICT Facts and Figures", 2015. Available at: http://bit.ly/1FOoa6p; *See* A4AI, "The 2015-16 Affordability Report", 2016, available at: http://bit.ly/2epYu5r.

[50] Carrillo, Arturo J., "Having Your Cake and Eating it Too? Zero-Rating, Net Neutrality and International Law", on *Stanford Technology Law Review*, Vol. 19, Nº 3, October 2016. Available at: http://stanford.io/2eXaHC1

[51] *See* Mirani, Leo, "Millions of Facebook users have no idea they're using the internet", *Quartz*, February 9, 2015. Available at: http://bit.ly/1DbSWnK

[52] *See* Telecom Regulatory Authority of India (TRAI), TRAI Letter to Ms. Ankhi Das, Facebook Director of Public Policy, India, South & Central Asia, January 18, 2016. Available at: http://bit.ly/1WrStGc

to the smooth functioning of the application – which is usually considered as reasonable discrimination – but may well be considered a permanent discrimination exclusively motivated by commercial reasons, in light of the fact that its sole purpose is to drive users' choice towards the sponsored applications. Lastly, it is essential to consider that only application having a commercial value are likely to be zero-rated by operators or sponsored by financially-capable providers, thus *de facto* excluding access to non-commercial content and services, such as political and educational material, from the spectrum of content that could be accessed for free.

Lastly, ZR platforms and application-agnostic data sponsoring deserve particular attention, for they present different rationales and determine different implications when compared with the abovementioned models. The best-known ZR platform is the controversial Internet.org initiative, launched by Facebook and some other Internet companies in 2013. The stated goal of the initiative is "bringing internet access and the benefits of connectivity to the two-thirds of the world that doesn't have them."[53] However, critics argue that Internet.org create a two-tiered Internet for users, ascribing to Facebook the same form of gatekeeping power that operators would like to gain through the implementation of blocking and measures paid-prioritisation schemes. Such gatekeeping power would ascribe to operators or Facebook, in the Ineternet.org case, the power to define what services may be accessed for free and what services require additional fees, in order to orientate consumer choice and acquire control over the Internet market. It seems important to note that, despite Internet.org stated purpose being "bringing internet access" to the unconnected, the platform has been conceived to provide access only to a very limited selection of applications. It is indeed only in reaction to pressure from NN advocates and facing the decision of several content providers – amongst which the Times Group[54] – to leave the platform that Facebook upgraded it, creating the FreeBasics project, which allows to zero-rate "any low-bandwidth online service that meets its technical guidelines."[55] In spite of this modification being hailed as Facebook intention to create "an open platform and anyone who meets these guidelines will be able to participate"[56]

[53] Internet.org, http://bit.ly/23UC7rP

[54] *See* Times Group, "Times Group commits to withdraw from internet.org; appeals to fellow publishers to follow suit and support net neutrality", *Times Internet Corporate Blog*, April 15, 2015. Available at: http://bit.ly/1DiNU8C

55 *See* Ribeiro, John, "Facebook's Internet.org opens platform to other online services", *Computerworld*, May 4, 2015. Available at: http://bit.ly/2eXwrOx

[56] *See* Facebook, "Announcing the Internet.org Platform", *Facebook Newsroom*, May

it must be noted that the original Internet.org persists unchanged – *i.e.* only including a reduced number of services – in a considerable percentage of countries in which such platform is available.[57]

It should be noted that, in countries where public policies fail to promote connectivity, ZR platforms such as Free Basics may be considered as a necessary and proportionate exception to NN principle in order to allow individuals to exercise their fundamental right to freedom of expression. However, such ZR platforms should be considered as a sustainable solution to foster connectivity but rather as temporary solutions and may be accepted only as long as they are open to any applicants respecting the technical guidelines, necessary to be included. As stressed by Rossini & Moore[58] the use of such suboptimal solutions may dissuade governments from working towards optimal solutions aimed at empowering unconnected community through the provision full Internet connectivity. Notably, authoritarian regimes may find it much more convenient to allow the provision of preapproved and easy-to-control ZR services, rather than full Internet connectivity.[59] This latter point is of particular relevance in light of the fact that, as mentioned above, Internet connectivity allows individuals not only to free express themselves but also to be producers of innovation, rather than mere consumers of online services. Hence, the ultimate goal of sustainable Internet policies should be the creation of prosumers able of freely expressing themselves, innovating and competing with established payers, rather than increasing consumers of already-dominant services.

The last ZR type is application-agnostic data sponsoring. In this model, a sponsor entity subsidise a limited amount of data that the operator will made available to users. Hence, differently from the service sponsoring model, this latter model does not imply discriminatory treatment with regard to content, application and services, due to the fact that users are free to utilise the sponsored data allowance for whatever purpose they wish. Hence, application-agnostic data sponsoring is fully compatible with NN. Examples of such model include Mozilla's Equal Rating project, the mCent application or the Free Basic Internet offering, proposed by Indian operator Aircel. The Mozilla initiative has been experimented in various African countries. Based on a partnership with telecom operator Orange, the project

4, 2015. Available at: http://bit.ly/1Pihrm7

[57] *See e.g.* the Colombian version http://bit.ly/1y9z70s and the Kenyan version of the project http://bit.ly/1wBONXu

[58] Rossini and Moore, "Exploring Zero-Rating Challenges: Views From Five Countries", A Public Knowledge Working Paper, 2015.

[59] Belli, Luca, *supra* note 41.

aims at offering a $40 smartphone, running the Firefox operating system and including unlimited text, conversation and 500 MB data allowance per month for six months.[60] On the other hand, the mCent application is bases on an innovative business model rewarding with data allowance users' participation to a variety of activities such as "application downloading and using apps, taking surveys, watching videos, signing up for a service, and/or participating in contests."[61] Lastly, operator Aircel has decided to offer 500MB data allowance to all new prepaid activations for a 90-day period, starting from the date of activation.[62] Although such plans may be categorised as ZR offerings, it seems evident that their goal is not to favour or disfavour specific content, applications or services, and for this reason application-agnostic data sponsoring seems to be fully compatible with NN.

The Marco Civil: a Brazilian Approach to Net Neutrality and Zero Rating

The MCI is the human-right-based framework, defining the legal basis of the Internet regulation in Brazil. In spite of its status of ordinary law, the MCI has been hailed as the Brazilian "Internet Constitution," due to the definition of funding elements of the Internet discipline in Brazil as well as its marked intention to protect fundamental rights and freedoms online. The MCI is considered an international hallmark of participatory democracy due to the online consultation process that led to its elaboration. The open and collaborative process leading to the elaboration of the MCI was initiated and jointly orchestrated the Center for Technology and Society at Fundação Getulio Vargas, together with the Brazilian Mistry of Justice.[63] The MCI was stimulated by former President Luiz Inácio Lula da Silva's commitment to develop a "Civil Rights framework for the Internet"[64] and was strongly backed by President Dilma Rousseff. Notably, reacting to the mass surveillance revelations by former NSA contractor and whistle-blower Edward Snowden, Rousseff urged the establishment of

[60] Dixon-Thayer, Denelle, "Mozilla View on Zero-Rating", *The Mozilla Blog*, May 5, 2015. Available at: https://mzl.la/1RbY81R

[61] *See* mCent, http://bit.ly/2glOcZ1

[62] The offering called Free Basic Internet should not be confused with Facebook initiative Free Basics.

[63] *See* Brazilian Internet Steering Committee (CGI.br), "Um pouco sobre o Marco Civil da Internet", April 20, 2014. Available at: http://bit.ly/2fQpL3E

[64] *See* Mário Coelho, "Lula quer regular a Internet", *Congresso em Foco*, November 24, 2009. Available at: http://bit.ly/2eVJ2l3

strong guarantees for human rights online at both the international and national level. Therefore, the MCI was the result of a blend of participatory democracy and strong political will to protect "freedom of expression, privacy of the individual and respect for human rights" while guaranteeing the "neutrality of the network, guided only by technical and ethical criteria, rendering it inadmissible to restrict it for political, commercial, religious or any other purposes."[65] In this perspective, the MCI rapporteur in the Chamber of Deputies Alessandro Molon argued that NN is a fundamental right and a cornerstone of democracy, enabling individuals to have access to a plurality of sources of information.[66] Hence, the enshrinement of NN into Brazilian legislation signal the understanding of the legislator that non-discriminatory treatment of Internet traffic has become an essential precondition for achieving properly functioning democracies, fuelled by plurality of information, ideas, opinions and innovation.

It is important to note that, at the Brazilian level, NN is advocated for since 2009, when the Brazilian Internet Steering Committee[67] – better known under its Brazilian acronym CGI.br – included NN in its Decalogue of fundamental Internet governance principles. The Decalogue's definition of NN, according to which "[f]iltering or traffic privileges must meet ethical and technical criteria only, excluding any political, commercial, religious and cultural factors or any other form of discrimination or preferential treatment,"[68] was repeatedly reformulated during the MCI elaboration process,[69] until its final version was approved in April 2014. Eventually, NN was enshrined in the MCI, imposing the operator's "duty to process, on an isonomic basis, any data packages, regardless of content, origin and destination, service, terminal or application."[70] Importantly, the MCI explicitly included NN amongst the principles defining "the discipline of the Internet

[65] *See* Statement by H. E. Dilma Rousseff, President of the Federative Republic of Brazil, at the 68th Session of the United Nations General Assembly, September 24, 2013.

[66] *See* "Molon Defende Neutralidade Da Rede e Critica Qualidade Da Internet Brasileira Em Conferência Internacional Da FGV-Rio", Molon Deputado Federal web page, June 11, 2015. Available at: http://bit.ly/2fQtApt

[67] The Brazilian Internet Steering Committee is a multistakeholder body aimed at "coordinating and integrating all Internet service initiatives in Brazil, as well as promoting technical quality, innovation and the dissemination of the services available." *See* http://bit.ly/2fQzlhJ

[68] *See* Brazilian Internet Steering Committee (CGI), "Principles for the Internet governance and use of the Internet". Available at: http://bit.ly/2fL3jlO

[69] *See* Ramos, Pedro Henrique Soares, "Arquitetura da Rede e Regulação: a neutralidade da rede no Brasil", Fundação Getulio Vargas, Escola de Direito de São Paulo, São Paulo, 2015. Available at: http://bit.ly/2fPlD1c

[70] *See* Marco Civil, art 9.

use in Brazil"[71], alongside fundamental rights such as privacy and freedom of expression, stressing the instrumental function of such principles "to promote (i) the right of all to access the internet; (ii) the access to information, to knowledge and participation in the cultural life and in the handling of public affairs; (iii) the innovation and the stimulus to the broad diffusion of new technologies and models of use and access."[72] Hence, the MCI ascribes to NN a primary position, including it amongst constitutional principles such as the protection of human rights and the promotion of innovation, in order to signify the crucial role of NN to foster a sustainable Internet environment.

The Brazilian legislator has considered NN as necessary to avoid the kind of control that can potentially limit Internet users' ability to receive and impart information and ideas, including their capacity to share innovation. In this sense, the non-discriminatory treatment mandated by the NN principle is supposed to allow users to be active developers of innovation and producers of content besides being mere consumers, thus unleashing a virtuous circle of innovation[73] and creating a level playing field for entrepreneurs and businesses to launch innovative products and services. For these reasons, the MCI choses to firmly protect NN, allowing operators to discriminatorily manage Internet traffic only as long as such management is "essential to the adequate provision of services and applications [or to the] prioritisation of emergency services."[74] Moreover, while the MCI promotes "freedom of business models"[75] on the Internet, it carefully specifies that such freedom cannot overcome NN, stating that commercial offering cannot "conflict with the other principles set out in this Law." As such, the plain reading of art. 9 MCI suggests that practices grounded on a differential treatment, such as ZR, cannot be allowed. However, due to the fact that such provision was supposed to be specified via Presidential decree, operators have started offering ZR plans in the Brazilian market, arguing that ZR does not contradict NN and waiting for the clarifications to be provided by the MCI regulation.

Between the end of 2014 and early 2016, the Brazilian Ministry of Justice organised a biphasic consultation aimed at developing the decree through a participatory process. As in other counties, Brazilian stakeholders have

[71] *See* Marco Civil, art 2.

[72] *Ibid*, art. 4.

[73] Williamson, Brian, Black, David and Punton, Thomas, "The open internet – A platform for growth", a report for the BBC, Blinkbox, Channel 4, Skype and Yahoo!, Plum Consulting, October 2011. Available at: http://bit.ly/2fVt61F

[74] *Ibid*, art. 9.

[75] *Ibid* art. 3.VIII.

responded to the consultation with quite polarised replies regarding ZR, displaying a telling division of stakeholder views. On the one hand, operators and network-equipment producers strongly supported the adoption of ZR models, while literally all other respondents to the consultation argued that ZR should be considered as incompatible with NN provisions.[76] Notably, ZR supporters argued that ZR would provide consumers with free (*i.e.* subsidised) access to selected services, applications or content, allowing the most price-sensitive consumers to access services that they otherwise would forego. Conversely, ZR detractors argued that, in the long-term, the potential benefits of ZR come at a considerable cost with regard to the development of the Brazilian digital ecosystem as well as the Brazilian citizens' freedom of information and opinion. Although ZR may be considered as a legitimate business model, it is important to recall that art. 2 MCI calls for strong protection human rights, plurality and openness and art. 3 explicitly subjects "freedom of business models" to the respect of "the other principles set out in this Law," such as NN. In this perspective, from the Brazilian consultation, it emerged that ZR aims at driving users towards the less expensive services rather than the more innovative or more useful ones, thus creating walled-gardens locking low-income users into subsidised services and information bubbles, predefined by the operators.

The consultation allowed the elaboration of Decree 8771/2016[77] that provides further guidance as regards the illegality of ZR within the Brazilian juridical system. Notably, art. 9 of the MCI decree prohibits any practice that "compromise the public and unrestricted character of Internet access and the funding elements and principles as well as the goals of internet usage in the country" or "favours applications offered by those responsible for transmitting, switching or routing or by companies in the same economic group." However, it is important to stress that, to date, Brazilian operators have refused the incompatibility of ZR and NN, including ZR services in a wide range of data plans. Furthermore, it is important to reiterate that, in Brazil, only four well-established applications are zero-rated, *i.e*. Facebook, Twitter, WhatsApp and Deezer. Hence, the Brazilian ZR panorama exemplifies tellingly the critiques according to which ZR plans likely consolidate well-established players, rather than promoting competition, the emergence of new services and media

[76] Brito Cruz, Francisco Carvalho et al., "What is at stake in the regulation of the Marco Civil?", Final report on the Public Debate Sponsored by the Ministry of Justice on the Regulation of Law 12.965/2014, InternetLab, 2015. Available at: http://bit.ly/1QZE8kP.

[77] *See* Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, Decreto Nº 8.771, 11 de Maio de 2016. Available at: http://bit.ly/1TRNpKo

pluralism. Indeed, as shown by the Brazilian example, only popular services are sufficiently attractive and have the necessary bargaining power to strike zero-rating deals. Moreover, such scenario corroborates the critiques according to which ZR has the potential to transform active Internet users into passive application consumers, thus prompting a shift from a general-purpose and generative Internet to predefined-purpose and stagnant Minitel-like[78] network.[79]

Although ZR may be seen as an efficient way of delivering sponsored services to users, it seems unquestionable that ZR is based on positive discrimination of such sponsored services, with the aim of creating users of specific services rather than Internet prosumers. Such evolution seems to be patently conflicting with art. 3 MCI, which establishes "the preservation and guarantee of network neutrality" as well as the "preservation of the participative nature of the network" as fundamental principles of the discipline of the Internet in Brazil. Moreover, by promoting the use of only four applications ZR, plans do not seem compatible with the respect and promotion of "free enterprising, free competition, […] plurality, and diversity" which is explicitly demanded by art 2 MCI. Therefore, jurisprudence would be welcome in order to clarify the compatibility of the existing ZR practice with the aforementioned MCI provisions as well as with art. 10, Decree 8771/2016, according to which "commercial offerings and billing models for internet access must preserve a single internet that is open, plural and diverse in nature and understood as a means for the promotion of human, economic, social and cultural development as well as contributing to the building of an inclusive and non-discriminatory society."

Conclusion

The fundamental rationale for NN is to maintain the Internet as an open and decentralised system, whose evolution can be directly fashioned by the Internet users that sit at the end-points. As I have noted, several ZR offerings have the potential to infringe the very rationale of NN while they make sense only when combined with data caps sufficiently low to make it interesting for an individual to enjoy the free data-allowance of a sponsored services. This means that in the absence of data caps or when data caps are

[78] The Minitel network was a closed system, particularly popular in France during the 1990s, in which only the operator could decide the services to be made available to users, while the French governmental agency in charge of telecommunications had the right to unilaterally approve or disapprove any service.

[79] Belli, Luca, *supra* note 37.

sufficiently abundant, consumers are not inclined to consider ZR offerings.[80] Hence, ZR practices may foster artificial scarcity, stimulating operators to keep data-allowance low in order to entice consumers with sponsored services. As I have argued, although some ZR models may be used as temporary solutions to allow unconnected individuals to communicate, it is important to note that more sustainable solutions exist. Particularly, public policies should aim at fostering full connectivity, allowing individuals to have the power of creating and sharing innovation, being active prosumers rather than passive consumers. In this sense, policy-makers should assess the costs and benefits of ZR but also consider alternative solutions such as community networks.[81] Community networks are already diffused in a variety of developed and developing countries and, differently from ZR schemes, they are based on individual empowerment through the creation of infrastructure from the edges, at the user level. The common characteristic of community networks is the use of networking technologies by, and for, a local community: they are deployed by a local community of individuals and organisations and subsequently managed by such community, pooling resources and coordinating efforts.

Such an approach is not merely theoretical but has already demonstrated the capacity to produce concrete and distributed benefits. Notable examples include the Guifi.net[82] network, with its over 33.000 thousand participants spread across the entire Catalonia region, in Spain, as well as the community networks created by the Argentinian association AlterMundi,[83] and the Indian Digital Empowerment Foundation.[84] The main goal of such network is to

[80] Arnold, R. *et al*., "The Value of Network Neutrality to European Consumers", a study commissioned by Body of European Regulators for Electronic Communications (BEREC), April, 2015. Available at: http://bit.ly/2f7apXc

[81] For an overview on community networking, *see* Belli (ed.), "Community Connectivity: Building the Internet from Scratch". Annual Report on the UN IGF Dynamic Coalition on Community Connectivity,, FGV Editor, 2016; Baig, R. et al., "Guifi.net, a crowdsourced network infrastructure held in common, Computer Networks", Catalunya, Barcelona, Spain Computer Networks, 2015, available at: http://bit.ly/1l5WVgr; *See also* Giovanella, Federica and Caso, Roberto, "Reti di Libertà. Wireless Community Networks: un'analisi interdisciplinare" on *Quaderni della Facoltà di Giurisprudenza*, Università degli Studi di Trento, January 2015; *See* De Filippi, Primavera and Tréguer, Félix "Wireless Community Networks: Towards a Public Policy for the Network Commons?" on *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*, Part III, Springer International Publishing, November 2015.

[82] *See* http://bit.ly/2fpvl9r

[83] *See* http://bit.ly/2fPQIXk

[84] *See* http://bit.ly/2eVQpZZ

empower communities through technology, allowing participants to both develop and manage the infrastructure as a common resource. Importantly, community networks allow offering and receiving any type of service on a non-discriminatory basis and with no inspection or modification of data flows within the network beyond what is strictly necessary for its operation. As such, community networks are not only compatible with the NN rationale but they also promote full user empowerment, particularly targeting unconnected populations. Indeed community networks are based on the use of easy-to-implement network models, which can be readily reproduced and exploited even by individuals lacking technical knowledge. Such network models are grounded on the use of "reference hardware based on readily available home equipment; an easy-to-build design for dual-band directional antennas; software (firmware) responsible for auto-configuration of network nodes and dynamic routing; a web interface for basic management and alignment of antennas; and a set of tools for network monitoring and mapping."[85]

As noted in Section II and III ZR practices may not be compatible with NN and may substantially limit the way in which individual may use and take profit from the Internet. On the contrary, community networks seem to offer a very concrete answer to the quest for digital inclusion, having not only the potential to create infrastructure from the edges but also to stimulate digital literacy, community empowerment and local content-and-service creation. In an era in which governments are frequently criticised for lacking political vision and prioritising the interests of well-established private actors, the promotion of sustainable connectivity through user-empowering approaches such as community networking would be a smart choice to restore much needed trust in policy-makers, while protecting a non-discriminatory and user-centric Internet.

Other References

Federal Communications Commission, *Preserving the Open Internet* , GN Docket Nº 09-191, WC Docket Nº 07-52, December 2010. Available at: http://bit.ly/1C35jEq

Schumann, Robert and Kende, Michael, "Lifting Barriers to Internet Development in Africa: suggestions for improving connectivity", Report for the Internet Society (ISOC), May 8, 2013. Available at: http://bit.ly/1MRw17S

[85] Echániz, Nicolás, "Community networks: internet from the first mile", on *FRIDA: 10 years contributing to development in Latin America and the Caribbean*, FRIDA Program, LACNIC, October 2015. Available at: http://bit.ly/1Nt5aKr

Chapter Four

Having Your Cake and Eating It Too? Zero-rating, Net Neutrality and International Law

Arturo J. Carrillo[1]

Abstract

This Article analyzes the international law response to the zero-rating conundrum. National debates rage across the globe on whether to permit zero-rating, which violates net neutrality, as a means of increasing connectivity, especially in the developing world. As a rule, these highly contentious discussions lack rigor, objectivity, and impact. They are characterized by a clash of dogmas: the sanctity of net neutrality principles, on the one hand, versus the imperative to close the digital divide or respect free markets, on the other. This Article seeks to bridge that dichotomy by invoking the applicable international law framework to analyze zero-rating as a limitation on net neutrality understood as a norm of human rights, which net neutrality demonstrably is. When viewed in this light, the zero-rating conundrum becomes a more tractable conflict of rights—the right to impart and receive information freely vs. the right to access the Internet—that can be constructively analyzed using the exceptions regime that human rights law provides precisely to resolve such conflicts. Under this framework, which legally binds almost 80% of the countries in the world, proposed

[1] Clinical Professor of Law; Director, International Human Rights Clinic; Co-director, Global Internet Freedom and Human Rights Project, George Washington University Law School. I am grateful to Luca Belli, Anupam Chander, Gene Kimmelman, Kevin Martin, Dawn Nunziato, Daniel O'Maley, Courtney Radsch and Carolina Rossini, for their comments. I would also like to thank the following GW Law School students for their research assistance: Ana González, Matthew Halldorson, Carrie James, Jannat Majeed, Nora Mbagathi, and Darke Zheng. This article was originally published in Stanford Technology Law Review in October, 2016 (19 STAN.TECH. L.REV. 364 (2016)).

exceptions to net neutrality like zero-rating must be examined under specific country conditions. These exceptions are assessed using a balancing test of factors, including necessity and proportionality, to determine whether, on the whole, freedom of expression is advanced or not in that particular context. This approach has the additional advantage of being able to accommodate inputs from other fields, like economics and technology policy. In short, understanding how human rights legal norms apply to net neutrality and zero-rating in practice should lead to better reasoned discourse on both sides of the debate, and thus to better outcomes.

Introduction

In the aftermath of the ferocious net neutrality debates in the United States, which culminated in the Federal Communications Commission's 2015 Open Internet Order,[2] attention shifted to similar policy discussions in Europe and elsewhere.[3] One struggle to protect net neutrality with far-reaching consequences is taking place in India, where government regulators in 2015 confronted intense social backlash over so-called "zero-rating" plans offered by local mobile operators.[4] The spark was an Indian telecom joining forces with Facebook in early 2015 to roll out Internet.org, the latter's online platform (now called "Free Basics"), with the stated objective of advancing connectivity in the developing world. Among other things, Internet.org offered limited access to a bundle of select online content and services free of charge.[5] Other Internet companies both large and small now offer free access

[2] Federal Communications Commission, Federal Register 19738, "Protecting and Promoting the Open Internet", Vol. 80, N° 70, , April 13, 2015, to be codified at 47 C.F.R. pts. 1, 8, 20. Available at: http://bit.ly/2frYDqL [http://bit.ly/2flZNkz] [hereinafter, 2015 Open Internet Order].

[3] *See, e.g.*, O'Reilly, Quinton, "The EU Has Plans for an Open Internet, but What Does it Mean?", *The Journal .Ie*, Dublin, July 11, 2015. Available at: http://bit.ly/2fKw0G6 [https://perma.cc/NTY6-SP63].

[4] *See* Arakali, Harichandan, "Amazon, Facebook Square Off Over Net Neutrality In India", *International Business Times*, April 17, 2015. Available at: Int'l Business Times, (Apr. 17, 2015, 12:57 PM), http://bit.ly/2eQejpl [https://perma.cc/HHH4-4H5S].

[5] Russell, Jon, "Facebook Takes Internet.org And Its Free Mobil Data Services To India", *Tech Crunch*, February 9, 2015. Available at: http://tcrn.ch/1z4fySt [https://perma.cc/G7Y8-RXER]; *see also* Mariella Moon, Mariella, "Free Basics by Facebook' Replaces Internet org Website and App", *Engadget*, September 24, 2015.Available at: http://engt.co/2fknTS9 [https://perma.cc/9UEY-FHR5](stating that "Free Basics" offers a menu of services and applications to users in Asia, Africa and Latin America to choose from.)

to the mobile Internet in scores of developing countries around the globe.[6]

In recent years, a number of governments including the United States have legislated strong net neutrality protections to ensure that freedom of speech and expression online are not warped by market forces, or otherwise unfairly curtailed by network providers.[7] A potential threat to net neutrality is zero-rating, which refers to "the practice by service providers of offering their customers a specific set of services or applications that are free to use without a data plan, or that do not count against existing data caps."[8] Numerous countries are in the process of developing regulatory frameworks that will determine if and when restrictions on net neutrality, in particular zero-rating, will be permitted.[9] But what could be wrong with offering limited but free access to the Internet to sectors of a population that would most likely not enjoy such connectivity or services otherwise?

Quite a bit, it turns out. Primarily, this is because zero-rating acts as a constraint on net neutrality, the principle that network providers—including mobile operators—must treat all data and content online equally[10] to guarantee the free flow of information and unfettered access to it.[11] From this perspective,

---

[6] *See infra* Part I.A.

[7] *See infra* notes 232 - 248 and accompanying text.

[8] *See e.g.* "Open Letter to Mark Zuckerberg Regarding Inernet.org, Net Neutrality, Privacy, and Security", Facebook, May 18, 2015. Available at: http://bit.ly/1L23He3 [https://perma.cc/DK58-36YX] [hereinafter *Open Letter*]; *see also* Baker, Mitchell, "Zero Rating and the Open Internet", *Lizard Wrangling Blog*, May 6, 2015. Available at: http://bit.ly/1lLOGyz [https://perma.cc/7NUP-3CU7].

[9] *See, e.g.*, "Net Neutrality: DoT Panel Against Facebook's Internet.org, Favours Airtel Zero", *India Today Tech*, July 6, 2015. Available at: http://bit.ly/1RfbXPs [https://perma.cc/E4S3-3MA9]; *see also* Marini-Balestra, Federico and Tremolada, Ricardo, "The EU Debate on Net Neutrality: What about Zero Rating?", Academia, 2015. Available at: http://bit.ly/2fLSXXV [https://perma.cc/CYH5-EP39]; Patricia Rey, "Net Neutrality in Mexico: Still a Long Way to Go", *BNAméricas*, February 27, 2015.. Available at: http://bit.ly/2fl8XLG [https://perma.cc/GQK8-QWKR].

[10] U.N. Special Rapporteur on Freedom of Opinion & Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression & ACHPR Special Rapporteur on Freedom of Expression & Access to Information, "*Joint Declaration on Freedom of Expression on the Internet*", OSCE, June 1, 2011. Available at: http://bit.ly/1CUwVap [https://perma.cc/JPT6-F642] [hereinafter Joint Declaration]; *see* 2015 Open Internet Order, *supra* note 1, at 1.

[11] Open Letter, *supra* note 7 ("Net neutrality supports freedom of expression and equality of opportunity by enabling people to seek, receive and impart information, and to interact as equals. It requires that the internet be maintained as an open platform on which network providers treat all content, applications and services equally, without discrimination. An important aspect of net neutrality states that everyone should be able to innovate without permission from anyone or any entity.").

'[z]ero rating' is [a] discriminatory technique where telecom operators allow customers access to select online content or services at no additional cost through a prior arrangement with content providers. The selected sites are rated at zero cost to the customers, violating the essence of net neutrality, which requires non-discrimination between different content and applications.[12]

Simply put, given that zero-rating violates net neutrality by definition, the controversy is over whether zero-rating should ever be allowed, and if so, when.[13] This is what I call the zero-rating conundrum. To date the sharpest clash involving this conundrum has been in India, where public debates since 2015 have garnered significant international attention.[14] The roll out of Internet.org in February of that year sparked waves of protest from Indian civil society and digital rights activists around the world.[15] They worried that Facebook, a for-profit multi-national corporation, would—through its Internet.org platform—become "gatekeeper" to the Internet for millions of mobile phone users in the developing world, with nefarious consequences for local innovation, competition, and social development.[16]

As the backlash to Internet.org began to unfold in India, Facebook CEO Mark Zuckerberg responded publicly to critics in both an opinion piece published by an Indian online financial paper and through a post on his Facebook page. He stated:

> [S]ome people have criticized the concept of zero-rating that allows Internet.org to deliver free basic internet services, saying that offering some services for free goes against the spirit of net neutrality. I strongly disagree with this. We fully support net neutrality. We want to keep the internet open. Net neutrality ensures network operators don't discriminate by limiting access to services you want to use.

[12] Vipul Kiran, Singh, "Permit Zero-Rating Schemes for a Limited Period", *The Financial Express*, July 9, 2015. Available at: http://bit.ly/2eOOpz2 [https://perma.cc/4F7T-F87P].

[13] The policy debate surrounding net neutrality in any given country will obviously be broader than just whether or not to allow zero-rating. For a detailed discussion of most (if not all) relevant considerations in such a debate, see Van Schewick, Barbara, "Network Neutrality and Quality of Service: What a Nondiscrimination Rule Should Look Like" on *Stanford Law Review*, Vol. 67, N° 1,, January 2015. Available at: http://stanford.io/2f4e6Nb. However, I will be focusing primarily on the key issue of zero-rating for the reasons explained in this Introduction.

[14] *See e.g.* Morozov, Evgeny, "Facebook Isn't a Charity. The Poor Will Pay by Surrendering Their Data", *The Guardian*, April 25, 2015. Available at: http://bit.ly/1DDtjtx [https://perma.cc/CA98-MVNE].

[15] *Id.*

[16] See *infra* notes 85-87 accompanying text.

> It's an essential part of the open internet, and we are fully committed to it. But net neutrality is not in conflict with working to get more people connected. *These two principles—universal connectivity and net neutrality—can and must coexist*.[17]

Commentators were quick to reply that Mr. Zuckerberg "can't have it both ways on net neutrality."[18] A journalist for Wired affirmed bluntly that if the question is "whether the Internet.org model runs counter to the core tenets of net neutrality, [the] answer [is] obvious." The two are irreconcilable. On this view, the question Mr. Zuckerberg and the proponents of zero-rating should be answering instead is "whether the same rules should apply in places where people don't have access to the Internet at all, let alone equal access."[19] The real question is whether it is acceptable "to suspend some of the net neutrality absolutism the tech community has rallied behind in the US if it serves a greater good in the world's poorest countries..."[20] This, too, is an essential dimension of the zero-rating conundrum.

By insisting that "universal connectivity" and net neutrality "can and must co-exist," Mr. Zuckerberg and Facebook are accused of wanting "to have their cake and eat it too." This adage is meant to convey that the ostensible goal—full respect for net neutrality—and the desired outcome—a global connectivity platform based on zero-rating—are inherently incompatible. If one subscribes to the "net neutrality absolutism" that characterizes certain sectors of the net neutrality debates in the United States, then that conclusion is inescapable. But is net neutrality as a principle really absolute? The issues reflected in the foregoing exchange have far-reaching consequences beyond the borders of any one country or region.

Other Internet companies, telecoms, and governments all over the world have kept a close eye on how the regulatory battles over net neutrality have unfolded in India, Europe and elsewhere.[21] Ultimately, India's regulator chose

---

[17] Zuckerberg, Mark, "Internet.org Does Not Violate Net Neutrality", *Live Mint*, April 16, 2015. http://www.livemint.com/Opinion/vewA4Z6qQ82IuN8yQKlqxK/Mark-Zuckerberg-on-Net-neutrality.html Available at: http://bit.ly/1EQmXeK [https://perma.cc/VZ9Q-ZSME];

18 Lapowsky, Issie "Mark Zuckerberg Can't Have it Both Ways on Net Neutrality", *Wired*, April 17, 2015. Available at: http://bit.ly/2fn3dsP[https://perma.cc/4ML9-FQQE].

[19] *Id*.

[20] *Id*.

[21] *See, e.g.*, Telecom Regulatory Authority of India [TRAI], *Consultation Paper on Differential Pricing for Data Services*, at 9, New Delhi, December 9, 2015. Available at: http://bit.ly/1JrDlkw [https://perma.cc/6ZLL-JWHT] [hereinafter "TRAI Consultation Paper"]; McCarthy, Kieren "Council of Europe Gets Tough on Net Neutrality: No Blocking,

to ban differential pricing, including zero-rating by telecoms, in February 2016.[22] In the United States, the FCC adopted a set of strong net neutrality protections that nonetheless leave the door open to zero-rated "sponsored data" plans, provided they do not unfairly or unreasonably disadvantage consumer choice and expression.[23] What that means is anybody's guess.

No matter how you look at it, there is a great deal at stake in the zero-rating debate. But *how* you look at it is, in fact, critical to addressing the inherent tension between net neutrality and zero-rating in a coherent manner. This Article approaches the issue by bringing a "new" perspective to the debate: international human rights law. This corpus of norms is itself not new, of course. However, in most countries, the polemics surrounding zero-rating and net neutrality regulation have been largely devoid of reference to human rights rules. Policy debates have focused instead on the social, economic, and technical dimensions of zero-rating, as reflected in the still modest but growing body of research and commentary on the subject.[24] But even as

Slowing Down, Degrading or Discriminating of Internet Traffic", *The Register,* Jan. 13, 2016. Available at: http://bit.ly/2g1qena [https://perma.cc/3MFZ-7M46] [hereinafter *Council of Europe gets tough on net neutrality*]. Brazil is an example of another front line in this battle. *See* Brito Cruz, Francisco and Coelho Marchesan, Jonas "Net Neutrality in Brazil: The Debate Continues", *InternetLab Blog*, February 4, 2016. Available at: http://bit.ly/2g1pfTU [https://perma.cc/B497-M4YU].

[22] *See* Gowen, Annie, "India Bans Facebook's 'Free' Internet for the Poor", *Washington Post*, Febuary 8, 2016. Available at: http://wapo.st/1W6GX28 [https://perma.cc/2CBQ-V8PB]; Hempl, Jesse, "India Bans Facebook's Basics App to Support Net Neutrality", *Wired*, February 8, 2016. Available at: http://bit.ly/1PKvhSj [https://perma.cc/9BMY-3PZA]. *See also* Part III.B. (discussing recent developments in India).

[23] See infra notes 232 - 249 and accompanying text.

[24] *See, e.g.*, 9th Internet Governance Forum—Istanbul, "Session Report: WS 208: Net Neutrality, Zero-Rating, and Development", September 3, 2014. Available at: http://bit.ly/2eWzltV [https://perma.cc/H6HM-5FL6]. Recent studies have begun to fill in the blanks on the lack of empirical data. *See, e.g.*, Center for Deliberative Democracy and Stanford Center on Democracy, Development, and the Rule of Law, "Increasing Internet Access to the Next Billion", 2015 [hereinafter Stanford Study]; *see also* Smith, Alex and Moskowitz, Ben, "Mobile for Development Impact. Approaches to Local Content Creation: Realizing the Smartphone Opportunity", GSMA and Mozilla Report, 2015, Available at: https://mzl.la/29P9WZZ [https://perma.cc/98KS-Y74D] [hereinafter "Mozilla Report"]; Thakur, Dhanarai, "The Impacts of Emerging Mobile Data Services In Developing Countries", Alliance For Affordable Internet, November 2015, Available at: http://bit.ly/2fUjJBn [https://perma.cc/EM6Q-3CHD]; Chair, Chenai, "Africa Supply Side Assessment of Zero Rating", Research ICT Africa, November 10, 2015, Available at: http://bit.ly/2fUkcmN [https://perma.cc/EM6Q-3CHD]; Ramos, Pedro Henrique Soares, "Towards a Developmental Framework for Net Neutrality: The Rise of Sponsored Data Plans in Developing Countries", TPRC Conference Paper, March 31, 2014. Available at: HYPERLINK "http://bit.ly/2eWxY3N" http://bit.ly/2eWxY3N [https://perma.cc/D7L6-HTA7]; Layton, Roslyn and Elaluf-Calderwood, Silvia

advocates on both sides of the debates intensify their research in search of better empirical data, their consideration of the *normative* framework of human rights law remains passing at best. This Article seeks to re-frame that perspective and, hopefully, expand it.

When net neutrality is analyzed as a human rights norm, which it demonstrably is, zero-rating issue takes on an entirely new dimension, one that is critical to understanding net neutrality's proper function in the real world. The zero-rating conundrum ceases to be cast as a divisive dichotomy of dogmas and transforms into something rather more tractable: a conflict of rights, of the type that is regularly confronted and resolved within the framework of international human rights law.[25] When viewed through the lens of human rights, "preserving [net] neutrality means preserving the power of *individuals* to make choices about how they use the Internet – what information to seek, receive, and impart, from which sources, and through which services."[26] Accordingly, the issue from a human rights perspective is this: *Can zero-rating ever be consistent with net neutrality principles, understood as the freedom enjoyed by all persons to seek, receive, and impart information in a nondiscriminatory manner?* Because even fundamental rights are not absolute, the answer to that question turns out to be *yes, sometimes, under certain circumstances*.

The remainder of this Article is dedicated to examining net neutrality as a human rights norm and the conditions under which that principle can be legitimately qualified by proposed restrictions such as zero-rating. It is divided into three Parts. Part I surveys the panorama of zero-rating around the world to establish a foundation for the legal and policy analyses to follow in Parts II and III, respectively. It first reviews the principal forms that zero-rating has taken and offers a working typology to facilitate the discussion of the relevant issues. Part I then surveys net neutrality and zero-rating over a

Monica, "Zero Rating: Do Hard Rules Protect or Harm Consumers and Competition? Evidence from Chile, Netherlands and Slovenia", August 15, 2015. Available at: http://bit.ly/2fub0VX [https://perma.cc/97H7-NJC5][hereinafter Layton & Elaluf-Calderwood]; Rossini, Carolina and Moore, Taylor, "Exploring Zero-Rating Challenges: Views from Five Countries", a Public Knowledge Working Paper, July 2015. Available at: http://bit.ly/2fRjbtB [https://perma.cc/MD29-Q4MQ][hereinafter Rossini Public Knowledge Report].

[25] See infra notes 250 - 334 and accompanying text.

[26] Center for Democracy & Technology, "The importance of Internet Neutrality to Protecting Human Rights Online", October 1, 2013. Available at: http://bit.ly/2gcxAEb [https://perma.cc/597U-9M44][hereinafter CDT Report 2013] (emphasis added). Network neutrality is also instrumental to preserving media diversity and pluralism on the Internet. This is discussed *infra* in Part II.B.I.

range of representative countries by region using both quantitative (statistical analysis) and qualitative (case study) methods. Part II outlines and analyzes the normative framework under international human rights law, focusing primarily on freedom of expression and non-discrimination principles. It explores the origins of the net neutrality principle to better understand its evolution as well as its relevance as a contemporary norm of human rights. Finally, Part III applies the human rights legal framework to zero-rating in light of the preceding data to demonstrate how policymakers, advocates, academics and others can utilize this "new perspective" to better evaluate the function and impact of zero-rating in context.

I. The Panorama: Zero-Rating Around The World

This second Part is divided into two sections. Section A scans the global panorama of zero-rating. It begins by providing an overview of the various forms that zero-rating takes and, where relevant, the principal sponsors of those initiatives. This allows for a useful differentiation between the various forms of purported zero-rated activities in effect or under study. This first section acts as a backdrop to the second, which takes a quantitative and qualitative look at the conditions under which net neutrality policies are implemented in different countries and regions. Section B first compiles key statistical indicators for a sample of countries selected by region. These indicators paint a picture of each country's economic, social and political development, especially in terms of fixed and mobile Internet access. Finally, Section B discusses the barriers to connectivity as they exist in these and other countries before outlining three case studies that exemplify the prevailing approaches to zero-rating.

I.A. The Global Panorama: Types and Sponsors of Zero-Rating

This section examines the principal configurations of zero-rating as it presently occurs. To recall, we have defined zero-rating as the practice of offering free access to certain online services or data for customers of particular mobile networks.[27] This is generally implemented by exempting traffic to certain sites

[27] Shears, Matthew, "No. 208 Net Neutrality, Zero-Rating & Development: What's the Data?", Internet Governance Forum, Available at: http://bit.ly/2fcXYch [https://perma.cc/BH29-SX9S]. It is important to note that this typology does not include public service zero-rating, such as some governments employ for purposes of emergency or other public services. An example is provided by the regional government of São Paolo state, in Brazil,

or through select applications from a subscriber's data caps.[28] Additionally, in some zero-rating arrangements, users can access the service even if they do not have a data plan.[29] These types of programs are popular in the mobile market because of the high cost of bandwidth compared to wired Internet, coupled with the low or non-existent availability of wired connections in many countries.[30] The goal of this section is to present a functional typology of private sector zero-rating practices that can facilitate the analyses to follow.

In this regard, there are at least four models of zero-rating practices: single-site or service zero-rating, sponsored data, compound zero-rating, and faux (or non-selective) zero-rating. These categories are not mutually exclusive: a given plan or platform may fit into more than one category depending on its characteristics. Each rubric is examined below.

I.A.I. Single-site or service zero-rating

In single-site or service zero-rating, one of the earliest adopted forms of zero-rating, a content provider contracts with one or more telecoms to provide users with free access to a version of its particular site or service free of charge. Generally, the zero-rated content can either be exempted from a customer's data plan "cap" or accessed wholly apart from any data plan. Unlike sponsored data plans (discussed below), single-site or single-service plans may not involve the content providers paying the telecom for the customer's zero-rated data usage, though they can. Such sites can be offered as a non-profit public interest service, e.g. Wikipedia Zero, or as a gateway to the greater Internet, where additional sites are accessible for a fee, e.g., Google Free Zone. Another example of a single-service application that telecoms zero-rate in a number

which subsidizes electronic government services through a publicly sponsored zero-rated platform. *See* Medeiros, Henrique, "Poupatempo No Celular: Acesso Patrocinado Custará R$ 20 Milhões ao ano para o Estado de SP", *Teletime*, September 28, 2015. Available at: http://bit.ly/2gdxKKM [https://perma.cc/9Z64-J39W]; *see also* Poupatempo, https://www.poupatempo.sp.gov.br/epoupatempo [https://perma.cc/Z47H-U4SZ] (the São Paolo regional government e-services website).

[28] *Id*.

[29] *Id.* Users generally are required to provide some personal data to subscribe to the zero-rated service or website, so in that sense they are not completely "free."

[30] Drossos, Antonios, "Forget Fast Lanes. The Real Threat for Net-Neutrality Is Zero-Rated Content", *Gigaom*, April 26, 2014. Available at: http://bit.ly/2fRpJIA [https://perma.cc/J6TW-ZLJB]; *see* Talbot, David, "Around the World, Net Neutrality Is Not a Reality", *MIT Technology Review*, January 20, 2014. Available at: http://bit.ly/2fChVK8 [https://perma.cc/6T85-PVWQ] (users do not have easy access to Wifi and no traditional connections at home).

of countries as a marketing strategy is WhatsApp, the world's most popular messaging app.[31] Telecom service providers benefit from these arrangements by catering to users who wish to utilize the free sites or services (and through payments from content providers where they exist) and incentivizing them to pay for data packages or complementary data usage.

The best-known examples of single-site zero-rating are Wikipedia Zero, Google Free Zone, and Facebook Zero, though there are important differences between them. Wikipedia Zero is a charitable initiative by the Wikimedia Foundation that partners with mobile operators to provide free access to Wikipedia to everyone.[32] Its stated goal is to "empower people around the world to develop and share freely licensed educational content."[33] It is currently available in 57 countries where it zero-rates access to its specially enabled websites through 75 different operators, reaching an estimated 600 million people.[34] Unique among zero-rating programs, Wikipedia Zero is publicly committed to providing transparency and accountability via ten operating principles.[35] These include: (1) carriers must zero-rate access to all parts of Wikipedia, and may not only zero-rate a portion of the site; (2) carriers must ensure that users do not mistakenly incur data charges and that users are prompted with a notice if they are about to leave a zero-rated page; (3) there will be no exchange of payment between Wikipedia Zero and the mobile carrier for providing the zero-rated services; and (4) there are no exclusive contracts—one carrier signing on with Wikipedia Zero does not prevent other carriers from doing the same.[36]

Google offers another single-site zero-rating type plan. Google Free Zone is an initiative that grants customers free access to Gmail, Google Search,

[31] WhatsApp 4, "How Popular Is WhatsApp Around the World?". Available at: http://bit.ly/2fcSwGr; Various telecoms zero-rate WhatsApp as a marketing strategy in Colombia, Ecuador, Mexico and Brazil. *See* Karisma Foundation, "¿Cómo se contrata en América Latina el acceso a Internet? ¿Qué tiene que ver con la neutralidad de la red?", June 2016. Available at: http://bit.ly/1slr7Ci; Rossini Public Knowledge Report, *supra* note 23, at 39-40.

[32] "Wikipedia Zero", The Wikimedia Foundation. Available at: http://bit.ly/1eWwNhp,[https://perma.cc/4HZX-MJBS]; "Mobile Partnerships", The Wikimedia Foundation. Available at: http://bit.ly/28Wok2H [https://perma.cc/NF65-C8HR] (last modified Mar. 30, 2016).

[33] "Wikipedia Zero Operating Principles", The Wikimedia Foundation. Available at: http://bit.ly/2fd3StT [https://perma.cc/D4XG-9CZQ] (last modified Apr. 3, 2015).

[34] "Wikipedia Zero", *supra* note 31. *See also* "Mobile Partnerships", *supra* note 31 (listing host countries and mobile partnerships).

[35] *See* "Wikipedia Zero Operating Principles", *supra* note 32.

[36] *Id*.

and Google+, the companies' social networking service.[37] Customers are able to freely access Gmail and Google+ from their mobile phone, but advanced functionality like downloading email attachments requires a data plan.[38] Additionally, customers can search Google through their phones without incurring data charges.[39] The Google Search functionality allows users to access any of the websites listed on the first page of Google Search results, free of charge.[40] If users want to access websites not included in Google's results, they are required to purchase a data plan.[41] Because Google Free Zone is effectively zero-rating access to some external content that is accessed through its search engine results, it can be viewed as having some characteristics of the compound zero-rating plans discussed below.[42]

Facebook Zero—not to be confused with Facebook's Internet.org initiative[43]—is a plan designed to allow users to access a limited version of Facebook on the Internet through their mobile device at any time, free of charge.[44] Smart phones and feature phones can access it on the web or through a popular app; on non-smartphones, for which it is optimized, Facebook Zero presents the user with a streamlined, text-only version of the social media site.[45] Launched in May 2010, Facebook partnered with more than 50 telecom operators to provide free access to Facebook Zero in 45 countries.[46] Facebook does not pay its telecom partners to provide the

[37] Press Trust of India, "Airtel Ties up with Google to Offer Free Search, Google+ and Gmail Services", *Gadgets360*, June 26, 2013. Available at: http://bit.ly/2gdvt2b [https://perma.cc/EW4A-TUQ5]. Google Free Zone is offered in the Philippines, Sri Lanka, India, Thailand, Nigeria and Kenya. *See* "Reduce Data Usage on Android, iOS and Desktop", *So Into Tech*, November 16, 2014. Available at: http://bit.ly/2fVKVh5 [https://perma.cc/FQ4X-ZYR3].

[38] *Id*.

[39] *Id*.

[40] *Id*.

[41] *Id*.

[42] Mott, Nathaniel, "Google Debuts Free Zone to Challenge Facebook for Dominance in Developing Countries", *Pando*, November 8, 2012. Available at: http://bit.ly/2fCsvRo [https://perma.cc/4GQ5-JP4E].

[43] *See* infra notes 81 - 88_and accompanying text.

[44] Wauters, Robin, "Facebook Launches Zero, A Text Only Mobile Site for Carriers", *Tech Crunch*, February 16, 2010. Available at: http://tcrn.ch/2fUAjkA [perma.cc/KJ27-MZ5Q].

[45] Mims, Christopher, "Facebook's Plan to Find Its Next Billion Users: Convince Them the Internet and Facebook Are the Same", *Quartz*, September 24, 2012. Available at: http://bit.ly/1q7We72 [https://perma.cc/Y4UF-RE23].

[46] *Id*.

service; nor does it use advertising.[47] Facebook Zero is made available to customers who have a data plan with one of the partnering telecom service providers.[48] If a user wants to access photos or follow external links, they receive a notification that they will be incurring data changes by doing so.[49] There is evidence that many eventually do so.[50] Additionally, people who access Facebook Zero are likely to invite their friends to do so as well, attracting new customers for the telecom provider.[51]

When compared with other forms of zero-rating, sponsored data and pure zero-rating in particular, these single-site or service plans have been relatively uncontroversial. Even so, both Google and Facebook have been criticized for acting as the "gatekeepers" to the Internet for the millions of users who access it exclusively through their zero-rated sites.[52] Nor does it help their case that in many parts of the developing world, single-site plans like Facebook Zero have led to startling misperceptions in the minds of millions of users about what the Internet is and is not.[53] In direct response to Facebook and Wikipedia's single-service plans, Chile became the first country to adopt net neutrality regulations prohibiting them outright,[54] although it later backtracked on Wikipedia Zero.[55] Aside from violating net neutrality principles, these single-site plans in Chile were criticized as representing "bubbles created by companies like Google and Facebook to make sure their products become synonymous with 'the Internet' in consumers' minds."[56]

---

[47] See Mims, *supra* note 44.

[48] See Wauters, *supra* note 43.

[49] *Id*.

[50] "One Year In: Internet.org Free Basic Services", Internet.org, July 27, 2015. Available at: http://bit.ly/2gcQRFz [https://perma.cc/S5WW-CSRB]; Mozilla Study *supra* note 23 at 12; Stanford Study *supra* note 23 at 5; West, Darrell M., "Digital divide: Improving Internet access in the developing world through affordable services and diverse content", Center for Technology Innovation at Brookings, February 2015. Available at: http://brook.gs/2f1egHp [https://perma.cc/SM2D-AMKN].

[51] Wauters, Robin, *supra* note 43.

[52] Mott, Nathaniel, *supra* note 41.

[53] Mirani, Leo "Millions of Facebook Users Have No Idea They're Using the Internet", *Quartz*, February 9, 2015. Available at: http://bit.ly/1DbSWnK [https://perma.cc/69EF-4RVW]. Out of 699 respondents in Nigeria and Indonesia using Facebook Zero, nearly 10 percent (68) said they did not use the Internet.

[54] Walker, Lauren, "How is Net Neutrality Working for the Countries That Have It?", *Newsweek*, September 10, 2014. Available at: http://bit.ly/1lWlkov. *See also infra* notes 203 - 227 and accompanying text.

[55] Rossini Public Knowledge Report, *supra* note 23, at 19.

[56] Mott, Nathaniel, "Chile Should Be Commended for Taking away Facebook and Wikipedia", *Pando*, May 30, 2014. Available at: http://bit.ly/2fVY6i4 [https://perma.cc/P3V6-8PTT].

I.A.II. Sponsored data

In this model, content providers contract with and pay a telecom service provider to offer a range of information or services at no cost to users. The best-known example may be AT&T's Sponsored Data service. Launched in January 2014, AT&T's program allows advertisers to sponsor mobile data for its subscribers.[57] Such sponsorship also includes allowing companies to sponsor "business-related data usage for [their] employees, or sponsor data as part of a customer loyalty program."[58] Similar sponsored data plans are being promoted by telecoms in other countries as well. In 2015 an Indian telecom, Bharti Airtel, launched a platform of zero-rated services, Airtel Zero, to some controversy.[59] This platform offered subscribers access to a range of sites and local services whose providers paid Airtel to be included.[60] Alternatively, the telecom company itself might sponsor (or exempt from data charges) a defined set of sites or services in order to enhance its competitiveness in relation to rival telecom providers.[61] T-Mobile's free music service is an example of this type of company "self-sponsored" data plan. Its "Music Freedom" arrangement enables subscribers to access music streaming services like Pandora, iTunes Radio, and Spotify, without counting it against the users' data usage caps.[62] In other words, T-Mobile itself exempts the selected content usage from its data charges and thus "pays" for the music streaming by customers.[63]

Sponsored data plans are popular among telecom service providers for a reason. Regardless of which version of the model a telecom adopts, it bene-

[57] Bergen, Mark, "Net Neutrality Likely to Permit Sponsored Data Plans", *AdvertisingAge*, February 12, 2015. Available at: http://bit.ly/17o2653 [https://perma.cc/7YCD-KPXE]. Sponsored data can take most any form, including advertising, games, commercial apps, or content. *See* "Sponsored Data Not Hurt by Net Neutrality, Benefits Consumers says Strategy Analytics", *PR Newswire*, March 11, 2015. Available at: http://prn.to/2eWX56A [https://perma.cc/9FUT-ETCW].

[58] Brandom, Russell, "Sponsored Data: AT&T Will Now Let Companies Buy Out Your Data Charges for Specific Videos and Apps", *The Verge*, January 6, 2014. Available at: http://bit.ly/1bLhMJO [https://perma.cc/LJ4N-ZBBM].

[59] "CEO Defends Airtel Zero Despite Backlash", *Gadgets Now*, April 18, 2015, Available at: http://bit.ly/2fuD6jK [https://perma.cc/7E7N-NQ7W].

[60] *Id*.

[61] "Data Caps", Public Knowledge, available at: http://bit.ly/2fW6TjL [https://perma.cc/SA4J-4V2D].

[62] Levy, Adam, "*T-Mobile Music Freedom Is Ultimately Bad for Consumers*", *The Motley Fool*, June 26, 2014. Available at: http://bit.ly/2eCl0gz [https://perma.cc/N9TP-W9VP].

[63] *Id*.

fits not just from the payments received from content providers (unless the telecom is the sponsoring entity), but also by giving users the opportunity to access free data or services on their network, making it more attractive to actual and potential subscribers. The content providers, of course, benefit by increasing their exposure to potential new customers and collecting some personal data from users. Sponsored data plans are similar to single-site plans because some may involve a particular content provider making payments to the telecom to offer their site, information, or services free to customers. Arrangements where Facebook Zero, or Google Free Zone paid their telecom partners to exempt access to their respective content and services from data charges would also fall into this category.

Sponsored data plans have been criticized on a number of grounds. Digital rights advocates have condemned AT&T's Sponsored Data service as a transgression of net neutrality principles because it treats different sources of content differently.[64] On purely economic and competition grounds, sponsored data "giv[es] companies with more resources and . . . capital to spend on advertising an upper hand," while disadvantaging start-ups and entrepreneurs who cannot afford to pay telecoms to make their content available to consumers for free.[65] Airtel Zero was criticized on the same grounds.[66] T-Mobile's "Music Freedom" falls into this category too, because it does not support every music streaming service, and thus can be perceived as prioritizing certain sources of online (music) content on its network at the expense of others.[67]

Proponents of sponsored data respond that so long as the service pricing is reasonable with equal access for all companies wishing to participate, there is no harmful discrimination or prejudice to consumers, only benefits.[68] On this view, non-discriminatory access to purchasing sponsored data reflects no anti-competitive or unfair behavior because everyone is

[64] Becker, Sam "Here's Why No One Is Buying into AT&T's Sponsored Data Plan", *The Cheat Sheet*, July 29, 2014. Available at: http://bit.ly/2eClZgO [https://perma.cc/U948-T97K].

[65] *Id*.

[66] "CEO Defends Airtel Zero (…)", *supra* note 58.

[67] *See, e.g.*, Masnick, Mike, "Music Freedom or Holding Consumers Hostage? Letting ISPs Pick Winners and Losers Is a Problem", *TechDirt*, June 19, 2014. Available at: http://bit.ly/1nRmbUE [https://perma.cc/A8AR-KPNV].

[68] *See, e.g.*, "Airtel Launches 'Airtel Zero': A Win-Win Platform for Customers and Marketers", Airtel, April 6, 2015. Available at: http://bit.ly/1H0l8L7 [https://perma.cc/NQ3K-9KV7]; Anderson, Steve, "Airtel Unveils Sponsored Data Services", TMCnet, April 7, 2015. Available at: http://bit.ly/2fUPV7H [https://perma.cc/FAV6-SUBJ]

treated equally; this "no harm, no foul" approach leads to the conclusion that there would be no meaningful violation of net neutrality under such circumstances.[69] Supporters in the United States and India have likened sponsored data plans to the "toll free" or "1-800" dialing approved by the FCC, whereby the public interest is served by companies paying for charges rather than the consumer.[70]

I.A.III. Compound zero-rating

Compound zero-rating plans are those in which a sponsoring company (or companies) partners with a telecom service provider to grant subscribers access to a bundle of selected sites and services. Generally, these zero-rated platforms provide free access to a wide range of local and other select content as determined by the sponsoring companies, often in consultation with government authorities.[71] Accordingly, these plans are more like a platform of curated offerings accessed through a subscriber's mobile phone. Unlike sponsored data services, they do not require payments to or by the telecoms, which can forego such fees in exchange for enhanced offerings to customers and an increased subscriber base.[72] Telecoms benefit by attracting new users who might not otherwise be able to (or want to) pay for a data plan and online access. The content providers and telecoms can claim both to be offering a service and creating new market opportunities for users to

[69] "CEO Defends Airtel Zero (…)", *supra* note 58.

[70] *See* "AT&T Introduces Sponsored Data for Mobile Data Subscribers and Business", AT&T, January 6, 2014. Available at: http://soc.att.com/2fRUzRm [https://perma.cc/ERD7-SKZ8]; Bode, Karl, "*Despite Limited Interest in AT&T's Sponsored Data, Company Still "Bullish" on Its Awful Precedent*", *Tech Dirt*, February 5, 2015. Available at: http://bit.ly/2ge51Wo [https://perma.cc/NU8Y-FFFE] ("To hear AT&T pitch it at the time, this would be akin to 'free shipping' or a 1-800 number for data . . . ."); "CEO Defends Airtel Zero (…)", *supra* note 58.

[71] Mark Zuckerberg and President Juan Manuel Santos of Colombia launch Internet.org in Bogota. "Internet.org App Launches in Colombia", Internet.org, January 14, 2015. available at: http://bit.ly/2g2eLjQ [https://perma.cc/9K62-QMQT]; *see also* Antunes, Anderson, "Mark Zuckerberg Meets with Brazil's President at the 7th Summit of the Americas, in Panama", *Forbes*, April 11, 2015, available at: http://bit.ly/2f8kdTb [https://perma.cc/CWG8-LD6L]; Constine, Josh, "Indian Prime Minister Tells Zuckerberg Social Media Creates a New Form of Diplomacy", *Tech Crunch*, September 27, 2015, available at: http://tcrn.ch/2gmxnhZ [https://perma.cc/6Y9K-2NGL].

[72] Post, David, "Facebook, Internet.org, and the Net Neutrality Bugaboo", *The Washington Post*, August 17, 2015, available at: http://wapo.st/2fZKOAK [https://perma.cc/SV34-UQRE].

access additional data or services for a fee.[73] Despite their apparent utility, these plans are among the most controversial type of zero-rating to date for a variety of reasons discussed below.

As mentioned above, Google Free Zone has attributes of both a single-service and a compound zero-rating plan.[74] Airtel Zero in India combined features of sponsored data and compound zero-rating before it was shut down by the Indian regulator's decision to ban all differential pricing by telecoms, including zero-rating.[75] But Facebook's original Internet.org, now part of the Free Basics connectivity platform, is an unalloyed example of a compound zero-rating plan.[76]

Founded in August 2013, Internet.org seeks to close the digital divide by providing entire populations in less developed countries with affordable access to dozens of services on the Internet without charge, with wider access provided for a fee.[77] It is an "initiative bringing together technology leaders, nonprofits and local communities to connect the two thirds [sic] of the world that doesn't have [I]nternet access."[78] For example, among the free sites and services that Internet.org offered in India before it was shut down were Facebook, Messenger, BBC World News, Bing Search, and Wikipedia. In addition, it gave access to other home-grown sites that provided local weather, area and sporting news, classified ads for employment,

[73] There is evidence that this business model works. Facebook reports that "more than half of the people who come online through Internet.org are paying for data and accessing the internet within the first 30 days". "One Year In: Internet.org Free Basic Services", Internet.org, July 27, 2015, available at: http://bit.ly/2fZOKBn [https://perma.cc/JCG2-PSBB]. *See also* Peel, Anna, "Facebook: More People Are Online Thanks to Internet.org", *Value Walk*, July 27, 2015, available at: http://bit.ly/2fJdaP7 [https://perma.cc/58AP-J4EU] (quoting Facebook VP Chris Daniels as saying that users who join Internet.org subsequently "want to move on and experience more Internet").

[74] *See supra* notes 35 - 40 and accompanying text.

[75] *See supra* notes 57 - 59 and accompanying text; Telecom Regulatory Authority of India (TRAI), Press Release No. 13/2016, February 8, 2016, available at: http://bit.ly/1Q4SEIh [https://perma.cc/4WQ5-N5H5].

[76] Constine, Josh, "Internet.Org's App with Free Access to Facebook, Google, Wikipedia, Local Info Launches in Zambia", *Tech Crunch*, July 31 2014, available at: http://tcrn.ch/1odKN6N [https://perma.cc/89BV-ZGJN]; Mirani, Leo, "Millions of Facebook Users Have No Idea They're Using the Internet", *Quartz*, February 9, 2015, available at: http://bit.ly/2fJmna6 [https://perma.cc/7S2J-SY5T]; "Update to Internet.org Free Basic Services", Internet.org, September 24, 2015, available at: http://bit.ly/2g11MRs [https://perma.cc/2SCT-Z2RT].

[77] "Who We Are", Internet.org, https://internet.org/about [https://perma.cc/VZL7-JR65].

[78] *Id*.

information on health, maternal and child care, and even music.[79] To date Facebook has partnered with Airtel, Ericsson, and Nokia, among others, in this endeavor.[80] Currently, Internet.org is available to over a billion people in at least 42 nations in Africa, Asia, and Latin America.[81] Those countries include Bangladesh, Colombia, Ghana, India, Indonesia, Kenya, Mexico, Nigeria, Pakistan, the Philippines, Senegal, South Africa, and Zambia[82]

Facebook's stated mission for the Internet.org/Free Basics platform is to bring connectivity to the part of the world's population that still lacks it.[83] Many question the altruistic justification for this initiative, claiming that it is at bottom a market-expansion tactic.[84] For example, the rolling out of Internet.org in India in February 2015 sparked a wave of protest from digital rights activists around the world concerned with protecting net neutrality, freedom of expression and privacy.[85] In a coordinated response to the public defense of Internet.org by Mark Zuckerberg,[86] dozens of global and national advocacy groups including Access, Bits of Freedom, and the Center for Media Justice took issue with Facebook's concept of net neutrality, claiming

[79] Alwani, Rishi, "Facebook's Internet.org Comes to India: Everything You Need to Know", Gadgets 360, February 11, 2015, available at: http://bit.ly/2g10tCe [https://perma.cc/N28Y-656P]. *See also* "Internet.org App Now Available in India", Internet.org, February 10, 2015, available at: http://bit.ly/2fZR6yQ [https://perma.cc/2349-UXXP]. Internet.org does not give users access to an email service. The Internet.org offerings vary from country to country, and most are not as extensive as those that were available in India. This is the case, for instance, in Zambia and Colombia. *See* Rosen, Guy, "Introducing the Internet.org App", *Facebook newsroom*, July 31, 2014, available at: http://bit.ly/1rS55Kp [https://perma.cc/W8SN-ZWKB]; Internet.org, *supra* note 70.

[80] *See* Lunden, Ingrid, "Facebook-Led Internet.org Partners with Nokia on SocialEDU in Rwanda, Unilever in India, Ericsson on New Lab to Connect Developing Economies", *Tech Crunch*, February 24, 2014, available at: http://tcrn.ch/2f4F5av [https://perma.cc/MRQ3-9V3Q].

[81] *See* Sirohi, Seema, "Sorry Mark Zuckerberg, the World Bank Also Disagrees with You", *The Economic Times Blog*s, January 16, 2016, available at: http://bit.ly/2fl6gik [https://perma.cc/E3SD-W8RH].

[82] "Where We've Launched", Internet.org, http://bit.ly/2g16vTd [https://perma.cc/F3XX-L5Q8].

[83] *See* "Announcing the Internet.org Platform", *Facebook Newsroom*, May 4, 2015, available at: http://bit.ly/1JL4Utg [https://perma.cc/FS8D-5AMY].

[84] *See, e.g.*, Imtiaz, Asif, "Nothing Altruistic About Facebook's Initiative to Spread the Internet", *US Finance Post*, January 6, 2014, available at: http://bit.ly/2fl66rg [https://perma.cc/XBH5-XRD9]; Shashidhar, KJ, "Sunil Mittal Calls It Right: What Zuck Is Doing with Internet.org Isn't Philanthropy", *Medianama*, March 9, 2015, available at: http://bit.ly/2fZZ1xB [https://perma.cc/4LDL-AUD5].

[85] *See supra* notes 3, 14, and accompanying text.

[86] *See supra* note 16 and accompanying text.

that it was not based on a "true" definition of the term.[87] They expressed concern "that access for impoverished people [was being] construed as justification for violations of net neutrality."[88] In their view, because the zero-rating underpinning Internet.org is "inherently discriminatory," it not only violates net neutrality but also "endangers freedom of expression and equality of opportunity by letting service providers decide which Internet services will be privileged over others, thus interfering with the free flow of information and people's rights *vis-a-vis* networks."[89]

In response to the criticism that it was acting as a "gatekeeper" by choosing certain apps, services, and content over others, thereby creating a "two-tiered" Internet for users, Facebook announced in May 2015 that it was opening its Internet.org platform generally to "any low-bandwidth online service that meets its technical guidelines."[90]

I.A.IV. Faux (or non-selective) zero-rating

Faux zero-rating plans are those that seem to implicate net neutrality but in effect do not. In this model, a content provider partners with one or more telecom companies to offer limited amounts of free data to users in exchange for meeting certain conditions, such as viewing an advertisement or downloading an application. Users are free to use the complementary data as they choose. Because neither the content providers nor the telecoms decide what applications, services, or sites a subscriber accesses with his or her allotment of free data, faux zero-rating plans do not raise the discrimination or anti-competitive net neutrality concerns that "selective" or "true" zero-rating practices do.[91] Strictly speaking, they are not zero-rating at all, if zero-rating is defined as a practice that limits consumer choice in accessing the mobile Internet, as it commonly is.[92] Telecoms and content providers benefit from faux

[87] *Open Letter supra* note 7.

[88] *Id*.

[89] *Id*.

[90] Ribeiro, John, "Facebook's Internet.org Opens Platform to Other Online Services", *Computerworld*, May 4, 2015. Available at: http://bit.ly/2eXwrOx [https://perma.cc/4TJ9-8HGV].

[91] *See* Bode, Karl, "*Mozilla: If Facebook Really Wants to Help Developing Nations, It Should Ignore Zero Rating and Fund Real Internet Access*", *Techdirt*, May 15, 2015. Available at: http://bit.ly/1IFSmmx [https://perma.cc/YPE8-FTWJ].

[92] *See* Baker, Mitchell, *supra* note 7 and accompanying text. ("Zero-rating as practiced today is 'selective zero-rating for a few apps and websites; exclusion for the rest of the Internet.'").

zero-rating plans by attracting new users to their brand, and/or to their specific hardware or software, while telecoms also benefit from offering customers the opportunity to enhance their data access, all without offending net neutrality.

Mozilla's so-called "equal-rating" strategies aimed at expanding markets while helping to close the digital divide in the developing world are a perfect example.[93] In Mozilla's view, prevailing practices of "selective" zero-rating are the wrong answer to the right question of how best to promote greater connectivity in the developing world:

The correct answer is that all data is transmitted at the same price, whether that price is "zero" or anything else. This way, consumers pick the content they choose to access based on the quality of that content, not the financial power and business partnerships of the provider. This way, new entrepreneurs can still reach any and all users on the Internet, even if they are a few people working in a co-working space with no ability to subsidize data charges.[94]

In furtherance of these strategies, Mozilla announced in May 2015 that it had partnered with Orange, a global telecom provider that operates in various African and Middle Eastern countries, to offer a low-cost Orange phone using the Firefox operating system in 13 new markets.[95] The Klif phone, as it is called, costs about $40 and comes pre-loaded with unlimited talk, text, and 500 MB of free data per month for six months.[96] This initiative presumably built upon Mozilla's experience in Bangladesh, where it has partnered with Grameenphone (owned by Telenor) to offer its users 20 MB of free data per day for Internet access if the customer first watches an advertisement.[97] In Mozilla's view, "[s]caling up arrangements like these could represent a long-term solution to the key underlying problems of digital inclusion and equality" without the negative consequences incurred by selective zero-rating practices.[98]

Mozilla is not the only company innovating in this field. Since 2014, Jana,

---

[93] Baker, *supra* note 90.

[94] *Id.*

[95] Dixon-Thayer, Danelle, "Mozilla View on Zero-Rating", *The Mozilla Blog,* May 5, 2015, available at: https://mzl.la/1RbY81R [https://perma.cc/N7ZB-VTEA]; "Firefox OS Proves Flexibility of Web", *The Mozilla Blog*, March 1, 2015, available at: https://mzl.la/1M0NJlP [https://perma.cc/563G-LFCE]. Countries where the Klif phone will initially be offered are Egypt, Senegal, Tunisia, Cameroon, Botswana, Madagascar, Mali, The Ivory Coast, Jordan, Niger, Kenya, Mauritius and Vanuatu.

[96] Dixon-Thayer, *supra* note 94.

[97] *Id.*

[98] *Id*.

a Boston-based company, has promoted its mCent app to much acclaim.[99] The app encourages users to access third-party sites or services free of charge by crediting their data plans for doing so.[100] Users are thus "awarded airtime for a number of different kinds of activities, including downloading and using apps, taking surveys, watching videos, signing up for a service, and/or participating in contests."[101] The content providers who partner with mCent, such as Twitter and Amazon, as well as local music and texting services, pay Jana to make their applications available for subscribers to test out through mCent.[102] It is projected to have upwards of 30 million users in the developing world.[103]

Likewise, the India and Silicon Valley-based start-up Marvin employs a strategy to reward customers with free data when they access content online through Marvin's application, Gigato. Like mCent, Gigato combines aspects of sponsored data and faux zero-rating.[104] Its corporate customers pay to have their sites and services advertised on a users' phone through strategically placed content and advertisements.[105] When consumers access the third-party sites, Gigato credits the users' data plan directly.[106] The subscriber can then use the data credits to access whatever Internet content they choose. As advertised, "Gigato provides free unrestricted Internet data for your Android. Use the apps you love and get megabytes recharged to your prepaid account."[107]

I.B. National Perspectives on Internet Access and Net Neutrality

In this section we turn our attention to the regional and national contexts in which net neutrality policies like zero-rating are implemented. It is divi-

[99] *See* Olson, Parmy, "This App Is Cashing in on Giving the World Free Data", Forbes, July 29, 2015. Available at: http://bit.ly/2g2x1d6 [https://perma.cc/S2M3-RRT6].

100 *See* Rossini, Carolina and Moore, Taylor, Public Knowledge Report; *supra* note 23, at 7.

[101] mCent, http://bit.ly/2flfATb [https://perma.cc/256Z-MRA7].

[102] *See* Olson, *supra* note 98.

[103] *See* Howard, Alexander, "Gigato Tried to Make Internet Access Affordable with Data Rebates", *The Huffington Post*, July 31, 2015. Available at: http://huff.to/2flgijs [https://perma.cc/N5JL-X9SC].

[104] *Id*.

[105] *See* Rossini, Carolina and Moore, Taylor, Public Knowledge Report; *supra* note 23; *see also* GigaTo, http://bit.ly/2gkMVlF [https://perma.cc/WZ5T-MA56].

[106] *See* Rossini, Carolina and Moore, Taylor, Public Knowledge Report; *supra* note 23.

[107] Gigato Application, Google Play, http://bit.ly/1SFxtZ9 [https://perma.cc/PU6D-XRDN].

ded into three sub-sections. The first focuses on marshaling key statistical indicators for a sample of ten countries organized by region (Africa, Asia, Europe and North America, and South America). They were selected using criteria aimed at putting together a functional cross-section of global experiences viewed from both a quantitative and qualitative perspective. The criteria applied were regional representation; policy or practice relating to net neutrality and zero-rating; status as a developed country, developing country, or least developed country;[108] and levels of democratic and Internet freedom. The quantitative indicators selected provide a cross-section of each country's developmental status in social, economic, and political terms, and include figures for fixed and mobile Internet coverage. Together this data paints a broad but useful panorama of the different domestic settings in which zero-rating takes place around the world. The second sub-section then shifts to a thematic perspective, looking at the various barriers to Internet access as they manifest in countries with low connectivity. The final section aims to score a deeper understanding of how zero-rating is being addressed by governments in different domestic contexts through three country case studies."

I.B.I. Background & Context

There are currently at least 60 states that actively authorize some form of zero-rating in practice.[109] But there is a growing number that have banned it or are in the process of doing so. Notably, the Council of Europe recently adopted net neutrality guidelines that could restrict zero-rating throughout Europe,[110] though effective implementation of those protections by member

[108] For a more detailed description of the typology of country development utilized throughout this article, see *infra* Table 3, *infra* notes 125-127; *see also* U.N. Stat. Division, Composition of Macro Geographical (Continental) Regions, Geographical Sub-regions, and Selected Economic and Other Groupings, October 31, 2013. Available at: http://bit.ly/2bQCsNZ [https://perma.cc/9MCQ-738U].

[109] *See* "Wikipedia Zero Operating Principles", *supra* note 32; Internet.org, "Wikipedia", http://bit.ly/2gmNqfS [https://perma.cc/T6SP-EPTD] (Colombia, Ghana, Guatemala, India, Kenya, Philippines, Tanzania, and Zambia); Google Free Zone (India, Nigeria, Philippines, Sri Lanka, and Thailand); Mims, Christopher, *supra* note 44; Drossos, Antonios, *supra* note 29; Wikipedia, "Facebook Zero", http://bit.ly/2g1cc3s [https://perma.cc/47LN-SX9L] (Bangladesh, Cameroon, El Salvador, Fiji, France, Germany, Greece, Georgia, Guinea, Indonesia, Kosovo, Malaysia, Morocco, Myanmar, New Zealand, Pakistan, Panama, Philippines, Poland, Qatar, Suriname, Trinidad and Tobago, Tunisia, United Kingdom, Zimbabwe).

[110] McCarthy, Kieren, *supra* note 20. ("The guidelines are not legally binding but will almost certainly result in legislation that follows its lead being passed across Europe.

States remains a concern.[111] In addition, the following countries have or have had laws that either do not permit or expressly ban zero-rating practices: Chile, Brazil, Norway, Netherlands, Finland, Iceland, India, Estonia, Latvia, Lithuania, Malta, Japan, and Slovenia.[112] Several countries that only discouraged zero-rating in the past now prohibit it.[113] Significantly, not one of the countries that currently prohibit zero-rating is located in Africa. Chile, Brazil and now India are the only developing nations to ban zero-rating to date, though enforcement is lax and the practice continues.[114] In order to better understand the profiles of each set of countries—those that permit zero-rating and those that do not—this sub-section compiles key indicators measuring the social, economic, and political conditions in a cross-section of ten countries from the principal regions of the world. It organizes the data into a series of illustrative tables, each organized to highlight critical factors in the analyses to follow in subsequent Parts of this article, as explained below.

Table 1 summarizes the current status in general terms of the selected countries' efforts to regulate net neutrality and zero-rating, organized by region, as follows:

The council is separate from the European Union, but it is influential, being made up of foreign ministers and other politicians from 47 member states.").

[111] Berners-Lee, Tim, Lessig, Lawrence and van Schewick, Barbara, "Four Days to Save the Open Internet in Europe: an Open Letter", Web Foundation, July 14, 2016. Available at: http://bit.ly/29H4APL [https://perma.cc/6UVQ-7JXU] [hereinafter Open Letter]; Bode, Kari, "Europe's Flimsy Net Neutrality Rules Go Live, Are Actually Worse than No RulesAt All", *Techdirt*, May 6, 2016. Available at: http://bit.ly/2fJGLaY [https://perma.cc/PWK9-W8VA].

[112] States that banned before India chose to do so in February 2016: Chile, Brazil, Norway, Netherlands, Finland, Iceland, Estonia, Latvia, Lithuania, Malta, Japan and Slovenia. *See* Romit Guha, Romit & Aulakh, Gulveen, "Zero Rating: What Are Countries Doing About It", *Gadgets Now*, April 21, 2015. Available at: http://bit.ly/2gkVXz7 [https://perma.cc/G6T3-3GLE]; Layton, Roslyn and Elaluf-Calderwood, Silvia Monica, *supra* note 23; *see also* Rossini, Carolina and Moore, Taylor, Public Knowledge Report; *supra* note 23, at 39 (finding that recently enacted net neutrality protections in Brazil do not allow for zero-rating exceptions).

[113] For states that discourage zero-rating and where wireless companies do not practice it, see Meyer, David, "Pro-net Neutrality Norway Advises Carriers to Avoid Zero-Rating", *Gigaom*, November 8, 2014. Available at: http://bit.ly/1zc9iHa [https://perma.cc/GF4R-95P5], (Norway, Finland, Sweden, Estonia, Lithuania, Latvia, Malta, and Iceland—of these countries all but Sweden now have laws against zero-rating).

[114] *See* International Telecommunication Union (ITU), Country Classifications by Region and Development Status, available at: http://bit.ly/2eKMoJr [https://perma.cc/M8GK-RCFF]; *see* U. N. Stat. Division, *supra* note 107; Rossini, Carolina and Moore, Taylor, Public Knowledge Report; *supra* note 23, at 16-20 (Chile) and 39-46 (Brazil). For a discussion of the current panorama in India, see *infra* Part III.B.

Table 1: Net Neutrality & Zero-Rating Context By Region

Country	Region	Net Neutrality	Zero-Rating
South Africa	**Africa**	Not regulated	Permitted
Zambia		Not regulated	Permitted
India	**Asia**	Not regulated	Banned
Malaysia		Not regulated	Permitted
Netherlands	**Europe**	Regulated by law[115]	Banned
Slovenia		Regulated by law[116]	Banned
Canada	**North America**	Regulated by administrative agency[117]	Banned
United States		Regulated by administrative agency[118]	Permitted in certain cases
Chile	**South America**	Regulated by law[119]	Banned*
Colombia		Regulated by law[120]	Permitted

Table 2 presents data on fixed and mobile broadband Internet access for these same countries. The statistics are ordered to highlight the percentage of fixed broadband subscriptions in each country, moving downwards from lowest to highest levels of penetration.

[115] Infra Part I.B.II.e.

[116] Wieland, Ken, "Mobile Operators in Slovenia Fall Foul of Net Neutrality Rules", Mobile World Live, January 26, 2015, available at: http://bit.ly/2fAEykL [https://perma.cc/E79K-GY8M].

[117] Government of Canada, News Release, "Archived—CRTC Continues to Set the Course for the Future of Television with Let's Talk TV Decisions", January 29, 2015. Available at: http://bit.ly/2fJFilb [https://perma.cc/9PWG-KLRC].

[118] Infra Part II.B.II.g.

[119] Infra Part II.B.II.a. *Zero-rating is banned by law but tolerated in practice.

[120] Infra Part II.B.II.b.

Table 2: Fixed & Mobile Broadband Internet Access

Country	Region	2014 Fixed Broadband subscriptions (per 100 people)[121]	2013 Mobile Broadband subscriptions (per 100 people)[122]	2014 Mobile Cellular subscriptions (per 100 people)[123]	2014 Internet Users (per 100people)[124]
Zambia	Africa	0.14	0.7	67	17.3
India	Asia	1.24	3.2	74	18.0
South Africa	Africa	3.21	25.2	150	49.0
Malaysia	Asia	10.14	12.5	149	67.5
Colombia	South America	10.27	7.9	113	52.6
Chile	South America	14.08	35.6	133	72.4
Slovenia	Europe	26.55	41.8	112	71.6
United States	North America	30.37	92.8	98	87.4
Canada	No Data	**34.38	41.0	83	87.1
Netherlands	No Data	41.02	62.3	116	93.2

** Canada's fixed broadband access data was not available for 2014, so the data from 2013 has been presented in its place.

Contrasted with the fixed broadband access statistics are those showing mobile phone coverage and wireless broadband subscriptions. European and North American countries have considerably higher fixed broadband penetration than those in other regions (South Korea and Japan being notable exceptions in Asia). But the data for mobile cellular coverage are largely comparable across regions, with especially high levels (more than 100%) in a number of Asian, African and South American States. Notably, South Africa has the highest mobile coverage of the ten countries studied, yet the third lowest fixed

[121] The World Bank, "Fixed broadband subscriptions (per 100 people)". Available at: http://bit.ly/1VWgtnl [https://perma.cc/EH9H-87DL].

[122] International Telecommunication Union (ITU), Country profile. Available at: http://bit.ly/1Pk9X5l [https://perma.cc/PSV4-PW9H].

[123] The World Bank , "Mobile cellular subscriptions (per 100 people)". Available at: http://bit.ly/1mbk1iH [https://perma.cc/ZF77-WVZB]. Mobile cellular subscriptions are defined as those that provide voice communication access to public mobile telephone service using cellular technology. Id.

[124] The World Bank, "Internet users (per 100 people)". Available at: http://bit.ly/1hq7God [https://perma.cc/9Y5B-9NT9].. Internet users are defined as people who have access to the worldwide network. Id.

broadband penetration. Also worth highlighting is the substantial difference between mobile *broadband* access, which is still relatively scarce in developing countries, and mobile cellular access in those same countries, which, as pointed out already, can be very high and on par with their more developed European and North American counterparts. It is important to recall here that the zero-rating plans described in the prior section are all accessed through cellular (non-smartphone) telephones and do not require broadband coverage.

Table 3 below highlights each country's gross domestic product (GDP) per capita in ascending order from lowest to highest. It contrasts the GDP data with each country's developmental and inequality rankings according to the United Nations Development Programme (UNDP). Looking at Tables 2 and 3 together, it appears—unsurprisingly—that per capita GDP correlates strongly with overall Internet usage, and in particular fixed broadband penetration. Interestingly, mobile coverage and, to a lesser extent, mobile broadband penetration show little correlation with GDP per capita or income inequality; for example, Chile has the highest mobile broadband penetration of any of the countries studied outside of Europe and North America, despite having a middling GDP per capita and the third highest income inequality of the group.

Table 3: GDP & Human Development Index Statistics

Country	Adult Literacy Rate (in percent)11	2014 GDP per capita12	GINI Inequality Index13 (0 is "perfect equality"; 100 is "perfect inequality")	2014 UNDP Human Development Index Rank (out of 187 countries) and Range Standing14
Zambia	84	4086.00	55.6	141 (Medium)
India	69	5,833.30	33.9	135 (Medium)
South Africa	93	13,046.20	63.4	118 (Medium)
Colombia	94	13,046.40	53.5	98 (High)
Chile	97	22,333.10	50.5	41 (Very High)
Malaysia	No Data	24,714.80	46.3	62 (High)
Slovenia	100	29,917.00	25.6	25 (Very High)
Canada	No Data	44,088.50	33.7	8 (Very High)
Netherlands	No Data	47,130.70	28.0	4 (Very High)
United States	No Data	54,629.50	41.1	5 (Very High)

Finally, Table 4 reviews several indicators reflecting each country's levels of democracy and political freedom, corruption, and Internet freedom, specifically. Generally speaking, the European and North American countries display stronger tendencies in these areas than most of the countries from the other regions. It is noteworthy that the countries in our study that have banned zero-rating possess the highest possible levels of democracy (9 or 10 out of 10). Additionally, most of the zero-rating banning countries score well on the Corruption Perception Index, with the exception of India and possibly Slovenia.

[125] Freedom House, "Freedom in the World 2015", 2015. Available at: http://bit.ly/2fCTl8Y [https://perma.cc/D3M4-G5JG].

[126] The World Bank , "GDP per capita, PPP (current international $)". Available at: , http://bit.ly/18gtvTm [https://perma.cc/D9W7-JB5A]. According to the World Bank, "PPP GDP is gross domestic product converted to international dollars using purchasing power parity rates. An international dollar has the same purchasing power over GDP as the U.S. dollar has in the United States." Id.

[127] The World Bank, "GINI index". Available at: http://bit.ly/TLu3fJ [https://perma.cc/EPZ6-23TJ] (reflecting the most recent statistics published by the World Bank: 2009-2013).

[128] United Nations Development Programme, Human Development Data (1980-2015), Statistical Tables, Table 1. Available at: http://bit.ly/1kYwvXA [https://perma.cc/S5B2-ARFV].

Table 4: Indices on Democracy, Freedom & Corruption[129][130][131][132]

Country	2015 Freedom House Index (1 is "most free"; 7 is "least free")15	2015 Freedom House Internet Freedom Score (0 is best, 100 is worst)16	2014 Polity IV Democracy Index (out of 10)17	2014 Corruption Perception Index18 (0 is "highly corrupt"; 100 is "very clean")
Malaysia	4	"Partly Free" – 43	6	52
Colombia	3.5	"Free" – 32	7	37
Zambia	3.5	"Partly Free" – 40	7	38
India	2.5	"Partly Free" – 40	9	38
South Africa	2	"Free" – 27	9	44
Slovenia	1	NO DATA	10	58
Chile	1	NO DATA	10	73
United States	1	"Free" – 19	10	74
Canada	1	"Free" – 16	10	81
Netherlands	1	NO DATA	10	83

I.B.II. Barriers to Connectivity

No one disputes the persistence of a vast gulf between the world's population that enjoys access to an Internet connection and the population that does not, nor the fact that most of that digitally enfranchised population live in developed countries. The total number of Internet users has grown rapidly over the past two decades to over 3 billion today, of which nearly 80% reside in developed countries.[133] "[D]eveloping countries [on the other hand] are home to about 90 percent of the 4 billion people not yet using the Internet."[134] So, for example, "[w]hile Europe has an Internet penetration rate of over 75 percent, only about [20 percent] of African households are connected."[135] This is true of other places as well: India and Indonesia, two

[129] Freedom House, "Freedom in the World 2015", 2015. Available at: http://bit.ly/2fCTl8Y [https://perma.cc/D3M4-G5JG].

[130] Freedom House, "Freedom on the Net 2015. Table of Country Scores", 2015. Available at: http://bit.ly/1M1okue [https://perma.cc/DRA3-ZWWK].

[131] Center for Systemic Peace, "Polity IV Annual Time-Series, 1800-2015", Integrated Network for Societal Conflict Research. Available at: http://bit.ly/1RD6fl7 [https://perma.cc/LT8X-6QMB].

[132] Transparency International, "Corruption Perception Index 2014: Results", 2014. Available at: http://bit.ly/1tLovwg [https://perma.cc/K6US-8GS7].

[133] *Id*.

[134] Stanford Study, *supra* note 23, at 3.

[135] *Id.*

of the world's most populous nations, have Internet user rates of under 20 percent.[136] These statistics speak not just to the existence of a digital divide *between* States, but also *within* them. The technical, political, social, and economic conditions for the digital divide *globally* are merely an agglutination of the causes behind the digital divide *domestically*, which separates the digital "haves" from the "have-nots" within a given society. Not surprisingly, then, because developing countries have the largest proportions of digitally disenfranchised people, to whom the great social, economic, political and cultural benefits offered by an Internet connection are not accessible, they are the front lines in the struggle to close both divides.[137]

Generally, the barriers to connectivity prevailing in most developing countries fall into two types: "hard" and "soft." Hard barriers are those external factors that shape whether technical access to an Internet connection exists or can be exercised in a particular society. Examples of such factors are a lack of physical infrastructure, the quality of connections to the Internet where one exists, and the high cost of access in low-income countries.[138] Soft barriers, on the other hand, are those that limit the personal capacity of potential users or their incentives to access an Internet connection where one is available or offered, such as education and literacy levels.[139] "Hard" and "soft" barriers to connectivity combine to perpetuate the digital divide within countries, and thus globally, though much more attention is generally paid to hard barriers.

A number of factors act as hard barriers to increased Internet connectivity in developing countries, mostly relating to lack of technical infrastructure, high cost, and accessibility. High levels of public and private investment are required to create a working wired Internet system, the political and economic conditions for which are not commonly present. For example, with few submarine cables leading to African countries in general, creating fixed connectivity is expensive, perhaps prohibitively so for the poorest States.[140] This helps explain why the wired broadband access in Zambia

[136] *See* "India", *supra* note 123 and accompanying text (Table 2: Fixed & Mobile Broadband Internet Access); Stanford Study, *supra* note 23, at 3.

[137] *See* Mozilla Report, *supra* note 23, at 5.

[138] *See* Stanford Study, *supra* note 23, at 5; "The 2015-16 Affordability Report", Alliance for an Affordable Internet, available at: http://bit.ly/1TA2JO3 [https://perma.cc/3Z3H-9N43]; Schumann, Robert and Kende, Michael, "Lifting Barriers to Internet Development in Africa: suggestions for improving connectivity", Report for the Internet Society (ISOC), May 8, 2013, available at: http://bit.ly/1MRw17S [https://perma.cc/AU5F-5GKC] [hereinafter Internet Society, "Lifting Barriers"].

[139] Stanford Study, *supra* note 23, at 5; Mozilla Report, *supra* note 23, at 6.

[140] Internet Society, "Lifting Barriers", *supra* note 137, at 7.

is less than 1 percent of the population; even in South Africa, the richest country in Sub-Saharan Africa, barely above 3 percent of the population is connected in this way.[141] This is due to the fact that large numbers of the rural population live a long distance from the closest node on a fiber network.[142] And while a recent increase in submarine cables has helped with the spread of the Internet in some parts of the African continent, landlocked countries are now forced to rely on a stake in a cable landing station in a neighboring country.[143] In short, "there is significant evidence that there are insufficient cross-border terrestrial connections in Africa, and that those available are not fully exploited."[144]

Other regions of the world face similar challenges, keeping fixed Internet access at low, even negligible levels. In India, less than 2 percent of the population enjoys wired access; in Malaysia and Colombia, that figure barely exceeds 10 percent; by contrast, wired subscriptions in developed countries surveyed above was closer to a third, on average.[145] Part of the problem for developing countries resides in extending connectivity to rural areas, which can be vast. In China, 63% of the offline population is rural.[146] In India, approximately 45% of the rural population lives without electricity.[147] Even where it is available, wired broadband access may be too expensive. A monthly broadband subscription costs about 60 dollars in Australia and Mozambique.[148] However, the average yearly gross income in Australia is 50,000 US Dollars; in Mozambique, it is less than 500. A broadband plan with a speed of 25 to 50 Mbps in Mexico City was 123.73 US Dollars on average in 2014, while in Amsterdam it was only 43.53 US Dollars.[149] Yet Mexico has a GDP per capita of 10,325.6 and the Netherlands has one of 52,172.2. And these figures obviously do not include the related expenses associated with wired access of purchasing an Internet-enabled device,

[141] *See supra* note 120 and accompanying text (Table 2: Fixed & Mobile Broadband Internet Access).

[142] Internet Society, "Lifting Barriers", *supra* note 137, at 8.

[143] *Id.* at 5-7.

[144] *Id.* at 7.

[145] *See supra* note 120 and accompanying text (Table 2: Fixed & Mobile Broadband Internet Access).

[146] *Id*.

[147] Internet Society, "Lifting Barriers", *supra* note 137, at 23.

[148] Graham, Mark, "Broadband Affordability", Geonet Project, September 7, 2014. Available at: http://bit.ly/2eNGx5R [https://perma.cc/SP6C-R27W].

[149] Russo, Nick, Morgus, Robert, et. al, "The Cost of Connectivity 2014", Open Technology Institute, New America, October 30, 2014. Available at: http://bit.ly/1Zw03AV. [https://perma.cc/T4T3-VYR3].

such as a personal computer or tablet. For these reasons, wired broadband penetration is low to negligible in many developing countries, where it is generally reserved for the urban and economic elites.[150]

The pervasive lack of physical infrastructure, plus the expense of getting wired access where it exists, increasingly leads people in developing countries to use mobile phones to access the Internet.[151] But there are significant obstacles to mobile access too. "On the infrastructure side, despite clear gains in coverage in recent years [. . .] a number of people continue to lack access: 10% of the global population lack access to basic voice and text services, and roughly 30% lack access to 3G/4G mobile broadband internet. Pertinently, the vast majority of these uncovered populations are low income and live in the rural regions of Asia and Sub Saharan Africa."[152] Cost continues to be another important barrier.[153] Even where mobile access is more available than fixed broadband, it is still expensive compared to local incomes.[154]

On average, mobile broadband costs in developing countries are twice as much as those in developed countries.[155] In developing countries, people can pay "between 8–12 percent of their average monthly income on mobile connectivity, and that is often just for voice and text."[156] In Zimbabwe or the Democratic Republic of Congo, for example, the average data plan is equivalent to 100% of the country's monthly GNI.[157] Similarly, in a place

[150] Mozilla Report, *supra* note 23, at 5-6.

[151] Mozilla Report, *supra* note 23, at 5-6; Internet Society, "Global Internet Report 2015: Mobile Evolution and the Development of the Internet", 2015, available at: http://bit.ly/2g2xtX5 [https://perma.cc/BT48-N9Y2]; McKinsey & Company, "Offline and Falling Behind: Barriers to Internet Adoption", 2014. Available at: http://bit.ly/29n9kb7 [https://perma.cc/2HMW-R4AW]. While just one quarter of users in developed countries access the Internet primarily through a mobile phone, in countries like Egypt and India the number is much higher at 70% and 59% respectively. *Id.*

[152] Mozilla Report, *supra* note 23, at 6.

[153] *See Id*. Lack of infrastructure, and even electricity outages, can impair cellular coverage; West, Darrell, *supra* note 49, at 3-4. Also, not all connections are of the same quality. While 94% of the rural population in the Netherlands is covered by at least a 3G mobile network, only 1% is covered in Zambia; International Telecommunication Union (ITU), "Measuring the Information Society Report", 2014, available at: http://bit.ly/1NUbnkf [https://perma.cc/4GY6-RFPH].

[154] Carew, Diana G., "Zero-Rating: Kick-Starting Internet Ecosystems in Developing Countries", Progressive Policy Institute, March 3, 2015. Available at: http://bit.ly/2fbApTJ [https://perma.cc/A73F-5YND].

[155] International Telecommunication Union (ITU), "ICT Facts and Figures", 2015. Available at: http://bit.ly/1QTSz61 [https://perma.cc/NP3B-T4XH].

[156] Carew, Diana, *supra* note 153.

[157] Mahapatra, Lisa, "Data Plans: Developed Countries Have the Most Affordable Mobile Broadband Plans", *International Business Times*, October 11, 2013. Available at: http://

like India, the average person would need to work 17 hours to afford a 500MB mobile data plan, in comparison to the three hours of minimum wage it would take in the United States to get unlimited data for a month.[158] In Zambia, the 500MB mobile data plan will cost 200 times what a gallon of milk would cost on average.[159] Compare this to the Netherlands, where a bundle of 500MB and unlimited calls and texts will cost 25 Euros per month and the minimum wage for a 36-40 hour workweek is 351.85 euros.[160]

In sum, in the context of both wired broadband and mobile phone Internet access, high cost is major obstacle for most consumers in the developing world. In the case of mobile access, it is arguably the primary one. Most people do not have the resources to afford an expensive data plan and pay the fees attached to accessing the Internet on a basic or feature phone, much less a pricey smartphone.[161] Fortunately, smartphones are rapidly becoming more affordable, and there is little doubt that they represent the future of mobile connectivity in the developing world.[162] What may be most surprising, however, is that even when people do have access to an Internet connection, they may choose not to use it, or be incapable of doing so. These are the soft barriers to access.

The lack of literacy in different forms is a roadblock to many users. Users who lack digital literacy, for example, may experience "unfamiliarity with or discomfort in using digital technologies to access and use information."[163] But if a potential user is also unable to read and write, connecting to the Internet will be that much more difficult.[164] Literacy rates in this regard tend to be lower—though not always substantially so—in the developing countries surveyed than the developed ones.[165] Another barrier is relevance: people are less likely to connect to the Internet if they do not see or understand

bit.ly/2g5qDBM [https://perma.cc/JM7T-6JFF].

[158] Eagle, Nathan, "How to Make the Internet Free in Developing Countries", *Tech Crunch*, June 1, 2015. Available at: http://tcrn.ch/2g3ZjDn [https://perma.cc/NEM4-TXW4].

[159] *See infra* notes 169-201.

[160] Government of the Netherlands, *Amount of the minimum wage*. Available at: http://bit.ly/2fMeBMN [https://perma.cc/B3R6-ZAEU]; Lycamobile, Bundle Offers, http://bit.ly/2bpKqeX [https://perma.cc/5DGD-JZNW].

[161] West, Darrell, *supra* note 49, at 2.

[162] *See* Mozilla Report, *supra* note 23, at 6-11.

[163] McKinsey & Company, *supra* note 150, at 4.

[164] *Id*.

[165] *See supra* Table 3 note 124. While some technologies, such as text-to-speech or voice recognition can facilitate the navigation even for illiterate users, most users who do not have the basic level of language proficiency necessary will find it difficult to engage with the Internet in a meaningful way. McKinsey & Company, *supra* note 150, at 42.

its usefulness to them. This arises, for instance, where there is insufficient content that appeals to them or relates to their day-to-day life.[166] Additionally, businesses in developing countries with low levels of mobile connectivity have few incentives to invest in providing online services precisely because there are so few Internet-accessing customers.[167] These factors combine to form a status quo of "low connectivity equilibrium" which can be difficult to overcome.[168] The proliferation in developing countries of mobile phone users in general, and smartphone users in particular, will not be as effective in closing digital divides as it could be, unless it is coupled with relevant local content offerings, and digital literacy programs aimed at new subscribers.[169]

I.B.III. Three Approaches to Zero-rating

The foregoing discussion uses quantitative data to illustrate the different contexts in which net neutrality policies and zero-rating practices take place around the world. In this sub-section we focus specifically on three of the countries examined above, each reflecting a different approach to zero-rating. The countries are Zambia, Chile, and the United States. Each country study integrates the economically, politically and technologically relevant data from the preceding sub-section with additional information about how net neutrality in general, and zero-rating in particular, have been addressed.

I.B.III.A. Zambia

One example of a developing nation that embraces zero-rating is Zambia. Zambia is a Southern African nation with a weak democratic system. It is a presidential republic, but through much of its independent history, Zambia has been controlled by a single political party, the United National Independence Party (UNIP). Zambia went through a period of decentralization in the early 1990s and has been undergoing economic reforms since the early 2010s.[170] The political climate in Zambia, however, is not fully

[166] West, Darrell, *supra* note 49, at 5; Internet.org, "State of Connectivity: 2014. A Report on Global Internet Access", 2014, available at: http://bit.ly/1EE9B0E [https://perma.cc/7H36-MALH]. Obviously, if access is not available in local languages, that too will further discourage access.

[167] Carew, Diana, *supra* note 153, at 3.

[168] *Id*.

[169] Mozilla Report, *supra* note 23, at 34-35.

[170] "Zambia among world's fastest growing economies—World Bank", *Lusaka Voice*, April 16, 2013. Available at: http://bit.ly/2g2AS8a [https://perma.cc/WU4R-ZSXL].

free according to Freedom House's 2016 Freedom in the World Report.[171]

As far as human development is concerned, Zambia is lagging, despite a significant increase in its Human Development Index (HDI) ranking from 2012 to 2013. As noted above in Part I.B (Table 3), in 2013 Zambia was in the bottom of the medium development range with a ranking of 141 out of 187 nations by HDI.[172] In 2012, however, it had ranked 163 with a lower HDI score than the average for "low development" countries, as well as for the sub-Saharan nations.[173] In any event, the country's GDP per capita is the lowest of any of the States surveyed;[174] for this reason, among others, the United Nations continues to list Zambia as one of the world's 48 "least-developed" countries as of 2014.[175]

Zambia allows for zero-rating: it was the first country in which Facebook rolled out Internet.org in July 2014.[176] The country apparently does not yet have a concrete legal or policy framework when it comes to net neutrality.[177] In general, net neutrality is not (yet) regulated in many African countries.[178] The Internet Service Providers' Association has stated that net neutrality is a "non-issue" in countries like South Africa.[179] Some argue that net neutrality laws address the quality of access and that only becomes relevant when there is a larger quantity of access.[180] They state this as the reason that net neutrality laws have not spread further throughout Africa.[181] While opponents of tighter net neutrality regulation in African countries do concede that zero-rating will

[171] Freedom House, "Freedom in the World 2016, Country Report: Zambia". Available at: http://bit.ly/2eNZrtf [https://perma.cc/DA8C-MJSV].

[172] *See supra* note 127 and accompanying text.

[173] United Nations Development Programme (UNDP), *The Rise of the South: Human Progress in a Diverse World. Zambia Country Profile*, 2013. Available at: http://bit.ly/2fbJN9L [https://perma.cc/MNY7-BNCS].

[174] *See supra* note 125 and accompanying text.

[175] *See supra* notes 125-129 and accompanying text (discussing the United Nations current LDC criteria and list).

[176] Rosen, *supra* note 78.

[177] *See* Freedom House, "Freedom on the Net 2015: Zambia". Available at: http://bit.ly/2fMtf6B [https://perma.cc/R396-WTAJ] (detailing legal framework that applies to Internet regulation in Zambia, with no mention of net neutrality norms).

[178] van Zyl, Gareth, "Is Net Neutrality a "Non-Issue" in Africa?", IT Web Africa. Available at: http://bit.ly/1kQZG45 [https://perma.cc/VWL4-TZYD].

[179] Internet Service Providers' Association (ISPA)," 'Net Neutrality' a Non-Issue in South Africa for the Present, Says ISPA", August 11, 2014. Available at: http://bit.ly/2g4dKYm [https://perma.cc/J4XD-AZGD].

[180] Song, Steve, "Net Neutrality in Africa", Many Possibilities, May 7, 2014. Available at: http://bit.ly/2g3Sbcl [https://perma.cc/6JR2-RL3H].

[181] *Id*.

make it harder for startups and easier for big names to dominate the market, they believe that "bad access trumps no access every single day of the week."[182]

Internet.org operates in Zambia through Airtel, a private telecommunications provider.[183] In addition to services such as Facebook, Messenger, AccuWeather, Google Search, and Wikipedia, Internet.org gives Zambians access to UNICEF's website for health and nutrition, including info on HIV/AIDS (Zambia uReport); other applications include a sports website, an independent news service, and a women's rights app.[184] Wikimedia Zero currently does not operate in Zambia.[185] The arrival of Internet.org is significant because, historically, Zambia has had low Internet penetration rates. Between 2010 and 2014, Zambia increased Internet user percentage by over 50 percent, but that brought the total up to only 15.4 percent of the population.[186] By some accounts it has reached as high as 17 percent.[187] In its territory, Zambia only has four secure servers per one million people.[188] As of 2010, only 1.3 percent of the population has Internet access at home, and less than 4 percent have a computer at home.[189] However, over 50 percent of households have a mobile-cellular telephone.[190] For these reasons, Zambia ranks 144 out of 166 countries ranked in the International Telecommunication Union's Information and Communications Technology Development Index.[191]

Although Zambia's telecommunications sector is limited, it is in a period of growth. It has had a single privately owned ISP since the 1990s, but other private companies are starting.[192] Moreover, the telecommunications regula-

---

[182] *Id*.

[183] *Id.*; Bloomberg, "Company Overview of Airtel Networks Zambia Plc". Available at: http://bloom.bg/2f7Seji.

[184] Honan, Mat, "Facebook-Backed Non Profit Brings Free Internet to Zambia", *Wired*, July 31, 2014. Available at: http://bit.ly/2fbP8hw [https://perma.cc/MZL7-C2G7]; *see also* Rosen, *supra* note 78.

[185] *See* Wikimedia Foundation, "Mobile Partnerships". Available at: http://bit.ly/28Wok2H [https://perma.cc/NYS9-CX8J].

[186] "Internet Users", *supra* note 123.

[187] "Freedom on the Net 2015", *supra* note 176.

[188] The World Bank, "Secure Internet Servers (per 1 million people)". Available at: http://bit.ly/2gnMfMj [https://perma.cc/GH96-L85L]. Pew Research Center, "Emerging Nations Embrace Internet, Mobile Technology", February 13, 2014. Available at: http://pewrsr.ch/1mg8Nvc [https://perma.cc/K7PQ-WYVU].

[189] ITU, *supra* note 121.

[190] *Id*.

[191] International Telecommunication Union (ITU), "MIS 2014 Report Charts". Available at: http://bit.ly/2foCDNe [https://perma.cc/HGG6-LDD7].

[192] Price Waterhouse Cooper, "Zambia Telecommunications". Available at: http://pwc.to/2fozM70 [https://perma.cc/4K2X-TEE3].

tor, the Zambia Information and Communications Technology Authority, is nominally independent.[193] Its mission includes regulation, monitoring, standard setting, and promoting competition in the telecommunications sector.[194] One of its strategic goals is to promote universal access in the population.[195] Unfortunately, Zambia is one of the most corrupt of the countries surveyed, tied with India and only marginally better than Colombia.[196] Overall, Transparency International ranks it 85 out of 175 countries in the world.[197]

There are two main obstacles to increased Internet connectivity in Zambia: the first is economic, and the second relates to infrastructure. As Zambia is a Least Developed Country (LDC), national incomes are very low, and it is difficult for individuals to spend money on Internet access rather than other pressing necessities. For instance, while a gallon of milk in Zambia will cost the equivalent of about 4.6 US Dollars, a mobile Internet data bundle of 500MB for 30 days will cost approximately 20 US Dollars.[198] Additionally, Zambia has a high tax burden on Internet access—the ratio of tax payments to mobile operator revenue is a high 53 percent.[199] Infrastructure limitations also hinder increased access. Since Zambia is a landlocked nation, it does not have access to submarine cables, which can increase competition and bring down prices.[200] In order to get access to these cables, Zambia would have to rely on coastal neighbors, which is not feasible in all situations.[201]

I.B.III.B. Chile

Chile was the first nation in the world to adopt a net neutrality law in 2010.[202] It is a South American country with a strong democratic system based on popular elections and a multi-party political system. It operates

[193] *Id*.

[194] Zambia Information and Communication Technology Authority, http://bit.ly/1j0n1PX [https://perma.cc/DL7F-E23D].

[195] *Id*.

[196] *See supra* Table 4.

[197] Transparency International, *supra* note 131; *see supra* Table 4.

[198] Numbeo, "Cost of Living in Zambia", available at: http://bit.ly/2g3UNam [https://perma.cc/QQN8-L43B]; *see also* GitHub Gist, "MTN Zambia Mobile Internet Data Sheet", available at: http://bit.ly/2g422z5 [https://perma.cc/47G4-FX8Z].

[199] McKinsey & Company, *supra* note 150, at 41.

[200] *Id*. at 47.

[201] *Id*.

[202] Walker, Lauren, "How Is Net Neutrality Working for the Countries That Have It?", *Newsweek*, September 10, 2014. Available at: http://bit.ly/1IWlkov [https://perma.cc/NA93-UNNN].

on a presidential system with laws enacted by congress and implemented by the president. Freedom House scores Chile as "Free" with top scores in both Civil Liberties and Political Rights,[203] whereas Press Freedom is categorized as only "partly free" based in part on a lack of competition in the media market.[204] Corruption levels are relatively low, especially by regional standards. Transparency International (TI) ranks it 21 out of 175 countries in terms of corruption, tied with Uruguay for the lowest levels in South America.[205] Despite middle of the road GDP per capita, Chile ranks high overall in human development. According to the UNDP, it is 41 out of 187 nations and has the highest human development in South America.[206]

As far as economic development, the United Nations classifies Chile as a developing economy with high income (advancing from upper middle income status in 2014).[207] Chile became a member of the Organization of Economic Cooperation (OECD) in 2010—the organization's first member in South America.[208] However, Chile also has high inequality, as evidenced by The World Bank scoring Chile at 50.8 in terms of GINI (where 0 is perfect equality and 100 is perfect inequality).[209]

As noted, Chile was the first nation in the world to adopt a net neutrality law in 2010,[210] which bans most kinds of zero-rating. At a normative level, the provisions established by the law create a "blanket" bar to practices that violate net neutrality.[211] Chile's net neutrality laws state that ISPs will not be

[203] Freedom House, "Freedom in the World, Country Report: Chile", 2014. Available at: http://bit.ly/2foB5Tm [https://perma.cc/7KZU-LDGA].

[204] Freedom House, "Freedom of the Press, Country Report: Chile", 2014. Available at: http://bit.ly/2gnPTpz

[205] Transparency International, *supra* note 131; *see supra* Table 2.

[206] United Nations Development Programme, *Chile: Human Development Indicators*, available at: http://bit.ly/1PtNyFq [https://perma.cc/57R6-XVKZ]; *see* United Nations Development Programme, *International Human Development Indicators*, http://bit.ly/1rAOGrY [https://perma.cc/PNT6-5NSX] (map showing Argentina as next ranked nation in South America at number 49).

[207] United Nations, *Country Classification*. Available at*:* http://bit.ly/1VctxnS [https://perma.cc/BK9C-5EAY].

208Organisation for Economic Co-operation and Development (OECD), "Members and Partners", available at: http://bit.ly/1fxLB6q [https://perma.cc/MR8F-EQ6M]; OECD, "Chile Signs up as First OECD Member in South America", November 1, 2010, available at: http://bit.ly/2g42bCR [https://perma.cc/HWS9-2EKW].

[209] The World Bank, *supra* note 126.

[210] Ley Nº 20.453, Principio de Neutralidad en la Red Para Los Consumidores y Usuarios de Internet, General de Telecomunicaciones, August 26, 2010, Available at: http://bit.ly/1msnmfa [https://perma.cc/M2P2-UA29]; Walker, Lauren, *supra* note 201.

[211] Subsecretaría de Telecomunicaciones, Circular 40 (Chile), Available at: http://bit.

able to "arbitrarily block, interfere, discriminate, hinder or restrict content, applications or legal services that users perform in their networks."[212] Initially, the law's prohibition on discrimination was applied to commonly zero-rated social media applications like Twitter, WhatsApp and Facebook.[213] In 2014, the *Subsecretería de Telecomunicaciones de Chile* (Subtel), the telecommunications regulator, announced that such services were no longer allowed, subjecting any company that utilized them to fines.[214] Internet.org was similarly shut down.[215] While net neutrality activists were pleased by Chile's approach, others called the practice shortsighted.[216] Citing Chile's high rate of mobile phone usage and relatively low wired and mobile internet usage, opponents argue that the Chilean plan lacked "nuance" and would hamper the growth of Internet access in the country.[217]

In practice, however, Chile's net neutrality law today only bans zero-rating by mobile operators of social media apps and services offered as promotional or commercial schemes.[218] Some forms of zero-rating continue to exist or be permitted by Subtel, including zero-rated social media platforms.[219] Notably, Subtel issued an opinion stating that Wikipedia Zero did not violate the terms of the law, or Subtel's interpretations of its net neutrality protections.[220]

Unlike most other developing countries, Chile has significant Internet penetration. As of 2013, over 66 percent of the country has Internet access, and it has 94 secure servers per 1 million people.[221] Nearly 70 percent of the population accesses the Internet daily,[222] confirming that Chile faces

---

ly/2g5Sodt [https://perma.cc/JYB8-M9C7]; Walker, Laurel, *supra* note 201.

[212] Global Voices, "Chile: First Country to Legislate Net Neutrality", September 4, 2010. Available at: http://bit.ly/2eOhKPf [https://perma.cc/3X4N-U8VF].

[213] Moody, Glyn, "Chile Bans Free Delivery of Social Media Services to Uphold Net Neutrality", *Techdirt*, June 16, 2014, available at: http://bit.ly/1DkxFGK [https://perma.cc/639J-QYEP]; Subsecretaría de Telecomunicaciones Colombia, *Ley de Neutralidad y Redes Sociales Gratis*, May 27, 2014, available at: http://bit.ly/1OfZ29Z [https://perma.cc/KC62-2V4C].

[214] Meyer, David, "*In Chile, Mobile Carriers Can No Longer Offer Free Twitter, Facebook or WhatsApp"*, Gigaom, May 28, 2014. Available at: http://bit.ly/2fDszCY

[215] Rossini Public Knowledge Repaort, *supra* note 23, at 17-18.

[216] Mirani, Leo, "When Net Neutrality Backfires: Chile Just Killed Free Access to Wikipedia and Facebook", *Quartz*, May 30, 2014. Available at: http://bit.ly/1mQGZem [https://perma.cc/A7FE-SHFG].

[217] *Id*.

[218] Rossini Public Knowledge Report, *supra* note 23, at 19-20.

[219] *Id. See, e.g.*, Claro Chile, http://bit.ly/1PDuP4J [https://perma.cc/G6TB-GG7A].

[220] *Id.*

[221] "Internet users", *supra* note 123; The World Bank, *supra* note 187

[222] "Emerging Nations", *supra* note 187.

relatively few specific barriers to Internet connectivity. As of 2011, over 40 percent of households had Internet access in their homes.[223] The country's infrastructure suffered a hit from the February 2010 earthquake, but combined public and private efforts have invested in rebuilding.[224] Although over 90 percent of Chileans own a cell phone, only 39 percent own a smartphone.[225] However, 55 percent of 18 to 29 year old Chileans have a smartphone, suggesting the breakdown is generational.[226] Finally, the telecommunications sector in Chile is privatized.[227] As we have seen, Subtel regulates the industry, including issuing licenses and promulgating standards.[228]

I.B.III.C. United States

The United States ranks as a free democratic country and the world's largest economy. Recent revelations regarding mass government surveillance have raised concerns regarding privacy and Internet freedom.[229] Corruption is relatively low (the country comes in seventeenth out of 175 nations according to TI).[230] According to the Human Development Report, the United States is a developed nation. It has high human development, ranking fifth of 166 nations.[231] Moreover, the United States has the highest human development score in the Americas.[232]

The United States does not prohibit zero-rating, but a pro-net neutrality bias requires that such practices be reviewed to safeguard against potentially unfair or harmful consequences.[233] In its 2015 Open Internet Order, the FCC

[223] International Telecommunication Union (ITU), "Core Indicators on Access to and Use of ICT by Households and Individuals (Excel)". Available at: http://bit.ly/1cblxxY [https://perma.cc/5CLS-DKKH] [hereinafter Core Indicators].

[224] *Id*.

[225] "Emerging Nations", *supra* note 187.

[226] *Id*.

[227] Rossini Public Knowledge Report, *supra* note 23, at 15-20 (describing Chile's regulation of the private telecom companies in that country).

[228] *Id*.

[229] Freedom House, "Freedom on the Net: United States", 2014. Available at: http://bit.ly/2eOi2FN [https://perma.cc/ML68-24RG].

[230] Transparency International, *supra* note 131; *see supra* Table 2.

[231] United Nations Development Programme, *United States: Human Development Indicators, Human Development Reports*. Available at: http://bit.ly/1N0VQnb [https://perma.cc/LFN4-ZNTB].

[232] *See supra* Table 3.

[233] *See* Carrillo, Arturo J. and Nunziato, Dawn C., "The Price of Paid Prioritization: The International and Domestic Consequences of the Failure to Protect Net Neutrality in the United States" on *Georgetown Journal of International Affairs*, Cyber V, 98, Summer 2015.

adopted a framework for regulating the Internet that is strongly protective of net neutrality in several respects.[234] First, the FCC defined the scope of its new Rules as applying to "both fixed and mobile broadband Internet access service."[235] Second, the FCC enacted three bright-line rules that go to the heart of net neutrality protections: no blocking;[236] no throttling;[237] and no paid prioritization.[238] Finally, the FCC devised a way to reach other types of conduct that may not come under the bright-line rules by establishing its "no unreasonable interference/disadvantage standard."[239] Under this rule, ISPs cannot unreasonably interfere with or disadvantage either end users' ability to use and access broadband service or Internet content or edge providers' ability to make such content available to end users.[240] In other words, the FCC decided that it would not apply a bright line rule to flatly prohibit sponsored data or "zero-rating" plans, but would instead evaluate these on a case-by-case basis under the "no unreasonable interference/ disadvantage standard."[241]

Internet penetration is high across the United States, ranging from metropolitan to rural areas. In 2014, the US far outranked all other countries examined by

[234] White House, *Net Neutrality: President Obama's Plan for a Free and Open Internet*. Available at: http://bit.ly/1xdiOy6 [https://perma.cc/XCJ6-AN3W].

[235] 2015 Open Internet Order, *supra* note 1, at ¶ 25.

[236] *Id.* ¶ 112. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not block lawful content, applications, services, or nonharmful devices, subject to reasonable network management."

[237] *Id.* ¶ 119. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not impair or degrade unlawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management."

[238] *Id.* ¶ 125. "A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not engage in paid prioritization. 'Paid prioritization' refers to the management of a broadband network provider's network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either (a) in exchange for consideration (monetary or otherwise from a third party), or (b) to benefit an affiliated entity."

[239] *Id.* ¶ 136. "Any person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not unreasonably interfere with or unreasonably disadvantage (i) end users' ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of their choice, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users. Reasonable network management shall not be considered a violation of this rule."

[240] 2015 Open Internet Order, *supra* note 1, at ¶ 136.

[241] *Id.* ¶ 152.

the OECD in Internet coverage, with a total of 100,192,000 fixed and wireless broadband subscriptions.[242] Regarding subscriptions per 100 people it came in sixteenth, with Korea and New Zealand being the only non-European countries to have a higher number of fixed and wireless subscriptions.[243] Eighty-four percent of the country has access, with 68 percent of adults accessing through mobile connections and 70 percent of households having high-speed broadband.[244] Currently, the access and scope of zero-rated services depend on different private mobile carrier options. T-Mobile, for instance, exempts specific music apps for zero-rating under some of its data plans, but not others.[245]

I.C. Concluding Observations

In this second Part, I reviewed the different types of private sector zero-rating practices and organized them into four basic categories: single-site; compound; sponsored data; and faux/non-selective. I presented empirical data relating to Internet access, net neutrality and zero-rating around the world, as well as the specific socio-economic and political contexts in which those issues exist. This included a survey of the various barriers to connectivity, especially the high costs associated with Internet access in the developing world, which is an essential piece of the zero-rating puzzle. And, by viewing all this data through the lens of three representative case studies, I hope to have conveyed a better sense of the primary approaches considered or adopted by countries around the world as they attempt to regulate net neutrality and zero-rating. Now we are ready to turn to the international law framework.

II. "New" Perspective: The International Law Framework

As important as it is to maintaining an open and free Internet, the principle of net neutrality is much more than that. Today, it is a well-established rule of international human rights law, an essential element of the rights to freedom of expression and non-discrimination online. But, how did it become so? No

[242] Organisation for Economic Co-operation and Development, "Broadband Portal", July 23, 2015. Available at: http://bit.ly/1cP4RGV [https://perma.cc/JK4G-9F5V].

[243] *Id*.

[244] Freedom House, *supra* note 228.

[245] Molen, Brad, "On T-Mobile, You Can Now Stream Music Without Hurting Your Data Plan", *Engadget*, June 18, 2015. Available at: http://engt.co/2g369lf [https://perma.cc/V5GG-BLFJ]; *see also*, *supra* notes 59 - 61 and accompanying text.

human rights treaty mentions the term "net neutrality," which was famously coined by U.S. law professor Tim Wu only in 2003.[246] More to the point: why does it matter? What is significant about the evolution of net neutrality from a U.S.-based normative principle and proposed policy priority, to a human rights rule binding on States? Why should – indeed, must – defenders and critics of net neutrality alike understand the human rights implications of that rule today? Those are the questions to be addressed here, among others.

In this Part, I trace the evolution of net neutrality as a human rights norm before situating it within the legal frameworks for analyzing such rights. It is divided into three sections. In the first, I respond to the question, "How did net neutrality become a norm of international human rights law?" This initial section looks at how net neutrality rose to become an integral part of freedom of expression, which is defined as the rights to impart, seek and receive information, on the one hand, and the right to Internet access or "connectivity" on the other. The second section outlines the contemporary legal frameworks involved, including non-discrimination norms and their effect on freedom of expression rights as applied. It also sets out the exceptions regime established in human rights law for determining when restrictions on fundamental rights by States are permitted. In the third and final section, I answer the question of why it is important, if not necessary, that we treat net neutrality as what it undisputedly has become: a multi-faceted norm of modern human rights law.

II.A. How Net Neutrality Became a Norm of International Human Rights Law

Net neutrality did not begin as a human right. Decades ago, the concept of an "open" or data neutral network was built into the nascent Internet by design.[247] This "openness" encompassed not just engineering in terms of software and standards, but also the liberal values of free speech and egalitarianism derived from the milieu in which the Internet was created.[248] The

[246] Wu, Tim, "Network Neutrality, Broadband Discrimination", on Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003. Available at: http://bit.ly/2fMR9yV

[247] Goldsmith, Jack and Wu, Tim, "Who controls the internet?: Illusions of a Borderless World", Oxford University Press, 2006.

[248] Lemley, Mark A. and Lessig, Lawrence, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era", on UCLA Law Review, Vol. 48, p. 925, October 1, 2000, available at: http://bit.ly/2g4fzql; *see also* Goldsmith & Wu, *supra* note 246, at 19.

"open Internet" was meant to guarantee the free, unregulated flow of information from "end-to-end," that is, without substantial interference during the transmission of data from one "intelligent" user to another, over the "dumb" pipes or physical network.[249] "One consequence of this design is a principle of non-discrimination among applications."[250] Another consequence was the meteoric growth and success of the Internet as a communications network.[251] Not surprisingly, early activists heralded the Internet as a great liberating force, not least because "cyberspace" was viewed as inherently free of the types of territorial boundaries, government regulation and economic control that plagued other communications systems.[252] It has since become abundantly clear that this is no longer the case, if it ever was.[253]

Though the concept was already present, the term net neutrality did not exist in discussion of Internet policy until 2003. It was born in the midst of a debate raging in the United States over how to best ensure "open access" to the Internet through regulation in light of the advances in broadband services at the turn of the century.[254] The concern was that allowing the integration of ISP and content provider services by cable companies would lead to a disruption of the "end-to-end" principle that, as just noted, had proven indispensable to the extraordinary growth of the Internet.[255] While promoters of "open access" proposed structural remedies aimed at preserving the Internet's natural architecture (i.e. prohibiting the proposed mergers),[256] Tim Wu proposed instead the adoption of a policy directive—net neutrality—that was the "concrete expression of a system of belief about innovation."[257] In so doing, he gave a proper name to the non-discriminatory character of the "end-to-end" principle at the core of the "open" Internet. In other words,

[249] *Id*, Lemley and Lessig, at 930-31. On the unregulated nature of the early Internet; *see also* Lawrence Lessig, Code: *Version 2.0,* New York, Basic Books, 2006. [hereinafter Lessig, Code].

[250] Lemley & Lessig, *supra* note 247, at 931.

[251] *Id*.

[252] Goldsmith & Wu, *supra* note 246, at 17-21.

[253] *See* Lessig, Code, *supra* note 248; Goldsmith & Wu, *supra* note 246; *see generally* Morozov, Evgeny, *The Net Delusion: The Dark Side of Internet Freedom*, New York, PublicAffairs, 2012.

[254] *See* Lemley & Lessig, *supra* note 247; Wu, *supra* note 245.

[255] Lemley & Lessig, *supra* note 247.

[256] *Id*.

[257] Wu, *supra* note 245, at 145. By prohibiting discrimination in the provision of broadband services and content, regulators could ensure that the competitive "playing field" remained level or "meritocratic" for application developers wanting to access those networks, regardless of who controlled them.

Wu sought to shift the terms of the U.S. debate about how best to preserve the virtues of the "open" Internet away from a discussion of the need for structural remedies towards one focused on normative policy-making and the pro-competition principle of net-neutrality.[258] He succeeded.[259]

It is unlikely that the academic proponents of net neutrality principles in the United States during the decade of the 2000s could have foreseen the international impact of their creation. Yet by 2015, the concept of a data-neutral network based on the "end-to-end" principle, as well as the term net neutrality itself, had been largely "uploaded' into human rights law and discourse.[260] Relative to the formation of international law generally, this evolution occurred in the blink of an eye. Essential to framing this process were definitive statements by the United Nations' primary human rights bodies confirming the convergence of human rights and the digital realm. Most notably, the United Nations Human Rights Council in June 2012 adopted its landmark resolution on "The promotion, protection and enjoyment of human rights and the Internet," in which it established that "the same rights that people have *offline* must also be protected *online*, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[261] A year before, in September 2011, the UN Human Rights Committee issued an updated General Comment on ICCPR Article

[258] At the time, Wu was less concerned with the preserving the architectural purity of the open Internet than he was promoting a form of "Darwinian competition" in which "only the best survive." Wu, *supra* note 245, at 142.

[259] No need to look further for evidence of this than the FCC's 2015 Open Internet Order adopting precisely the type of net neutrality principle posited by Wu in 2003. *See* 2015 Open Internet Order, *supra* note 1.

[260] *See, e.g.*, Belli, Luca, "End-to-End, Net Neutrality and Human Rights", on *Net Neutrality Compendium: Human Rights, Free Competition ant the Future of the Internet,* Springer International Publishing, 2015, p. 22-23. Available at: http://bit.ly/2fMWYfD.

[261] U.N. Human Rights Council, *The Promotion, Protection, and Enjoyment of Human Rights on the Internet,* ¶ 1, U.N. Doc. A/HRC/20/L.13, June 29, 2012, available at: http://bit.ly/2g667kw [https://perma.cc/BFA4-RQLJ] (emphasis added). In a prior resolution from 2011, the HRC had already made reference to the importance of safeguarding the freedom of expression rights of journalist and media workers on the Internet as part of a more general statement about media freedoms. U.N. Human Rights Council, *Information and Communications Technologies for Development*, U.N. Doc. A/RES/66/184, December 22, 2011. At the same time, Internet governance and the importance of digital technologies for development has long been a subject of attention in the United Nations, which spearheaded the WSIS process and sponsored regular Internet Governance Forums. *See, e.g.*, U.N. Human Rights Council, *Freedom of Opinion and Expression*, U.N. Doc. A/HRC/RES/12/16, October 2, 2009.

19 in which it expressly established that the Covenant's protections were equally in force for all "Internet-based modes of expression."[262] While the Human Rights Council's resolution in itself does not possess any normative force, it is hugely significant as a unanimous decision by the UN's premier human rights institution not just to recognize this convergence, but to urge it forward as well. Though not as high profile as the Council's resolution, the Human Rights Committee's revised General Comment 34 is arguably the weightier statement, because it is imbued with legal force.[263]

Yet neither the Human Rights Council's resolution nor the Human Rights Committee's General Comment mentions net neutrality *per se.* The first official recognition of net neutrality's incorporation into international human rights law was the June 2011 Joint Declaration on Freedom of Expression and the Internet issued by the United Nations Special Rapporteur on Freedom of Opinion and Expression; the Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media; the Organization of American States (OAS) Special Rapporteur on Freedom of Expression; and the African Commission on Peoples and Human Rights' Special Rapporteur on Freedom of Expression and Access to Information [hereinafter "Joint Declaration"].[264] Among the principles set out in the Declaration is the terse imperative that "[t]here should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application."[265] No rationale is given to explain how or why this principle was now a norm of human rights on the Internet.[266] A more fulsome discussion of net neutrality's

[262] U.N. Human Rights Committee, General Comment No. 34, ¶¶ 12, 15, 39, 43, & 44, U.N. Doc. CCPR/C/GC/34, September 12, 2011. [hereinafter HRC General Comment 34].

[263] The Committee's interpretations of the ICCPR's provisions are, under the treaty itself, authoritative, and as such obligate States to comply. International Covenant on Civil and Political Rights art. 40, Dec. 16, 1966, 1976 U.N.T.S. 999 [hereinafter ICCPR].

[264] Joint Declaration, *supra* note 9.

[265] *Id*. ¶ 5(a).

[266] The preamble notes that the subject matter of the Joint Declaration was "discussed . . . together with the assistance of *ARTICLE 19, Global Campaign for Free Expression* and the *Centre for Law and Democracy*." *Id.* What is clear is that net neutrality had figured prominently for several years prior in the advocacy work carried out by international NGOs like Article 19 and others. *See, e.g.*, Belli, Luca and De Filippi, Primavera, "The Value of Network Neutrality for the Internet of Tomorrow", Report of the Dynamic Coalition on Network Neutrality, 2013, available at: http://bit.ly/2f8rbEm; Belli, Luca, "Council of Europe Multi-Stakeholder Dialogue on Network Neutrality and Human Rights", Strasbourg, May 29-30, 2013, available at: http://bit.ly/2grppEk [https://perma.cc/ZQ5Y-RE9N]. So it is fair to assume that this work, as well as the specific consultation with the NGOs, shaped the Joint Declaration.

relationship to freedom of expression did not appear until December 2013, when the Inter-American Commission's Special Rapporteur published her report entitled *Freedom of Expression and the Internet*.[267]

Building on the Joint Declaration she signed, the OAS Special Rapporteur on Freedom of Expression, Catalina Botero, observed in her 2013 Report that "[n]et neutrality is part of the original design of the Internet [and] is fundamental for guaranteeing the plurality and diversity of the flow of information."[268] Interpreting the American Convention on Human Rights, the Special Rapporteur affirmed categorically that respecting net neutrality "is a necessary condition for exercising freedom of expression on the Internet pursuant to the terms [of the Convention's] Article 13."[269] Curiously, neither of the UN Special Rapporteur's 2011 reports on freedom of expression and the Internet (one to the Human Rights Council, the other to the General Assembly) mentions, much less discusses, net neutrality.[270] Nor has the African Commission's Special Rapporteur Faith Pansy Tiakula apparently pursued the topic in her subsequent publications or advocacy.[271]

Following the lead of her OAS counterpart, the OSCE's Representative on Freedom of the Media, Dunja Mijatović, similarly continued to advocate for net neutrality as a core principle of human rights. In June 2014, in response to the U.S. Federal Communications Commission's proposed rules to regulate net neutrality, the OSCE Representative published a report citing the Joint Declaration that concluded "that the FCC's Proposed Rules threaten the free flow of information on the Internet and endanger freedom

[267] Inter American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, Catalina Botero Marino, *Freedom of Expression and the Internet*, 2014. Available at: http://bit.ly/1SyvDM3 [https://perma.cc/6FSP-R583] (hereinafter OAS Special Rapporteur Report).

[268] *Id.* ¶¶ 27-28.

[269] *Id.* ¶ 25. Article 13 of the American Convention states that "[e]veryone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice" and that "the right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions". American Convention on Human Rights art. 13, Nov. 22, 1969, 114 U.N.T.S. 148-49.

[270] *See infra* notes 288-299 and accompanying text.

[271] *See* African Commission on Human and Peoples' Rights, *Special Rapporteur on Freedom of Expression and Access to Information*. Available at: http://bit.ly/2f8wAez [https://perma.cc/5JAZ-VY6C].

of expression and freedom of the media values."[272] In her presentation of the report, Mijatović observed that "[t]he Internet was conceived as an open medium with the free flow of information as one of its fundamental characteristics [. . .]. This should be guaranteed without discrimination and regardless of the content, destination, author, device used or origin."[273]

At a minimum, it is evident from the foregoing that the process of uploading the principle of net neutrality into official human rights *discourse* globally is well underway.[274] Somewhat less apparent is exactly how, as a technical matter, this principle integrates fully into the international law framework for human rights. Certainly by now it seems obvious that "the purpose of this principle is to ensure that free access and user choice to use, send, receive or offer any lawful content, application or service through the Internet is [sic] not subject to conditions, or directed or restricted, such as blocking, filtering or interference."[275] This was an important part of what the UN Human Rights Council and Human Rights Committee intended to cover when they affirmed the extension of human rights law into the digital realm, though neither body mentioned net neutrality by name. But is that the extent of the convergence of net neutrality and human rights law? What other dimensions or ramifications are there to incorporating net neutrality into freedom of expression's panoply of rights? Are there other human rights that might be implicated too? A handful of academics and civil society commentators have started to explore the legal justifications behind the status of net neutrality as a norm of human rights.[276] But more theorizing

[272] Nunziato, Dawn C., "The U.S. Federal Communications Commission's Proposed Rulemaking in The Matter of Protecting and Promoting the Open Internet", Organization for Security and Co-operation in Europe (OSCE), May 15, 2014. Available at: http://bit.ly/2go84ev [https://perma.cc/BQP3-EJR7].

[273] Organization for Security and Co-operation in Europe (OSCE), Press Release, "OSCE Representative Warns that U.S. Proposed Rules on Net Neutrality Can Hurt Online Media Freedom", June 16, 2014. Available: http://bit.ly/2fp4ZXy [https://perma.cc/TMD7-PYGB].

[274] *See, e.g.*, Belli, Luca and van Bergen, Matthijs, "Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet ", Council of Europe, Steering Committee on Media and Information Society CDMSI, 4 th meeting, Strasbourg, 3-6 December 2013, Misc19. Available at: http://bit.ly/2fMPiKB; *see also* OAS Special Rapporteur Report, *supra* note 266. By "official" human rights discourse I am referring to that produced by intergovernmental human rights organizations and their experts charged with providing authoritative interpretations of international human rights law.

[275] OAS Special Rapporteur Report, *supra* note 266, at ¶ 25.

[276] *See, e.g.*,Belli, Luca and De Filippi, Primavera, *supra* note 265; CDT Report 2013, *supra* note 25.

is needed in this direction if the foundations of net neutrality as a norm of human rights are to be secured.

II.B. Net Neutrality and Contemporary Human Rights Law

The human rights law foundations supporting a net neutrality norm are not well understood. In this respect, I seek to clarify three premises in this section. First, by outlining the international law framework governing freedom of expression and its several constituent rights, it becomes clear that net neutrality reacts with more than just the right to impart or access information without restrictions. In particular, the right to access the Internet, or "connectivity," is an equal normative imperative to the realization of freedom of expression. Second, to appreciate how net neutrality operates as a guarantor of freedom of expression requires understanding how the distinct non-discrimination rules built into human rights law are separately natural receptors of that principle as well. And third, regardless of whether one prefers to view net neutrality primarily as a function of expression or as a non-discrimination norm, it is a norm of human rights that, as such, is subject to the exceptions regime established by international law for determining the permissible limits States can impose on fundamental rights. This means that, like all such rights, it is not absolute.

Before turning to the discussion at hand, it is necessary to briefly recall the scope of a State's duty to respect and guarantee respect for human rights under international law. It is well settled that States must do three things to comply with their human rights obligations. First, they must act in good faith to adopt the laws and other measures necessary to implement and give effect to those human rights they are bound to respect.[277] Second, they must ensure that their agents do not violate human rights directly through their actions or omissions, and if they do, provide adequate and effective remedies

[277] *See* Human Rights Committee, *General Comment No. 31 on The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, ¶ 3, U.N. Doc. CCPR/C/21/Rev.1/Add. 13, (May 26, 2004) [hereinafter HRC GC 31]; *see also* Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, art. 1, *opened for signature* Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter European Convention on Human Rights] (entered into force Sept. 3, 1953); Organization of African Unity, African [Banjul] Charter on Human and Peoples' Rights, art. 1, *opened for signature* June 27, 1981, 1520 U.N.T.S. 123 [hereinafter Banjul Charter on Human Rights] (entered into force Oct. 21, 1986); Organization of American States, American Convention on Human Rights, art. 1, Nov. 22, 1969, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123 (entered into force July 18, 1978).

for victims to redress those transgressions.[278] Third, States have an affirmative duty to guarantee the enjoyment of human rights to all persons in their territory or under their jurisdiction, which means they must act diligently to prevent the abuses by third parties, and provide adequate and effective remedies whenever such private actor abuses occur.[279] In this latter respect:

[T]he positive obligations on States…to ensure [human] rights will only be fully discharged if individuals are protected by the State, not just against violations of [these] rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of [these] rights in so far as they are amenable to application between private persons or entities. There may be circumstances in which a failure to ensure [human] rights as required by [international law] would give rise to violations by States . . . of those rights, as a result of States . . . failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm causes by such acts by private persons or entities.[280]]

II.B.I. Freedom of Expression in International Law

Few rights are as defined with such particularity as freedom of expression. Article 19 of the ICCPR, for example, affirms the right "to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of [] choice."[281] This language mirrors that of Article 19 of the Universal Declaration of Human Rights [hereinafter "UDHR"].[282] Substantially similar language is found in Article 10 of the European Convention on Fundamental Rights and Freedoms, Article 13 of the American Convention on Human Rights.[283] Mo-

[278] *See* HRC GC 31, *supra* note 276, at ¶¶ 8, 15; European Convention on Human Rights, *supra* note 276, art. 13; American Convention on Human Rights, *supra* note 276, art. 25.

[279] *See, e.g.*, HRC GC 31, *supra* note 276. This affirmative duty under international human rights law contrasts sharply with the primarily negative one imposed on government actors by the First Amendment in the United States. *See* Nunziato, Dawn C., *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*, Stanford University Press, 2009.

[280] HRC GC 31, supra note 276, at ¶ 8; *see also* Application of Convention on Prevention and Punishment of Crime of Genocide (*Bosn. & Herz. v. Serb. & Montenegro*), Judgment, 2007 I.C.J. 43, ¶¶ 166, 430. (finding that there is an due diligence obligation for States "to employ the means at their disposal... to prevent persons or groups not directly under their authority from committing" acts of genocide. ¶166).

[281] ICCPR, *supra* note 262 arts. 19(2).

[282] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at 19 (Dec. 10, 1948).

[283] European Convention on Human Rights, *supra* note 276, art. 10; American Convention on Human Rights, *supra* note 276, art. 13.

reover, many if not most nations in the world have adopted norms protecting free speech and expression in their constitutions.[284] Freedom of expression enjoys near universal acceptance worldwide, not least because it is correctly viewed as an enabler of several other basic human rights. These include not just the corollary rights to hold opinions and religious beliefs without interference, but others as well, such as the right to education, the right to freedom of association and assembly, the right to full participation in social, cultural and political life, and the right to social and economic development.[285]

Traditionally, freedom of expression has been broken down into several constituent elements, namely: (1) the right to impart or express information and ideas generally; (2) media rights; (3) the right to seek and receive information and ideas generally; and (4) the right to access information "held by public bodies."[286] In particular, it is important to highlight the importance of media pluralism, which States are bound to promote by taking "appropriate action […], to prevent undue media dominance or concentration by privately controlled media groups in monopolistic situations that may be harmful to a diversity of sources and views."[287]

Since the rise of electronic communications, the foregoing framework of freedom of expression has evolved to accommodate the transmission and receipt of information and ideas via the Internet. As noted in the preceding sub-section, it is settled that the constituent rights comprising freedom of expression will today apply to all "internet-based modes of communication."[288] What this means as a practical matter is that "[a]ny restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3 [of Article 19]."[289] I'll come back to the exceptions regime below.

---

[284] *See, e.g.*, Mendel, Toby, *et. al*., *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Publishing, 2012. Available at: http://bit.ly/1l9bEkV

[285] United Nations, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/66/290, August 10, 2011, ¶ 61 [hereinafter SR GA Report 2011].

[286] Human Rights Committee, *General Comment No. 34: Article 19 (Freedoms of opinion and expression)*, ¶¶ 11, 18, U.N. Doc. CCPR/C/GC/34 (Sep. 12, 2011) [hereinafter HRC GC 34]. Each of these is described more fully in General Comment No. 34. Media rights, for example, are described in more detail in ¶¶ 13-17, 37-42.

[287] *Id.* ¶ 40.

[288] *Id.* ¶ 12.

[289] *Id.* ¶ 43.

It is likewise helpful to recall here that the State responsibility regime summarized at the outset of this section specifically "requires States to ensure that persons are protected from any acts by private persons or entities that would impair the enjoyment of the freedoms of opinion and expression to the extent that these…rights are amenable to application between private persons or entities."[290] States have an affirmative duty, therefore, to adopt measures and act diligently to ensure that freedom of expression rights are protected from private actor conduct that might impinge on the enjoyment of those rights by others.[291]

Rounding out the panoply of freedom of expression rights relating to net neutrality is the newest dimension of the right to access information: connectivity.[292] Put simply, "[g]iving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet."[293] This positive obligation means that for States to meet their duty to respect and fulfill the right to freedom of expression, they must guarantee that all people within their territory have access to "the means necessary to exercise this right, which [today] includes the Internet."[294] Accordingly, the UN Human Rights Committee has called upon States "to take all necessary steps to foster the independence of…new media…such as internet and mobile based electronic information dissemination systems…*and to ensure access of all individuals thereto*."[295] Connectivity is thus "essential" to realizing freedom of expression.[296]

The good faith duty incumbent on States to work diligently towards the effective implementation of freedom of expression is equally as relevant to progressively realizing other fundamental rights too, such as the rights to education, health, socio-economic development, and political participa-

[290] *Id.* ¶ 7.

[291] *See supra* notes 282--283 and accompanying text.

[292] There does not appear to be a universally accepted definition of connectivity in international law or practice. "Connectivity" is understood here as access to any kind of Internet connection that provides full or partial access to services, applications and information available online. *See* SR GA Report 2011, *supra* note 288.

[293] Joint Declaration, *supra* note 9, at 3; *see also* Human Rights Council Res. 20/8, ¶ 3, U.N. Doc. A/HRC/20/L.13 (June 29, 2012).

[294] *See* SR GA Report 2011, *supra* note 284, ¶ 61.

[295] HRC GC 34 *supra* note 285, ¶ 15 (emphasis added); *see also* OAS Special Rapporteur Report, *supra* note 266, ¶ 11 ("It is important for all regulation to be based on dialogue among all actors and to maintain the basic characteristics of the original environment, strengthening the Internet's democratizing capacity and fostering universal and nondiscriminatory access.").

[296] *See* SR GA Report 2011, *supra* note 284, ¶ 61.

tion.[297] It is for these reasons that the top experts of four major human rights legal systems stressed in 2011 that, at a minimum, States are required to "[p]ut in place regulatory mechanisms – which could include pricing regimes, universal service requirements and licensing agreements – that foster greater access to the Internet, including for the poor and in 'last mile' rural areas."[298] In modern times, it is difficult to overstate the transcendental role that connectivity as an integral part of freedom of expression plays in the realization of human rights generally.

II.B.II. Non-discrimination in International Law

Non-discrimination is a first order principle of international human rights law. "Non-discrimination, together with equality before the law and equal protection of the law without any discrimination, constitute a basic and general principle relating to the protection of human rights."[299] It is for this reason that, once again mirroring the UDHR, the ICCPR establishes that States are obligated "to respect and to ensure to all individuals within [their] territory and subject to [their] jurisdiction the [human] rights recognized…without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[300] At the same time, "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law."[301] This provision prohibits "discrimination under the law and guarantees to all persons equal and effective protection against discrimination on any ground," or based on any kind of distinction of the types listed above.[302] Anti-discrimination principles substantially similar to these appear in every universal and regional human rights treaty.[303] So, to the extent that net neutrality is best understood as a

[297] Human Rights Council Res. 20/8, ¶ 3, U.N. Doc. A/HRC/20/L.13 (June 29, [2012]); *see also infra* notes 321-334 and accompanying text. On the duty of States to implement their basic human rights obligations, *see, e.g.*, ICCPR, *supra* note 262 at art. 2(2).

[298] Joint Declaration, *supra* note 9 ¶ 6(e)(i).

[299] Human Rights Committee, *General Comment No. 18 on Non-discrimination (Thirty-seventh session, 1989)*, Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 (July 29, 1994) at 26 [hereinafter HRC GC 18].

[300] ICCPR, *supra* note 262 at art. 2; *see also* HRC GC 18, *supra* note 298 ¶ 1.

[301] ICCPR, *supra* note 262 at art. 26.

[302] HRC GC 18, *supra* note 298 ¶ 1.

[303] *See e.g.* European Convention on Human Rights, *supra* note 276, art. 14; Banjul Charter on Human Rights, *supra* note 276, art. 2; American Convention on Human Rights, *supra* note 276, art. 24.

principle of non-discrimination applied to users' rights to request, receive or impart data or information online, it meshes organically with the core non-discrimination norms of international human rights law.

Unlawful discrimination of any type is a negation of human equality and dignity. Under international human rights law it is defined as any "distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or *other status*, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms."[304] But not all discrimination is *per se* illegal. International law differentiates between negative and positive discrimination. The "principle of equality sometimes requires States parties to take affirmative action in order to diminish or eliminate conditions which cause or help to perpetuate discrimination prohibited [by international law]."[305] For this reason, "[n]ot every differentiation of treatment will constitute [unlawful] discrimination, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a purpose which is legitimate under the [international law]."[306]

The remaining question is what counts as "other status" for purposes of determining what additional distinctions might lead to negative (or positive) discrimination. Of relevance is the fact that international human rights law recognizes distinctions based on *economic* status or criteria, and evaluates whether their purpose or *effect* is to nullify or impair the exercise or enjoyment of other human rights.[307] So, for example, the UN Human Rights Committee found that Iceland's legal differentiation between two groups of fisherman, one of which was forced to pay exorbitant catching fees to the other to whom the State had granted permanent, exclusive quota-based licenses for historical reasons, constituted an unlawful distinction based on unreasonable "property entitlement privileges."[308] On the other hand, as noted above, where such a distinction is based instead on "reasonable and objective" criteria, and is intended to advance a valid State aim, it can be

[304] HRC GC 18, *supra* note 298 ¶ 7 (emphasis added).

[305] *Id.* ¶ 10

[306] *Id.* ¶ 13

[307] *See* Human Rights Committee, *Haraldsson v. Iceland*, Communication Nº. 1306/2004, October 24, 2007, ¶ 10.3. Available at: http://bit.ly/2fct8ml [https://perma.cc/NH8A-PM2X].

[308] *Id.* ¶¶ 10.3–10.4. ("The Committee concludes that ... the property entitlement privilege accorded permanently to the original [fishing] quota owners, to the detriment of the [other fishermen], is not based on reasonable grounds.")

deemed to reflect a "legitimate differentiation" under international law.[309] So, for instance, a State could adopt temporary tax breaks for low-income workers in a critical but depressed sector of the economy, say, construction.[310] Even though the measures would discriminate against similarly situated workers in other sectors that did not receive the tax breaks, the State arguably would be pursuing a legitimate aim (bolstering an important sector of its economy and advancing socio-economic rights) by utilizing objective criteria (focusing on low-income, depressed sector workers) to adopt reasonable measures (tax breaks of limited duration) to meet that aim.[311] Such a policy would likely not violate the non-discrimination obligations imposed by international human rights law.

II.B.III. The Exceptions Regime for Freedom of Expression

Human rights norms in general, and freedom of expression in particular, are not absolute.[312] Human rights law expressly permits certain restrictions on the right to freedom of expression that "respect [] the rights or reputations of others" or advance "the protection of national security, or of public order…, or of public health or morals."[313] These are, generally speaking, legitimate aims that will justify State action when acting to curtail fundamental human rights such as expression.[314] But, of course, there may be others. We saw how States can in limited circumstances apply positive discrimination to address the social and other consequences of prior invidious discrimi-

[309] *See supra* notes 307-308 and accompanying text.

[310] *See, e.g.*, Human Rights Committee, *R.P.C.W.M. Brandsma v. Netherlands*, Communication Nº. 977/2001, April 1, 2004,¶¶ 6.3-6.4. Available at: http://bit.ly/2fxsQnY [https://perma.cc/YV53-YBWV].

[311] *Id.* The Human Rights Committee did not reach the case on the merits, finding it inadmissible for lack of evidence that the tax payment schemes at issue were substantially comparable. However, the HRC's discussion of the underlying issues suggests that it might otherwise have found such a scheme to advance the State's legitimate aim in a permissible manner.

[312] A good example is ICCPR, *supra* note 262, at art. 20, which explicitly enumerates a series of offensive forms of expression that States *must* curtail in order to meet their obligations under the treaty. ("1. Any propaganda for war shall be prohibited by law. 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.").

[313] ICCPR, *supra* note 262, at art. 19(3); HRC GC 34, *supra* note 285, at paras. 28-32.

[314] *See* Frank LaRue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/23/40, April 17, 2013, ¶.28 ("The framework for article 17 of the ICCPR enables necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations").

nation.[315] In addition to pursuing a legitimate goal, a State seeking to limit freedom of expression must ensure that any restrictions are "provided by law," "necessary" to meet that aim, and "proportional."[316] The existence of this exceptions regime, however, is not a blank check: "When a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself."[317] In other words, exceptions must remain exceptional, and cannot become the rule.[318]

Each element of the exceptions framework merits further explanation. The legitimate aims States can pursue are stipulated in international law.[319] Here, it is worth highlighting the objective of protecting or advancing *other people's rights* as a basis for restricting a given norm. Defamation laws are classic examples of hard limits imposed on freedom of expression to protect the reputation of others.[320] And just as "legitimate differentiation" in favor of historically disadvantaged groups can affirmatively advance the goals of non-discrimination,[321] so too can freedom of expression rights be curtailed to promote the freedom of expression rights of others.[322] Thus, for example, "it may be permissible to protect voters [who wish to express their political opinions] from forms of expression that constitute intimidation or coercion."[323]

---

[315] *See supra* notes 306—307 and accompanying text.

[316] ICCPR, *supra* note 262 at art. 19(3); HRC GC 34, *supra* note 285 at ¶¶ 24-26, 33-34; SR GA Report 2011, *supra* note 284, ¶ 15.

[317] HRC GC 34, *supra* note 285, at para. 21.

[318] "[T]he relation between right and restriction and between norm and exception must not be reversed." *Id*.

[319] ICCPR, *supra* note 262, at arts. 19, 20.

[320] HRC GC 34, *supra* note 285, at para. 47 ("Defamation laws must be crafted with care to ensure they comply with paragraph 3 and that they do not serve, in practice, to stifle freedom of expression").

[321] *See supra* note 311 and accompanying text.

[322] HR GC 34, *supra* note 285, at para. 28 ("The term 'rights' includes human rights as recognized in the [ICCPR] and more generally in international human rights law… The term 'others' relates to other persons individually or as members of a community.").

[323] *Id*; obviously this implicates the distinct Art. 25 right to vote as well, without diminishing the relevance of the political expression that is realized through voting. *See Vladimir Viktorovich Shchetko v. Belarus*, Communication Nº. 1009/2001, U.N. Doc. CCPR/C/87/D/1009/2001 (2006), at para. 7.4 ("The Committee recalls that under article 25(b), every citizen has the right to vote, and that in order to protect this right, States parties to the Covenant should prohibit any intimidation or coercion of voters by criminal laws and that such laws should be strictly enforced (4). The application of such laws constitutes, in principle, a lawful limitation of the right to freedom of expression, necessary for the respect of the rights of others"), available at: http://bit.ly/2fxtaDj ; *Leonid Svetik v. Belarus*, Communication Nº. 927/2000, U.N. Doc. CCPR/C/81/D/927/2000 (2004), at para. 7.3 (stating the same proposition), available at: http://bit.ly/1jAPl8F

In practice, States are typically given leeway in determining what policies they can adopt to advance or meet specific goals within the general categories of legitimate aims identified.[324]

Assuming that a State's goal is to advance a legitimate aim recognized by international law, any proposed restriction on freedom of expression must not only be provided by law, it must also be necessary and proportional. This is meant to set a high bar for recognizing a small set of narrowly tailored measures.[325] Generally speaking, such restrictions should be enacted into formal law through a transparent and participatory political process.[326] In any case, such laws "must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly."[327] They must also be accessible to the public.[328] In addition, to be "necessary," legally enacted limits must be "directly related to [meeting] the specific need on which they are predicated,"[329] i.e., they must be effective at doing what they are intended to do. A restriction is not indispensable, and thus "violates the test of necessity[,] if the protection could be achieved in other ways that do not restrict freedom of expression."[330] Finally, any steps taken by States to limit expression, even if legitimate and necessary, cannot be "overbroad."[331] Proportionate measures are those that are "appropriate to achieve their protective function" and "the least intrusive amongst those [available]."[332]

In sum, the foregoing sub-sections have clarified the technical grounds

[324] *See Leo Hertzberg et al v. Finland*, Communication Nº. 61/1979, U.N. Doc. CCPR/C/OP/1 (1985), available at: http://bit.ly/2fUqWi2 [https://perma.cc/BV6H-TR3G] (recognizing "a certain margin of discretion [that] must be accorded to the responsible national authorities" in deciding whether to broadcast discussions related to homosexual relations in national media); *see also* Schmidt, Markus, *Book Review, Coming to Grips with Indigenous Rights*,10 Harv. Hum. Rts. J. 313, 338, 1997 (interpreting HRC decisions as based on the margin of appreciation rationale); *see also* Legg, Andrew, The Margin of Appreciation in International Human Rights Law: Deference and Proportionality, Oxford, Oxford University Press, 2012 ("There are no clear cases in the Inter-American Court of Human Rights (IACtHR) and the United Nations Human Rights Committee (UN HRC) that reject the margin of appreciation as resulting in relativism about human rights").

[325] *See* HRC GC 34 *supra* note 290, at para. 35.

[326] *See* United Nations, *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/17/27, May 16, 2011 (by Frank La Rue), ¶ 24.

[327] HRC GC 34, *supra* note 285, at para. 25.

[328] *Id*.

[329] *Id* at para. 22.

[330] *Id* at para. 33.

[331] *Id* at para. 34.

[332] *Id* at para. 34.

upon which net neutrality's formal incorporation into international law as a human rights norms are premised. Specifically, I have shown that freedom of expression is composed of various constituent norms, several of which react with net neutrality. In addition to the "classical" right to impart or access information, the right to access the Internet—connectivity—is today essential to the full realization of freedom of expression. Moreover, I explained how the non-discrimination principles built into human rights law interact with freedom of expression, and why they too are natural receptors of net neutrality. Finally, I outlined the frameworks that govern when and how States may enact legitimate exceptions to freedom of expression and non-discrimination rules. This exposition of the exceptions regime under international law explains why neither freedom of expression nor non-discrimination norms are entirely exempt from State-imposed restrictions that advance legitimate State aims, such as the advancement or protection of the rights of others. Any such limits, however, must not only be enacted in law, but must also be demonstrably necessary and well-tailored to achieving the lawful ends identified.

II.C. Why International Human Rights Law?

Why does it matter that net neutrality is today a consolidated norm of international human rights law? With few exceptions, most discussions to date of zero-rating have centered on the economic, social, and technical implications of allowing or prohibiting such practices in a given country.[333] Though some attention has been paid to net neutrality as a norm that promotes and protects human rights,[334] this perspective has not yet been fully extended to zero-rating. As it turns out, re-framing net neutrality and zero-rating as human rights issues way leads to a range of significant consequences.

There are a number of substantive and strategic advantages to invoking the human rights legal framework in this regard. First, under human rights law, net neutrality is defined in human-centric rather than data-centric terms.[335] This shift is not merely semantic because it portends important implications for that norm's implementation, especially in terms of connectivity. In particular, it means that zero-rating practices as transgressions of net neutrality can no longer be discussed in all-or-nothing terms. Instead, these

[333] *See supra* note 23 and accompanying text.

[334] *See, e.g.*, CDT Report 2013, *supra* note 25; *see also* Luca Belli EC Report, *supra* note 265 and accompanying text.

[335] *See supra* notes 280-283 and accompanying text.

practices have to be viewed as proposed limits on *some* peoples' freedom of expression (understood as net neutrality) intended in substantial part to enhance the freedom of expression rights of *others* (i.e. through expanded access). Second, as explained in the prior section, this re-framing places net neutrality issues squarely within a universally recognized normative framework that imposes clear legal obligations on a majority of States.[336] Safeguarding net neutrality thus becomes a duty incumbent on governments, rather than merely a compelling or controversial policy alternative. This ensures that discussions about how to limit net neutrality like those taking place in the United States, Europe, Mexico, and a host of other countries, transpire within the same, universally applicable regime established by international law, promoting greater normative consistency across the board.[337]

Last but not least, for all the foregoing reasons, the human rights framework provides structure and rigor to what often are heated contests of unmoored dogma: net neutrality absolutism clashing with the inviolability of the market place. Evaluating net neutrality regulation as a function of the State's duties under international law opens practical pathways for constructively debating zero-rating, because it establishes normative parameters that apply equally to all sides engaged in the discussions. People stop talking *past* each other, and start talking *to* each other. At the same time—and this is critical—the human rights approach is the only one that expressly accounts for all the others. Those who view net neutrality as a sacred network principle will pay little heed to what the economists and free market advocates say; others who critique net neutrality as a malleable priority preference may prioritize competition, consumer choice, or the public interest. In other words, the prevailing perspectives—social, economic, technical—that characterize the net-neutrality and zero rating debates do not easily accommodate each other, if at all. Very few pay anything more than lip service to human rights.

Human rights law is different: it is the unifying "theory of everything." All other approaches have a place in the normative framework as quantitative and qualitative *inputs* for the analysis of the State's obligations to

[336] The ICCPR has 168 State Parties, encompassing over 85% of the worlds population. *See* United Nations Treaty Collection, Chapter IV, Human Rights, *International Covenant on Civil and Political Rights*,available at: http://bit.ly/2fxxYs7. In addition, the Universal Declaration of Human Rights is considered a source of customary international law, which would cover the remaining UN member States in substantially similar fashion. *See, e.g.*, Office of the High Commissioner of Human Rights, *Digital Record of the UDHR*, February 2009, available at: http://bit.ly/2fjQUwY [https://perma.cc/ZW9H-PL5M].

[337] The Council of Europe has taken this approach. *See* "Council of Europe Gets Tough on Net Neutrality…", *supra* note 20.

promote and protect the rights of their people. Data on whether or not zero-rating practices advance or hinder meaningful Internet access are integral to the analysis of the *necessity* of the proposed measures. Market studies of the impact of zero-rating practices on innovation, competition, and user experience will factor into the analysis of whether the zero-rating practices authorized are *proportional*. Issues of policy are folded into the discussion of what constitutes a *legitimate aim* of States seeking to restrict freedom of expression by curtailing net neutrality through differential pricing (or other means). As I will show in the final Part, whether one is evaluating the legitimacy of the State's objectives, or the nature of differential pricing and its impact on net neutrality, all relevant data— social, economic, political, technical—will play a role and be balanced against countervailing factors also recognized by the human rights framework. The same cannot be said of any other approach.

III. Towards a Human Rights Analysis of Zero Rating

Human rights can be invoked by advocates on all sides of the net neutrality and zero-rating debates. Those who defend an essentially unqualified concept of net neutrality insist that people's rights to receive or impart information and ideas freely should rarely if ever be compromised (though most admit the need for a few exceptions, for example, to reasonably manage the network or protect its integrity). They believe that maintaining a near blanket prohibition on any differentiation in the handling of Internet traffic, and preserving the purity of the "end-to-end" principle, is the best—if not the only—way to truly preserve the integrity and unbound potential of the network.[338] For these reasons, among others, they prefer to seek alternatives to zero-rating in the developing world that can advance the laudable goal of increasing full connectivity without sacrificing network neutrality. Proponents of zero-rating practices, on the other hand, frequently justify their position by pointing to the daunting digital divide and the imperative to empower the masses of unconnected people living primarily in the

[338] *See, e.g.*, Crawford, Susan, "Zero for Conduct", *Backchannel*, January 7, 2015. Available at: http://bit.ly/2g9oWI1 ("The aim of net neutrality is to preserve the Internet as the crucial open sidewalk for communication that it has become. The reason that the Chinese, Russian and Cuban governments fear open Internet more than anything else is that it allows users to gather and speak to one another. (. . .) Linking and building are fundamental attributes of the Internet—innovation and speech without permission—and that must not be compromised").

developing world by any means available. In this more pragmatic view, the ends justify the means: the best way to improve the situation of those disenfranchised people, they say, is to ensure their right to access at least some of the Internet in the first place, as an onramp to fuller Internet access, thus enabling them to exercise their freedom of expression and enjoy the benefits of other human rights as well, even if that means curtailing net neutrality through zero-rating.[339]

As a rule, when advocates for either side make express reference to human rights in support of their arguments, those references tend to be cursory at best. Even when digital rights advocates invoke human rights more formally, the supporting analysis is either lacking or deficient. This Article has addressed such normative gaps by clarifying the operation of the applicable human rights legal framework; that was the object of Part II. In this final Part, I consider that framework *in context* with reference to the empirical data presented in Part I. In particular, I review the key elements of the exceptions regime—legitimate aim, necessity, and proportionality—to better illustrate how they would apply in country-specific conditions like those described in Part I.B. To achieve this, I draw from prior discussion of other key topics, namely the typology of zero-rating practices and the barriers to connectivity. This should deepen the understanding of how human rights analysis applies to these issues.

III.A. Legitimate Aim

States are increasingly under pressure to close the global digital divide. The United Nations' Sustainable Development Goals commit States to "[s]ignificantly increas[ing] access to information and communications technology and striv[ing] to provide universal and affordable access to the Internet in least developed countries by 2020."[340] Whether a State's aim to do so is legitimate or not when proposing restrictions on net neutrality, such as differential pricing, will depend on that country's social, economic, and political conditions. States with high levels of connectivity, whether wired or mobile or both, will face different challenges than those with large percentages of their population on the wrong side of the digital divide. Most

[339] *See, e.g.*, Hempel, Jessi, "Inside Facebook's Ambitious Plan to Connect the Whole World", *Wired*, January 19, 2016. Available at: http://bit.ly/1ncpvOg [https://perma.cc/4DZ6-NP8Q].

[340] United Nations, *Sustainable Development Goals, 9.c*. Available at: http://bit.ly/1Qk5cqI

States in this latter category are developing countries, where the vast majority of unconnected people live.[341] It is therefore easier for a country such as Zambia, where less than 20 percent of its people have Internet access, to claim that by promoting zero-rating it is advancing a legitimate State aim, i.e., promoting connectivity, than for the United States to do so, given its access rate of nearly 90 percent.[342] The key to understanding the legitimate aim element, however, is not Internet penetration rates *per se*, but the barriers to connectivity that keep them low in many countries.

To advance a legitimate aim, a developing country's zero-rating policies must address the principal barriers to connectivity. Primary among these is the relatively high cost of accessing data via Internet on wired and mobile platforms. One reason Internet access is far greater in developed countries is its relative affordability. As a rule, such countries have higher per capita incomes and lower inequality rates than developing ones. Wired and mobile penetration rates are also high, as more people can afford the necessary hardware and data plans. There are few hard barriers to connectivity for most. And there are fewer "soft" barriers as well, such as low literacy and education levels, that can keep people off the Internet even where access is affordable. In short, the barriers to connectivity are simply not as high in developed countries, if they exist at all, as they are in most parts of the developing world. It follows that governments in developed countries will generally face an uphill battle to justify restricting net neutrality to allow for zero-rating as a means of enhancing connectivity.[343]

It should be evident by now that generating greater opportunities to connect for the digitally disenfranchised sectors of society can substantially advance the realization of freedom of expression and other basic human rights in any country marked by a significant digital divide.[344] The benefits of increasing access in the developing world are too well established to bear repeating here. For these reasons, zero-rating plans, though discriminatory for economic reasons, might still constitute a "legitimate differentiation"

[341] *See supra* notes 132 – 166 and accompanying text.

[342] Freedom House, *supra* note 228.

[343] Open Letter, *supra* note 110. "In advanced economies like those in the European Union, there is no argument for zero-rating as a potential onramp to the Internet for first-time users." *Id.* This does not mean that developed countries could not justify zero-rating practices by pointing to other potentially legitimate aims including, perhaps, advancing non-harmful forms of public and private sector zero-rating that advance the public interest or well-being without unduly impacting competition, innovation, or expression.

[344] *See supra* notes 132 – 201 and accompanying text.

under human rights law if they meet the other elements of the exceptions regime test.[345] Developing States with digital divides that choose to promote this goal will likely have a legitimate aim. Expanding Internet access is no less essential to realizing freedom of expression and other basic human rights than ensuring the general right to impart or receive information in a non-discriminatory manner, which is what net neutrality does. So the main challenge for most States struggling to bridge their domestic digital divide by promoting greater connectivity will be whether the proposed means are necessary *and* proportionate, as well as prescribed by law.

III.B. Necessity

Necessity is a factual question. What restrictions are indispensable to tackling a recognized problem or challenge *in a given context* will turn on: (a) the extent to which they are effective; (b) the nature of the problem addressed; (c) the existence of viable alternatives; and (d) the effectiveness of those alternatives. It is important to note that "necessary" does not mean "exclusive," especially where the challenges faced are substantial and/or complex. A related issue is who is best positioned to determine when a particular measure is "necessary" to meet the objectives sought, and when it is not. For purposes of the ensuing discussion, references to "zero-rating practices" will refer to those described in the typology presented above in Part I.A.

There is evidence that zero-rating practices can increase the number of people accessing at least parts of the Internet, and sometimes the full Internet, by lowering the cost of access.[346] "For example, in less than a year, Facebook's zero-rating initiative Internet.org…won more than 9 million [new] users."[347] According to Facebook, more than half of these users went on to pay for additional access to the Internet within 30 days of joining.[348] Certainly a large number of governments have bet on this approach being true in practice when promoting or condoning zero-rated platforms as a means of promoting connectivity, and thereby development.[349] Few critics

[345] *See supra* note 307 and accompanying text. ("The "principle of equality sometimes requires States parties to take affirmative action in order to diminish or eliminate conditions which cause or help to perpetuate discrimination prohibited [by international law.]").

[346] *See* "One Year In", *supra* note 49.

[347] Stanford Study, *supra* note 23, at 5.

[348] *See* "One Year In", *supra* note 49.

[349] *See supra* note 32 and accompanying text; *see also, e.g.*, Babu, Anita, "Zuckerberg to Visit India on Oct. 28, First After Internet.org Rebranding", *Business Standard*, October 17, 2015, http://bit.ly/2fUy9yr [https://perma.cc/JDS7-H5XB].

of zero-rating dispute that offering reduced cost or free access to some Internet services can work in favor of increasing mobile subscriptions and some connectivity. Instead, most critics focus their attention on the perceived *harms* generated by such practices—the creation of "walled gardens" for users or the impact on competition—which they claim outweigh the potential benefits.[350] Regardless, there is no question that more empirical research is needed to confirm the circumstances under which zero-rating practices can be effective in overcoming the crucial barrier of high access costs, the extent of that effectiveness, and the countervailing consequences of adopting such practices.[351]

The very same is true of the faux or non-selective zero-rating practices that purport to facilitate public connectivity at reduced cost without offending net neutrality, perhaps even more so.[352] As of this writing, there is little data or analysis available on the impact and effectiveness of zero-rating *alternatives* as such, though important initiatives are underway to change that. For example, Mozilla is researching the effects of its "equal rating" initiatives in the field.[353] Another example is provided by community networking, which advocates say expands full connectivity in both rural and urban areas.[354] These initiatives, to answer the questions posed by the necessity prong of the exceptions regime, would have to ascertain the positive and negative consequences for freedom of expression of implementing a particular zero-rating *alternative* in a given local context, and comparing those outcomes to similar ones obtained for zero-rated practices conducted in the same or similar context. There is no other way to know whether zero-rating practices achieve greater, similar, or lesser levels of connectivity than those that "could be achieved in other ways that do not restrict freedom of expression."[355]

The upshot is that we are a long way from being able to say with any certainty that zero-rated connectivity-enhancing approaches are significantly more or less effective at closing the digital divide in a particular setting than any of the current alternatives. Add to this the sheer magnitude of the

[350] *See* Open Letter, *supra* note 7.

[351] *See* Thakur, *supra* note 23.

[352] *See, e.g.*, TRAI Consultation Paper, *supra* note 20, para. 18.

[353] *See* Mozilla Study, *supra* note 23.

[354] *See* FGV Direito Rio, "Community Networks: Lesson [sic] from International Practice", *Youtube,* April 29, 2016, http://bit.ly/2geo0NJ [https://perma.cc/2F6C-JYWS].

[355] *Id.* at para. 33.

social, economic, political, and cultural challenges facing States in the developing world that seek to establish access to the Internet for their people,[356] and it becomes impossible to exclude *ab initio* any presumptively viable approach as unnecessary, even if it offends net neutrality. Moreover, there is good reason to believe that the principal problem addressed—closing the digital divide in those countries where it is most prevalent—is substantial and complex enough to require an amply diversified response.[357] For these reasons, it is not possible at this point to simply dismiss zero-rating practices as unnecessary or dispensable on the grounds that they are either not effective enough, or that there are better alternatives available that can achieve the same or better results. This means that the most fertile ground for critics of zero-rating measures in these situations is that offered by the evaluation of proportionality.

III.C. Proportionality

At the heart of the proportionality element is the balance between advancing the legitimate aim identified and the human rights cost of achieving it.[358] If a proposed restriction on freedom of expression advances such an aim effectively enough to be considered necessary, the question becomes whether it has been configured appropriately, such that the positive gains from enacting it outweigh the negative consequences sufficiently to justify the curtailment of that underlying right. "When assessing the proportionality of a restriction on freedom of expression on the Internet, the impact of that restriction on the ability of the Internet to deliver positive freedom of expression outcomes must be weighed against its benefits in terms of protecting other interests."[359]

In other words, proportionality can only be determined with reference to a particular situation and specific circumstances. Exceptions that sweep too broadly may threaten to "swallow the rule,"[360] while those that deliver minimal or negligible benefits will be unlikely to advance a legitimate aim. Finally, for such measures to pass muster under this legal standard, they should be the least

[356] *See supra* notes 126 – 165 and accompanying text.

[357] *See* Carrillo, Arturo J., "Comment on Differential Pricing for Data Services" [in India], December 30, 2015, at 6 (unpublished manuscript) (on file with author).

[358] For a detailed discussion of the nature and role of proportionality in human rights adjudication, see Legg, *supra note* 323, Ch. 7.

[359] Joint Declaration, *supra* note 9, para. 1(b).

[360] *See supra* note 320 and accompanying text.

intrusive available to ensure the desired ends.[361] If they are not, the balance would tip *against* the legality of such a measure. In sum, once the other elements of the exceptions regime are met, whether a proposed zero-rating practice is proportionate or not is a factual question of relative balance between its pros and cons.[362]

There are several factors to keep in mind when engaging in the balancing analysis of proportionality, which is where much if not most of the zero-rating debate in the developing world should focus. General factors include the *type* of zero-rating practice at issue, its particular *configuration*, and the perceived *benefits* it can bring in relation to the legitimate aim sought;[363] the *nature of the Internet access* and content provided; the existence and *comparable effectiveness* of non-net neutrality offending alternatives; and any other *negative consequences* of that zero-rating practice on users' enjoyment of their basic human rights.[364] The Center for Democracy and Technology has developed a complementary framework of more specific factors that serve to better identify "the potential benefits and harms" of particular zero-rating arrangements.[365] These include the principle of non-exclusivity, a presumption against sponsored data plans, attention to privacy and data security, providing technical assistance and training in local markets, transparency and regulation.[366] The function of this framework can be summarized as follows:

With respect to edge providers, the overriding concern is the potential for market distortion as edge providers are either excluded from preferential arrangements or coerced to modify their content and services to benefit from them. Thus, whether arrangements are exclusive (particularly exclusive to affiliates of the network operator), sponsored, or limited to particular sources or types of content and applications are all highly relevant considerations. For users, the ability to maintain the control of the content and services they access or create via the Internet is the overriding consideration. User choice in selecting zero-rated content, the availability and cost of metered content, and the transparency of zero-rating arrangements are significant factors in determining whether zero rating can spur broadband adoption and access to the open Internet. Finally,

361 *See supra* note 323 and accompanying text.

362 *See* Legg, *supra note* 323, at 181 (describing proportionality as a legal test centered on "assessing side effects" of a proposed restriction).

363 *See supra* Part I.A.

364 *See* Legg, *supra note* 323, at 181 (The "legal proportionality test [entails] the assessment of the side effects, means, and even ends of state action.").

365 Stallman, Erik and Adam, R. Stanley, "Zero Rating: A Framework for Assessing Benefits and Harms", Center for Democracy & Technology, January 2016. Available at: http://bit.ly/2gdfwa0 [https://perma.cc/K8AM-TUG5].

366 *Id.* at p. 22-23.

whether zero rating will serve as an on-ramp to "full" Internet access or a roundabout of curated offerings that users exit only at great effort and expense, if at all, depends on some fundamental attributes of the broadband market: existing levels of adoption and deployment, competition, and digital literacy and education.[367]

To understand how such factors operate, we must examine them in context. Take the example of Zambia, profiled in Part I.B.III. One of the principal criticisms of the Internet.org/Free Basics platform operating in Zambia, a compound zero-rating practice, has been that it offers only limited access to certain select sites and services on the Internet as curated by Facebook (in partnership with Airtel, the local telecom), creating an Internet "for poor people."[368] Critics say that, in addition to violating net neutrality in principle, this model of compound zero-rating creates an invidious "walled-garden," which is "absolutely inappropriate" because it "creates a synthetic 'online' experience for users that isn't the Internet."[369] They claim, moreover, that in developing countries like Zambia, zero-rating platforms such as Internet.org/Free Basics can have prejudicial economic consequences by "empower[ing] market concentration, restrict[ing] local innovation and reduc[ing] user choices."[370] All these compelling concerns can be placed on the "negative and potentially negative consequences" side of the proportionality scale. But they must be contrasted and weighed against the countervailing "positive and potentially positive consequences" on the other.

And there are palpable benefits to consider. According to Facebook, a year after the roll-out of Internet.org in Zambia, with its emphasis on granting access to a range of basic services sites of interest to the public,[371] the goal of increased connectivity had been substantially advanced, there and elsewhere:

> Internet.org brings new users onto mobile networks on average over 50% faster after launching free basic services [than before they were launched], and more than half of the people who come online through Internet.org are paying for data and accessing the internet within the first 30 days. These points show that Internet.org is not only a successful tool in helping bring people online, but it is successful in showing people the value of the internet and helping to accelerate its adoption.[372]

---

[367] *Id.* Executive Summary.

[368] *See* Honan, *supra* note 183

[369] Crawford, *supra* note 337.

[370] Ramos, Pedro Henrique Soares, *supra* note 23.

[371] *See supra* note 184 and accompanying text.

[372] *See* "One Year In", *supra* note 49; *see also* "Facebook's Internet.org App Offers Free Internet Access in Zambia", *BGR*, August 18, 2014, available at: http://bit.ly/2fk2xnL[https://perma.cc/A2AL-EKV9].

Facebook is not the only one saying that zero-rating platforms like Internet.org can have positive effects on increased connectivity rates,[373] or that they may not be as harmful to innovation, competition and user choice as the naysayers claim.[374] And while access is limited to a suite of selected sites offering free basic services, these services have been geared towards local needs and content.[375] It can also be noted that, in response to concerns about Internet.org's impact on local competition and innovation, Facebook made changes to the platform's specifications to make it non-exclusive and more accessible to service providers and application designers, in order "to work with as many mobile operators and developers as possible to extend the benefits of connectivity to diverse, local communities around the world."[376] This was intended to reduce the harm to competition and innovation that a closed platform would have.

The balancing of pros and cons required by proportionality can only be carried out in relation to the underlying problem addressed and the obstacles to resolving it. In the case of Zambia (and other developing countries), this means the domestic digital divide and barriers to connectivity. Despite improvement in recent years, Zambia is still ranked by the United Nations as one of the "least-developed" countries in the world.[377] Internet penetration rates are dismal: less than 2 percent of the population has wired Internet access at home, and it is unlikely that the hard barriers to increased connectivity will allow for much improvement on that front. On the other hand, the total number of Internet users is around 15 percent, thanks to much higher mobile phone coverage among the population. Even so, there is a substantial gap between that 15 percent, and the 67 percent that have mobile phones generally, suggesting an opportunity to narrow the divide by promoting greater mobile connectivity.[378] This is where the compound zero-rating platform Internet.org/Free basics has stepped in.

In the Zambian context, it is therefore possible to argue from a human rights law perspective that, in light of the country's deep connectivity crisis, the benefits in terms of increased access offered by Internet.org/Free Basics, although limited to select services, still outweigh the disadvantages of that

[373] *See supra* note 348 and accompanying text.

[374] Layton and Elaluf Calderwood, *supra* note 23, at 28-32.

[375] *See supra* notes 184 and accompanying text.

[376] *See* "One Year In", *supra* note 49.

[377] *See supra* notes 125 - 129 and accompanying text (discussing the United Nations current LDC criteria and list).

[378] *See supra* notes 122 and 186, and accompanying text.

zero-rating practice, making it an appropriate, and thus proportional, measure under the circumstances. This argument is premised on an acceptance that the Internet.org/Free Basics platform increases access among the digitally disenfranchised in Zambia, and benefits them in meaningfully relevant ways, despite not immediately offering the full Internet to everyone who subscribes. On this view, some Internet, with the possibility of more Internet, is still better than no Internet at all, at least for the time being.[379] Both hard and soft barriers to connectivity are surmounted, as both the numbers of users and their online experience increase.[380] Facebook's efforts to optimize the openness of the platform have also lessened the negative impact of curtailing net neutrality. And, crucially, an advocate claiming that Internet.org/Free Basics is a proportional restriction on net neutrality in Zambia can credibly argue that no better, less intrusive alternatives to that type of compound zero-rated platform currently exist. If these premises hold, the pro-human rights argument in support of Internet.org/Free Basics in Zambia, and other developing countries like it, is incontrovertible.

III.D. Zero-Rating in Context

The foregoing sections underscore the importance of evaluating net neutrality and its zero-rated exceptions in context. The situation in Zambia reflects one pole of the human rights spectrum of analysis because it qualifies as a "Least Developed Country" with high barriers to connectivity. For the reasons discussed above, Zambia is most likely complying more effectively with its international human rights obligations by *permitting* zero-rating practices that it would be by *banning* them. On the other end of that spectrum are developed countries like the Netherlands and the United States, which ban and partially allow zero-rating, respectively. In those countries, both home and mobile Internet access is affordable and ubiquitous.[381] Net

[379] This is not an uncommon view in developing countries. *See* Hill, Liezel and Martinez, Andrés R., "Kenya Says That Access Trumps 'First World' Problem of Net Neutrality", *Bloomberg*, February 24, 2016. Available at: http://bloom.bg/1nOJCCc [https://perma.cc/CU6Y-EZ7X].

[380] The Kenyan Minister of Information, Communications and Technology Joe Mucheru observes that "people who don't have any access to the Internet often don't understand its value. Access to services like Free Basics brings that awareness, and they're often then willing to pay to get access to more tools and information." *Id.*

[381] *See supra* notes 232 - 248 and accompanying text; *see also* Mayer, David, "Dutch and Slovenian Regulators Nail Carriers Over Net Neutrality", *Gigaom*, January 27, 2015, Available at: http://bit.ly/1EfQqPn [https://perma.cc/B2U2-HMXQ].

neutrality protections are strong, and exceptions narrowly defined, at least in the case of the Netherlands.[382] In that country, there are few barriers to connectivity as a practical matter, so any rationale to support imposing restrictions on net neutrality must be grounded in some *other* aim recognizable as legitimate, in addition to the requirement that the means be necessary and proportionate to achieve that legitimate aim. Thus, for example, reasonable measures for Internet traffic management that impinge on net neutrality are nonetheless accepted (like in most countries) as a justified because they are necessary, proportionate, and limited in time.[383] In short, the Netherlands is most likely complying more effectively with its international human rights obligations by *prohibiting* zero-rating than by *permitting* it.

Still unclear is how the United States' new rules allowing for "sponsored data" will be interpreted by the FCC.[384] When is a sponsored data or zero-rated plan not based on "unfair" or "unreasonable" discrimination in contravention of net neutrality? Past FCC practice supports the claim made by some experts that limited exceptions to pricing controls with clear public interest or consumer benefits may survive the FCC's case-by-case scrutiny where little or no negative impact on competition or consumer choice is perceived.[385] A different question is whether they would survive a human rights analysis.[386]

Then there is the middle ground between the two poles. States like Slovenia and Chile, which manifest features of both developing and developed countries, make for harder cases.[387] Here, the analysis required by international human rights law is more complicated because, among other

[382] *See* Rossini Public Knowledge Report, *supra* note 23 at 35.

[383] *See* "Council of Europe gets tough on net neutrality", *supra* note 20.

[384] *See supra* note 244 and accompanying text. To date, complaints have been brought or threatened against sponsored data plans by Comcast (Stream TV), Verizon (FreeBee), and T-Mobile (Binge On), among others. *See* Daniel A. Lyons, Daniel A., "Usage-Based Pricing, Zero-Rating, and the Future of Broadband Innovation", *Free State Foundation Perspectives* 11, Nº 1, Boston College Law School Faculty Papers, January 4, 2016, available at: http://bit.ly/2eYJKjf (arguing that the FCC should not interpret its net neutrality protections too narrowly in relation to innovative practices involving zero-rating that benefit consumer choice but do not result in anti-competitive harm).

[385] *See supra* note 68 and accompanying text. Veteran U.S. communications law experts repeatedly point to the FCC's allowance for toll free numbers as an example of how the public interest can successfully drive policy exceptions to telecommunication pricing rules. Toll free numbers are frequently paid for by sponsoring companies to allow consumers to communicate for "free" with businesses. *See* Federal Communications Commission, "What is a Toll Free Number and How Does it Work?", November 3, 2015, available at: http://fcc.us/2fKCTJg [https://perma.cc/5SBN-8ZC2].

[386] *See* Carrillo & Nunziato, *supra* note 232.

[387] *See supra* Part I.B.

reasons, the factors to balance tend to even out. For example, Chile enjoys relatively high levels of Internet access and affordability leading to substantial penetration rates, though not as high as those in developed countries like the Netherlands, which bans zero-rating more categorically.[388] Some barriers to connectivity remain, though they are lower than those found in most developing countries. Even so, inequality levels in Chile are high, and significant sectors of its society remain unconnected.[389] The telecoms sector is privatized and highly competitive, expanding consumer choices. It is thus difficult to say whether zero-rating practices, to the extent they are being permitted in Chile, could be justifiable under the human rights regime without looking at them on a case-by-case basis in light of the framework outlined above. The point here is not to offer a definitive statement of Chile's (or any other country's) compliance with its human rights obligations. Rather, the idea is to illustrate how a more rigorous analytical framework can be applied to such policy questions to enhance their constructive consideration. This "new" perspective on net neutrality and zero-rating similarly lays the groundwork for deeper normative research and consideration of these issues.

Conclusion: Having Your Cake and Eating It Too

It turns out that, under certain circumstances, zero-rating can be compatible with net neutrality understood as a norm of human rights. In other words: sometimes, you *can* have your cake and eat it too. But that normative reality does not, in itself, respond to the underlying question of *when* the requisite conditions are met in a given country, or by *which* particular zero-rating arrangements, so as to justify the practice in this way. For that, one must engage with the human rights law framework as outlined and developed above. In the Introduction, I invoked the contentious net neutrality debates in India during 2015 to illustrate the zero-rating conundrum in action. Despite some progress, India continues to be an ideal case study of the challenges involved in regulating net neutrality effectively.

The initial question provocatively posed in the Introduction was whether Facebook in India could "have its cake and eat it too" by promoting its zero-rated Internet.org/Free Basics platform while simultaneously holding itself out as a champion of net neutrality. India's regulator decided in February 2016 that it could not by banning all differential pricing by telecoms, thereby

[388] *See supra* note 110 and accompanying text.
[389] *See supra* Part I.B.III.B. (Chile country case study).

pulling the plug on Internet.org/Free Basics and similar offerings.[390] Surprisingly, however, the Indian regulator soon thereafter executed an embarrassing "flip-flop" by issuing two new net neutrality-related consultations,[391] which advocates believe threaten to reintroduce zero-rating "through the back door."[392] If nothing else, this "confused" approach to regulating net neutrality in general, and zero-rating in particular, confirms that the question of what arrangements might constitute acceptable restrictions on net neutrality in the Indian context has yet to be decided.[393] It also means that India continues to struggle with the zero-rating conundrum.

A better way of reformulating the initial question posed is whether India, in deciding to prohibit differential pricing and private sector zero-rating, is maximizing the enjoyment by its people of basic human rights like freedom of expression, and thus adequately complying with its international human rights obligations. Based on the international law framework outlined in prior Parts and India's yawning digital divide,[394] the answer is probably no. This "new" perspective supports the position that by reframing the debate on net neutrality in human rights terms, regulators and advocates in India and elsewhere would gain a more consistent and comprehensive approach to evaluating the issues. This, in turn, would foster more constructive debates and, ultimately, better policymaking. The Indian regulators recent *volte-face* might just signal an opportunity to reevaluate its position in those terms.

390 *See supra* note 21 and accompanying text.

391 Kasuhik, Manu, "TRAI's Web of Confusion", Business Today, July 31, 2016. Available at: http://bit.ly/2gdkNOR [https://perma.cc/4L5P-T3X5].

392 Singh, Parminder Jeet, "Free Basics, Through the Back Door", *The Hindu*, July 5, 2016. Available at: https://perma.cc/35QB-2Z22.

393 Kasuhik, *supra* note 390.

394 . *See supra* note 123 (Table 2). In India, less than 20% of the population has Internet access of any kind. *Id.*

Chapter Five

Europe's "Right to Be Forgotten" in Latin America

Daphne Keller[1]

Executive Summary

This article addresses tensions between the so-called "Right to Be Forgotten" (RTBF) and Internet users' free expression and information rights, particularly as those rights are recognized in Latin America. It reviews troubling developments based on two European legal sources: the Court of Justice of the European Union's (CJEU) 2014 *Google Spain*[2] case, which required the search engine to delist certain search results, and the EU's pending General Data Protection Regulation (GDPR).

The GDPR is a once-in-a-generation overhaul of EU Data Protection law. It will come into effect and displace previous Data Protection Law in 2018. Its new RTBF provisions tilt the playing field strongly in favor of erasing online speech, creating a serious imbalance between expression and privacy rights.

---

[1] Daphne Keller is the Director of Intermediary Liability at the Stanford Center for Internet and Society. She was previously Associate General Counsel for Intermediary Liability and Free Speech issues at Google. In that role she focused primarily on legal and policy issues outside the U.S., including the E.U.'s evolving "Right to Be Forgotten." Her earlier roles at Google included leading the core legal teams for Web Search, Copyright, and Open Source Software. Daphne has taught Internet law as a Lecturer at U.C. Berkeley's School of Law, and has also taught courses at Berkeley's School of Information and at Duke Law School. Her extensive public speaking in her field includes testifying before the UK's Leveson Inquiry and Parliamentary Committee on Privacy and Injunctions. Daphne practiced in the Litigation group at Munger, Tolles & Olson and is a graduate of Yale Law School and Brown University.

[2] European Court of Justice, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD),* Case C-131/12, May 13, 2014, at para. 94, available at http://bit.ly/2fbElQH.

Latin American lawmakers and advocates have an opportunity to avoid this imbalance in their own laws. Indeed, there are strong arguments that the GDPR provisions could not pass legal and constitutional muster or comply with human rights commitments in the region. Lawmakers can robustly protect privacy and data protection rights without accepting the harm to speech from poorly designed RTBF laws.

The Article will (1) review the legal background of the RTBF in Europe, and its relationship to other notice and takedown regimes for online speech, (2) discuss the substantive and procedural restrictions to free expression under that law, with a focus on new provisions of the GDPR, and finally (3) identify important differences between relevant EU law and that of many Latin American countries.

The divergences between European and Latin American legal frameworks suggest the following possible approaches for policymakers grappling with RTBF proposals in legislation, litigation, or administrative enforcement:

- Not treating intermediaries as data controllers of speech posted by their users, or spelling out narrower controller obligations with respect to speech.
- Not emulating the removal process set forth in the GDPR, but instead drawing on intermediary liability law to identify any obligations and ensure procedural checks against over-removal.
- Vetting any RTBF proposals against Latin America's unique and pro-free-expression human rights framework.
- Vetting any RTBF proposals against existing legal rights grounded in privacy, defamation, or other sources of law, then identifying whether RTBF would support claims not already covered in those laws, whether those new claims are desirable as a policy matter, and what carefully tailored free expression protections should apply to them.

Introduction

Recent European legal developments in the so-called Right to Be Forgotten fit poorly with legal and human rights frameworks in Latin America. These developments may be of particular concern in the many Latin American countries whose laws track the EU's 1995 Data Protection Directive – the law applied in *Google Spain*.[3] While that case applied only to search

[3] In 2012 this list included Argentina, Uruguay, Mexico, Perú, Costa Rica and Colombia. Leiva, Aldo M., "Data Protection Law in Spain and Latin America: Survey of Legal Approaches", *American Bar Association International Law News*, Vol. 41, No. 4, 2012, available at http://bit.ly/XJ9xyA. In 2016, laws in some 14 countries in Latin America

engines, follow-on cases in the EU seek to apply the same requirement to Internet hosts, such as Facebook. Latin American lawmakers will need to decide similar questions under their own laws. The high level questions arising from these developments will be relevant in every country where lawmakers struggle to reconcile rights to privacy and free expression in online communications.

My own understanding of this issue arises both from my current work at Stanford and from my background as an attorney for Google In 2014, I traveled with the Advisory Council to Google on the Right to Be Forgotten, and heard analysis from both the independent experts who made up that Council and the numerous distinguished speakers who testified at its public meetings.[4] I do not pretend to be an expert in Latin American law. But even a beginner's review of case law and human rights instruments there suggests that the RTBF as it has evolved in Europe would be a poor fit. My hope is that this analysis will be helpful to the region's many remarkable advocates for human rights as national debates about RTBF play out.

I. Discussion

I.A. Legal Origins of the "Right to Be Forgotten" Online

The so-called "Right to Be Forgotten" has longstanding antecedents in European law, for example under German laws designed to help rehabilitated criminals. What was new with the *Google Spain* ruling was the firm grounding of such a right in the EU's broad and powerful Data Protection Directive[5]. The right articulated in that case – to compel search engines to delist certain results for certain search queries – is, many argue, itself no more than a "Right to Be Delisted." It does not compel deletion of web pages or archival materials, and it certainly cannot control human memory. By this reasoning, the RTBF moniker is a misnomer. Nonetheless, the RTBF

and the Caribbean offered some form of Data Protection. Rich, Cynthia, "Data Privacy Laws in the Western Hemisphere (Latin America, Caribbean and Canada)", *Bloomberg BNA - World Data Protection Report*, Vol. 16, No. 6, June 2016, available at http://bit.ly/2fjXULC; there are economic and other reasons to emulate EU law, as the simplest means to be deemed "adequate" for data transfers to national companies doing business in the EU. Cerda Silva, Alberto, "Personal Data Protection and Online Services in Latin America", available at http://bit.ly/2fjY7y9.

[4] Google Advisory Council, *"The Advisory Council to Google on the Right to be Forgotten"*, Final Report, February 2015, available at: http://bit.ly/1r2Vv7e.

[5] Data Protection Directive, available at: http://bit.ly/1f9oJZ7.

terminology has resonated and been repeated around the world, taking on a life of its own beyond the EU legal context.

In Latin America, new cases and legislative proposals advancing RTBF have moved rapidly in the wake of the *Google Spain* case. In some cases, national law already recognizes rights to suppress certain information about one's past, for example in financial or criminal matters.[6] Colombia's Supreme Court in 2015 delivered a nuanced ruling, putting RTBF responsibilities on a web publisher rather than search engines, rooted in part in media law and criminal law.[7] Moreover, many countries' constitutions include *habeas data* provisions, which some argue support rights similar to the EU RTBF.

Questions about the influence of EU law are particularly acute for the many Latin American countries – including Chile, Argentina, Uruguay, Mexico, Costa Rica, Peru, Nicaragua and Colombia - with laws directly modeled on the EU's Data Protection laws, and for countries like Brazil where similar laws have been proposed.[8] Legislatures have significant economic motivation to track EU law, in order to be deemed "adequate" for commercial and other transfer of data from the EU.[9] Latin American Data Protection laws typically include provisions very similar to the ones interpreted in the *Google Spain*, giving data subjects rights to access, rectify, cancel and object to processing of their personal data.[10] Provisions like these were applied by Mexico's Data Protection agency in 2015, in a RTBF order subsequently reversed by a court.[11]

---

[6] Derechos Digitales, "What are the implications of the right to be forgotten in the Americas?", September 2015, available at http://bit.ly/2eL0DNh; See also, Cerda Silva, *supra* note 3 ("For the Supreme Courts of Argentina and Costa Rica, processing personal data on paid debts infringes fundamental rights, whereas for the Supreme Court of El Salvador it does not").

[7] Derechos Digitales, *supra* note 6; *see also* Constitutional Court, "*On behalf of a minor vs. "El nuevo día" newspaper & Instituto Colombiano de Bienestar Familiar"*, Judgment T-453/13, July 15, 2013, available at http://bit.ly/2eAkRJ1 (newspaper, not search engine, liable for disclosing identity of allegedly abused minor); Constitutional Court, *"Martínez vs. Google Colombia & El Tiempo publishing house"*, Judgment T-040/13, January 28, 2013, available at http://bit.ly/1FylMlk (search engine not responsible for accessing, correcting, or deleting search results discussing plaintiff's past criminal process).

[8] Voss, W. Gregory and Castets-Renard, Céline, "Proposal for an International Taxonomy on the various forms of the 'Right to Be Forgotten': a Study on the Convergence of norms", *Colorado Technology Law Journal,* Vol 14, Nº 2, Colorado, University of Colorado Law School, 2016, p. 314.

[9] *See*, Cerda Silva, *supra* note 3. Adequacy determinations made by the European Commission under the 1995 Directive will remain in effect, but could be challenged or revoked in the future under the GDPR. See discussion at http://bit.ly/1FylMlk.

10 Voss and Castets-Renard, *supra* note 8.

[11] *See* http://eleconomista.com.mx/tecnociencia/2016/08/24/anulan-resolucion-inai-sobre-derecho-olvido.

At the same time, some aspects of Latin American law and culture diverge widely from an EU-style RTBF. Eduardo Bertoni, who now heads the Argentine Data Protection agency, called the RTBF moniker "offensive" and wrote that if such a law allowed perpetrators of human rights violations to achieve delisting from Google, it would be "an enormous insult to our history (to put it lightly)."[12] As one Mexican data protection expert put it, "we cannot understand the right to be forgotten as it has been understood by the ECJ because of cultural divides."[13] This divide was already evident in some pre- *Google Spain* case law. For example, in 2013 the Colombian Constitutional Court twice rejected RTBF-like claims against Google.[14]

The region also has powerful case law and legislation protecting the online free expression rights of Internet users, in ways that set it apart from the EU. Implementation of these rights has been inconsistent and in too many cases fallen victim to political corruption, but the intellectual and legal framework remains robust.[15] Brazil's Marco Civil establishes that platforms in most cases need only remove user-generated content if a court has adjudicated it unlawful, and states that this rule is necessary "in order to ensure freedom of expression and to prevent censorship."[16] Chile's Intellectual Property law, too, requires removal only pursuant to court orders.[17] Argentina's Supreme Court arrived at a similar conclusion, reasoning from first principles and constitutional rights. In the landmark *Belen Rodriguez* case, it rejected strict liability, instead predicating intermediary liability on actual knowledge of unlawful content. In dicta, it said that platforms should remove online speech only after adjudication by a competent public authority.[18]

---

[12] Bertoni, Eduardo. "The Right to Be Forgotten: An Insult to Latin American History", *The Huffington Post*, 24th September, 2014, available at http://huff.to/1ucd9pk.

[13] Carson, Angelique. "The Responsibility of Operationalizing the Right To Be Forgotten", The International Association of Privacy Professionals (IAPP), March 12, 2015, available at http://bit.ly/2ek4eRB, quoting Mexican attorney Rosa Maria Franco Velázquez. In striking contrast, the head of Spain's DPA said the RTBF "does not affect the right to know."

[14] Corte Constitucional de Colombia, *supra* note 7.

[15] Some experts have even seen backsliding in recent Inter American Court rulings. *See* http://bit.ly/2hJlGxC.

[16] Federal Law Nº 12.965, April 23, 2014, available in English at http://bit.ly/1gubZiQ.

[17] Law Nº 20.435, May 4, 2010, Art. 85, available at: http://bcn.cl/nol; Chile's Supreme Court also upheld an appellate ruling limiting Internet platforms' obligations to remove allegedly defamatory content, also on grounds of free expression. Supreme Court, "*Suazo vs Reclamos.cl*", 07/06/09. Available at http://bit.ly/2f2LoQT.

18 Corte Suprema de Argentina, "*Rodríguez M. Belen c/Google y Otro s/ daños y perjuicios"*, Judgment R.522.XLIX, 10/28/14. Available at: http://bit.ly/2f2LoQT; India's Supreme Court reached a comparable outcome in "*Shreya Singhal v. Union of India"*, Nº. 167/2012, Criminal Judgment 03/24/15.

This widespread embrace of a court order requirement for Internet content removal stands in contrast to European case law. Most EU countries have consistently accepted notice from interested individuals, without judicial oversight, as an adequate basis for removal of online speech. A partial exception is Spain: Spanish legislation initially required court orders, but the Spanish Supreme Court struck this standard down as inconsistent with the EU-wide eCommerce Directive.[19] A lower court subsequently held that considerations of free expression nonetheless mandated a court order standard, except for legal violations that are "unquestionable, manifest and beyond doubt."[20]

Latin America's special concern for free expression rights is grounded in the region's human rights instruments. Article 13.3 of the American Convention on Human Rights seems to foresee intermediary liability issues of today, saying

The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.[21]

This concern for indirect censorship and private controls is squarely on point for laws that, like *Google Spain*, effectively assign RTBF adjudication to private companies. So, too, are Article 8's guarantee of "competent, independent, and impartial tribunal, previously established by law," and the due process element of the Inter American Court's three-part test for content restrictions.[22]

The Organization of American States' Declaration of Principles on Freedom of Expression is also relevant. It says,

> Privacy laws should not inhibit or restrict investigation and dissemination of information of public interest. The protection of a person's

[19] Tribunal Supremo de Madrid, Sala en lo Civil, "*Asociación de Internautas",* Judgment Nº 773/2009, 11/10/09. Available at http://bit.ly/2f76g8H, discussed at http://bit.ly/2fscOQA.

20 Barcelona appellate court, "*Royo v Google*", Judgment 76/2013, February 13, 2013; a line of UK cases wrangled with the same question, but in many cases addresses it under domestic defamation law rather than eCommerce Intermediary Liability standards. Nonetheless one case, "*Davison v Habeeb",* England and Wales High Court (Queen's Bench Division), November 25, 2011, held that a mere allegation that a user's post was defamatory did not establish knowledge or removal obligation for a blog host.

[21] American Convention on Human Rights, "Pact of San Jose, Costa Rica", available at: http://bit.ly/1Ac82L9.

[22] *See*, Joint Declaration on Freedom of Expression and Responses to Conflict Situations. Available at: http://bit.ly/2gD6F4J

> reputation should only be guaranteed through civil sanctions in those cases in which the person offended is a public official, a public person or a private person who has voluntarily become involved in matters of public interest. In addition, in these cases, it must be proven that in disseminating the news, the social communicator had the specific intent to inflict harm, was fully aware that false news was disseminated, or acted with gross negligence in efforts to determine the truth or falsity of such news.[23]

This framework for privacy-based limitations on speech will be important as signatories of the convention confront RTBF legal proposals.[24]

I.B. Overview of Relevant Data Protection Law

The right established in the EU's 1995 Data Protection Directive, and in many Latin American laws, is distinct from pre-existing privacy rights. It is a broad right to limit processing of all information relating to oneself, not just information that causes harm or invades personal privacy. The EU's Directive sets forth the detailed legal and administrative framework for protecting this right, including specific legal grounds for regulated entities to process personal data about individuals. Where these grounds are not met, processing is unlawful.

Entities that process personal data are generally classified as either controllers or processors. Controllers are, roughly speaking, entities that hold personal data and decide what to do with it. Because they are the decision-makers, they have more obligations under the law – potentially including compliance with erasure or "Right to Be Forgotten" requirements. Processors hold personal data, but follow instructions from a controller about what to do with it. Their legal duties are correspondingly fewer. In a simple example, a firm that holds records about its employees is a controller of their personal information; if it outsources payroll operations under contract with a payroll company, that company is a processor. The CJEU's determination that Google acted as a controller with respect to information indexed in its web search service was a key holding of *Google Spain*.[25]

[23] Principle 10. Available at http://bit.ly/15lje4M

[24] Because privacy rights predate data protection rights in most legal instruments, there are important questions whether older discussions of privacy apply to both. In this case, the answer seems to be yes.

[25] *Id.* at para 82, 85-88.

The CJEU's ruling left open the critical question of the status of other important OSPs, including hosts such as Twitter or YouTube. If those intermediaries, too, are controllers, then the scope of potential Internet speech suppression under the RTBF is significantly broader. There are some strong arguments against this outcome – for example, that hosts cannot be controllers because they only process content at the direction of a user, who is herself the controller. The few cases to date have reached inconsistent results on this question.[26] Free expression-based arguments against RTBF obligations for hosts are also potentially stronger than for search engines, because removing information from a hosting service may eliminate it entirely from the Internet – sometimes leaving even the author with no copy of her work, as occurred with one author's Blogger account in 2016. [27]

I.C. Intermediary Liability Law

The law of intermediary liability limits and defines the legal responsibility of technical intermediaries for content posted online by third parties.[28] Intermediary liability in the EU is governed by Articles 12-15 of the eCommerce Directive,[29] as implemented in the national laws of Member States. Protected intermediaries can range from Internet access providers like Telefonica to social media hosts like Twitter to search indexes like Google, and more.

Under most intermediary liability laws, platforms have no obligations to police user speech, and no liability for unlawful user content they are unaware of. In some legal systems, even knowledge of tortious user expression, including expression adjudicated as unlawful by a court, does not create any legal obligations for the intermediary. The US Communications Decency

[26] Compare "*CG v Facebook Ireland Ltd & Anor*", High Court of Justice in Northern Ireland (Queen's Bench Division), 20 February, 2015, available at http://bit.ly/1f9oJZ7 (Facebook is controller) and Spanish Blogger case, 2015. Available at http://bit.ly/2fezYoK (blog hosting platform is not a controller).

[27] In 2016 an artist reported that Google had deleted 14 years of his work, including his only copies of some, by taking down content he had posted to the company's Blogger service. See "Google's deleted an artist's blog, along with 14 years of his work", *Science alert*, July 18, 2016, available at: http://bit.ly/2aw3Hfw

[28] Latin American laws are discussed above. In the US, key intermediary liability laws are the DMCA 17 USC 512, available at http://bit.ly/24wrfDr and CDA 230 47 USC 230, available at: http://bit.ly/1hlnlbP

[29] European Parliament and of the Council of the EU, Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), June 8, 2000, available at: http://bit.ly/2faazhi

Act Section 230 works this way, and has been credited with facilitating the tremendous economic and technological boom of US tech companies over the past two decades – and with avoiding suppression of lawful speech by cautious or risk-averse intermediaries. In many other countries, removal obligations exist but are limited to protect rights of Internet users.

Many laws, including the EU eCommerce Directive, treat knowledge as a trigger for intermediary action: once the intermediary is aware of unlawful content, it must take it down or face liability itself. Speech platforms typically operate notice and takedown systems to remove user content under these laws. In principle, intermediaries should only remove user content if the legal allegation in the notice is correct and the content actually is illegal. In practice, notice and takedown processes are widely misused to target lawful content, and multiple studies confirm that intermediaries often simply acquiesce to removal requests, including improper ones.[30] Some companies do put real effort and resources into identifying and rejecting unfounded removal requests. I am proud to say that I was part of this effort at Google. But both anecdotal and statistical evidence tell us that such efforts, alone, are often not enough. Information improperly targeted for removal under notice and takedown systems ranges from religious,[31] political,[32] and scientific[33] content to consumer reviews.[34]

The numbers behind this issue are significant. Intermediaries receive a *lot* of bogus removal requests. In the «Right to Be Forgotten» context, Google says that has been asked to delist 1.6 million webpages, and that around 57% of these requests fail to state valid legal claims even under the EU's expansive RTBF law.[35] Microsoft's Bing search engine also reports that over half of the RTBF requests it gets are groundless.[36] Privacy regulators seem to agree: a review of cases brought to national authorities concluded that "in the great majority of cases the refusal by a search engine

[30] *See* list, available at http://stanford.io/2fBMNhk.

[31] Galperin, Eva, "Massive Takedown of Anti-Scientology Videos on YouTube", Electronic Frontier Foundation, September 5, 2008, available at: http://bit.ly/2eRFGzP.

[32] Rodriguez, Salvador, "Russia, Turkey Asked Twitter To Remove Hundreds Of Tweets As Government Censorship Attempts Skyrocket", *International Business Times*, September 2, 2015, available at: http://bit.ly/2fsi7zP

[33] Timmer, John, "Site plagiarizes blog posts, then files DMCA takedown on originals", *Ars Technica*, February 5, 2013, available at: http://bit.ly/2ekn5Ms.

[34] Lee, Timothy B., "Criticism and takedown: how review sites can defend free speech", *Ars Technica*, June 1, 2011, available at: http://bit.ly/2dZl1tg

[35] Google, "European privacy requests for search removals", available at: http://bit.ly/1FdZMGD

[36] Microsoft, "Content Removal Requests Report", available at: http://bit.ly/2faRmwc

to accede to the request is justified."[37]

To counteract the over-removal problem, lawmakers and human rights advocates around the world have developed procedural rules for notice and takedown. Such rules, including penalties for bad-faith notices and opportunities for accused speakers to "counter-notice," are intended to act as a check on over-removal. The Manila Principles, a widely-endorsed "gold standard" for intermediary liability, lists numerous other procedural tools including notice formalities and transparency requirements.[38] This Article will explore the issue of procedural protections for online speech in as they arise in the RTBF context in Section II.B.

I.D. The Collision of Data Protection and Intermediary Liability Issues in the RTBF

Historically, few lawyers have drawn a connection between data protection and the law of intermediary liability. In European practice, the two fields use very different vocabularies, and are for the most part interpreted, enforced and litigated by different practitioners.

The CJEU's 2014 "Right to Be Forgotten" ruling in *Google Spain* changed that.[39] The court determined that Google was a controller of information in search results, with corresponding obligations to curtail processing of that data upon request. The remedy ordered by the court was not complete erasure of the information, either from search results or from Google's underlying indexing infrastructure. Rather, the search engine was required to de-list results only when users searched for the plaintiff's name.[40] The court prescribed what is effectively a notice and takedown system to remove search results, but arrived at this remedy through the language and logic of data protection – with no reference to Europe's intermediary liability rules. *Google Spain* follow-on cases will likely force lower courts to grapple more directly with questions about how the two areas of law fit together.

In 2018, however, the entire framework of Data Protection law underlying *Google Spain* will be replaced by the GDPR. For the first time, the law will mandate specific steps for erasing personal data, including in the RTBF context. It also authorizes extremely high fines - 4% of annual

[37] European Commission Press Release Issued by the Article 29 Data Protection Working Party, Bruselas, June 18, 2015. Available at http://bit.ly/1OoWVnP

[38] Manila Principles, https://www.manilaprinciples.org/

[39] European Court of Justice, *supra* note 2.

[40] European Court of Justice, *supra* note 2, at para. 94.

global turnover or €20 million – against controllers who fail to comply. [41] This financial exposure, combined with legal provisions that are ambiguous at best or highly pro-erasure at worst, makes the GDPR a bigger threat to online speech than the current EU law under *Google Spain*.

The mismatch between Data Protection and notice and takedown systems arises in large part from conflating "back-end," privately stored" user data and publically available speech. Data Protection law was created and evolved largely as a system of rules for back-end data processing – the things your bank, doctor, or health club might do with personal information they hold in their files, for example. For intermediaries, back-end processing includes things like tracking users' online behavior in storage systems such as logs, profiles, or accounts. Data Protection law rightly applies to this kind of data, and provides individuals with access and erasure rights – regardless of whether the company also happens to be an intermediary platform for user generated content. A human-rights-based analysis of erasure requests for back-end data is relatively straightforward. Only two sets of rights are implicated: those of the requesting data subject, and those of the company. Presumably the requester's data protection rights will prevail in most cases. Data protection rules under both the 1995 Directive and the GDPR are broadly reasonable for this two-party situation. Because of the law's historical focus on this scenario, however, the data protection legal framework has few rules and little precedent for addressing public online speech -- the very different data at issue under the RTBF. [42]

Requests for intermediaries to erase *another person's* online expression are very different from a human rights perspective. They affect at least four parties: the requesting data subject; the intermediary; the person who posted the content online; and other Internet users who want to view it. Procedures designed for back-end data deletion and a two-party interaction are not adequate to protect and balance the rights of these four very different parties. When they are applied to online speech, rights to free expression suffer.

II. Free Expression Issues Raised by the RTBF

Human rights lawyers' concerns about RTBF and free expression broadly fall into two categories. The first concerns the substantive right: should

[41] GDPR Art. 83.

[42] One exception is Opinion 1/2008 on Data Protection issues related to search engines - WP 148 (04.04.2008) (distinguishing back-end "user data" from indexed "content data"), p.14. Available at: http://bit.ly/2eo8Ohx

people be able to suppress truthful information about their past, and if so, what limits should be placed on the right? The second is procedural: if a RTBF exists, who should adjudicate its application, and under what rules? In the *Google Spain* ruling and GDPR, EU lawmakers arrived at troubling answers to both of these questions – answers that stand in considerable tension with Latin American legal protections.

II.A. Free Expression and the Substantive Scope of the RTBF

As Eduardo Bertoni has said, the RTBF is a Rorschach test. People project a wide array of meanings onto it. Many of those involve harms already addressed in existing laws governing defamation or other dignitary and reputational harms. Those laws, in Joris van Hoboken's words, "entail intricate doctrines to balance the interests in society in the publicity of and about others and the interests of privacy and dignity of natural persons.[43] For the RTBF, however, those elaborate doctrines, limitations, and defenses do not yet exist. Lawmakers – or Google – are left to reinvent them.

The *Google Spain* court said that Google should remove data that is inaccurate[44] or "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing."[45] This includes truthful information[46] and information that causes no prejudice to the person seeking removal.[47] The Court identified one exception:

> when it appears, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.[48]

The Court did not expand on this public interest balancing test. However, it noted that "as a rule" the public's interest in information does not outweigh

[43] Van Hoboken, Joris, "The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment", Report for the European Commission, Amsterdam, May 2013, at 23. Available at: http://bit.ly/LrCKYE

[44] European Court of Justice, *supra* note 2, para. 92.

[45] *Id.* at para. 94 (paraphrasing Directive Article 6.1(c)).

[46] *Id.* at para. 92.

[47] *Id.* at para. 96.

[48] *Id.* at para. 97.

the data subject's rights to erasure.[49] In an omission that is striking to many human rights advocates, the Court did not identify or discuss the other affected free expression rights: those of the webmaster or publisher.[50] The ruling was widely criticized both for setting a vague standard and for elevating data protection rights above information access rights, rather than weighing them equally. As former UN Special Rapporteur for Freedom of Expression Frank La Rue, a Guatemalan human rights attorney by training, explained:

> The right to privacy and to data protection is a fundamental right intimately linked to the exercise of the right to freedom of expression, and they should be understood as complementary and never in conflict with each other. The right to be forgotten, as such, does not exist… The decision of any authority to delete information or to block search engines can only be based in the fact that the form of obtaining such information or the content of such is malicious, is false, or produces serious harm to an individual.[51]

La Rue's formulation draws on important substantive limits in pre-*Google Spain* law – and in the Inter-American Convention -- protecting speech that is not malicious, false, or harmful. This approach stands in striking contrast to the CJEU's expansive standard, which allows deletion of truthful and non-prejudicial information.

La Rue also linked RTBF law to issues of political violence and human rights abuses.

> In the case of human rights, one of the fundamental principles to eradicate impunity is to establish the truth of human rights violations when they exist, and this is recognized as the right to truth of the victims and their families but also to society as a whole to reconstruct historical memory, to memorialize the victims of the past.

Despite concerns raised by La Rue and others, new RTBF provisions under the GDPR do little to improve on the CJEU's guidance. The law ex-

[49] *Id.*

[50] *See* Peguera, Miquel, "The Shaky Ground of the Right to be Delisted", on: *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 18, Nº 3, 2016, p. 555. Available at: http://bit.ly/2ghbOMB. Because the CJEU does not accept amicus or intervener briefs, and the newspaper that published Mr. Costeja's information could not be a party. No one before the court directly represented those interests.

[51] Google Advisory Council, *supra* note 4.

cuses controllers from erasing information needed "for exercising the right of freedom of expression and information."[52] But it defers to EU Member State law to define what those rights actually are, and how to balance them with data protection rights.[53] EU Member States have already had this obligation for two decades under the 1995 Directive, and many have failed to fulfill it.[54] Some countries have never passed the required legislation at all, others have enacted laws that fall far short of the goal of balancing expression and privacy rights.[55]

In addition, some GDPR protections extend only to journalistic, artistic, academic or literary expression. This formulation is not unique to EU law, but it is a problem for democratic participation in online speech. Most Internet users lack the credentials to qualify for these limited exemptions. Important content left unprotected under this standard could include consumer reviews of dangerous business practices and first person accounts of abuse by family members or people in positions of power.[56]

More problems arise from institutional imbalance in government support for data protection rights and free expression rights under the GDPR. A person asserting data protection rights has an audience and presumptive ally in the DPA, which can provide inexpensive and efficient enforcement for valid claims. By contrast, the legal avenues available to a publisher or online speaker asserting free expression rights against RTBF removals under European law are scant. In most cases, her only recourse is to courts of law, where she can attempt to sue either the intermediary or the data subject who requested removal. Neither claim is likely to succeed – in most cases there is no clear cause of action against an individual whose false accusation led

[52] Art. 17.3. Notably, this provision does not change OSPs' obligations to immediately "restrict" content from public before assessing whether a free expression defense might apply. See Section II.B. below.

[53] Art. 85.

[54] *See* Erdos, David, "Fundamentally Off Balance: European Union Data Protection Law and Media Expression", Research paper Nº 42/2014, University of Cambridge, Faculty of Law, July 25, 2014. Available at: http://bit.ly/2fgRXfc

[55] *Id*, p. 11. "The laws of three countries (Croatia, Czech Republic and Spain) provide no media derogation at all from any part of the data protection scheme".

[56] The GDPR also importantly lacks clarity about *whose* free expression rights matter: the intermediary's or the user's. While most free expression advocates would identify the user as the most important rightsholder, EU caselaw – including the *Google Spain* ruling – has sometimes looked solely to the rights of defendant OSP. *See* Keller, Daphne, "Litigating platform liability in Europe: new Human Rights case law in the Real World", *The Center for Internet and Society Blog*, Stanford Law School, April 13, 2016, available at: http://stanford.io/2fFmxyG

an intermediary to remove content, or against the intermediary for taking that accusation at face value.

The GDPR's cumulative disadvantages to speech rights would be relatively harmless if data protection law still primarily applied to back-end data held and processed internally by companies. Applying the same rules to Internet users' public online expression, however, strips them of robust protection for their online participation and speech. Jurisdictions in Latin America can provide that protection, without compromising data protection or privacy rights under their own national law.

II.B. Procedural Protections For Free Expression and the RTBF

One important critique of the *Google Spain* ruling was that it effectively put decisions balancing European users' speech and privacy rights into the hands of foreign technology companies, instead of national courts. Of course, such decisions are already put in private hands under many existing Intermediary Liability laws. As discussed above, well-crafted notice and takedown laws can temper the risk to online expression by imposing procedural checks on over-removal. For example, Chile's Intellectual Property law establishes procedures to notify the accused infringer when someone asks to remove her content, and allow her to "counter-notify" to defend against the accusation.[57]

The CJEU's *Google Spain* decision did not prescribe any particular process for Google to follow in assessing and acting on RTBF claims. The Court did not reference Intermediary Liability laws under the eCommerce Directive, perhaps because it is widely assumed in the EU that those provisions do not cover data protection.[58] Subsequent opinions by data protection regulators have added modest procedural improvements, but nothing approaching the robust notice and takedown rules endorsed in many countries' Intermediary Liability laws.[59] The GDPR will introduce procedural rules that are considerably worse -- replacing existing uncertainty about notice and takedown processes for RTBF with a novel process that lacks even basic

[57] Law No. 20.435, May 4, 2010, amending Intellectual Property Law, Art. 85U.

[58] This complex point of EU law is discussed in my forthcoming article. Disputes stem in part from eCommerce Directive language stating that it does not apply to questions covered by the Data Protection Directive. Art. 1.5(b). *See* Data Protection Directive *supra* note 5.

[59] Article 29 Data Protection Working Party. "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12". Adopted on November 26, 2014. Available at: http://bit.ly/1rz3sgx.

procedural protections for online speech.

The GDPR, a comprehensive update and reform of the 1995 Data Protection Directive will come into force on May 25, 2018. Because it is a Regulation rather than a Directive, it will not have to be implemented as separate legislation in each member state of the EU. Rather, it will automatically go into effect. The GDPR covers a lot of ground, with provisions addressing everything from data transfer, to company codes of conduct and appointment of data protection officers.

The GDPR is riddled with ambiguities, including in the RTBF provisions. Some perpetuate existing, unresolved questions under the 1995 Directive. Others are new. We are unlikely to see expert consensus anytime soon about everything the GDPR means. On the upside, this creates openings for litigation and policy advocacy regarding the GDPR's impact on Internet intermediaries and user free expression. On the downside, it leaves Intermediaries with unclear instructions, coupled with powerful financial incentives to assume the most conservative interpretation of both substantive and procedural rules about RTBF removals.[60] Since only intermediaries – not the accused speakers – know about the request and can participate in DPA proceedings, this in turn reduces the chances for DPAs or courts to review improprieties and adopt interpretations more favorable to free expression.

The GDPR's notice and takedown rules must be derived from scattered sections throughout the document. Close evaluation shows a removal process like this. Considerably more detail about the GDPR process can be found in my forthcoming article, or in blog posts on the Stanford CIS website.[61]

1. An individual submits a removal request. There are no specific requirements for information the individual must provide to substantiate her request or confirm it does not conflict with the public interest.[62]
2. In most cases, prior to assessing the request's legal validity, the intermediary temporarily "restricts" the content so it is no longer publicly available.[63]

[60] Fines can mount to 4% of annual global turnover or €20 million. Art. 83.

[61] Keller, Daphne, "Series conclusion and summary: intermediaries and free expression under the GDPR, in brief", *The Center for Internet and Society Blog*, Stanford Law School, December 1, 2015, available at: http://stanford.io/2fFtX4U; *See also* the Spanish-language summary of final GDPR RTBF provisions: http://stanford.io/2fFogE7

[62] *See* generally Art. 17.1(c) and Art. 12.3-12.6. By contrast, Chile's Intellectual Property Law specifies formalities and required information for removal requests. *See* Law No. 20.435, *supra* note 57, Art. 85 Q.

[63] Art. 18.

3. The intermediary reviews the requester's legal claim to decide if it is valid. For difficult questions, the intermediary may be allowed to consult with the user who posted the content.[64] The GDPR identifies free expression rights as a factor in this decision, but adds no guidance on balancing these against data protection rights.[65]
4. For valid claims, the intermediary proceeds to "erase" the content.[66] There is no indication that this "erasure" can ever mean less than 100% deletion, although the *Google Spain* precedent would seem to support less drastic action. For invalid claims, the intermediary is supposed to bring the content out of "restriction" and reinstate it to public view. There are no apparent consequences if it doesn't reinstate the content.
5. The intermediary informs the requester of the outcome, and communicates the removal request to other controllers processing the same data.[67]
6. If the intermediary has information about the user who posted the now-removed content, it seemingly must disclose it to the individual who asked for the removal.[68]
7. In most cases, the accused publisher receives no notice that her content has been removed, and no opportunity to object. The GDPR text does not spell out this prohibition, but does nothing to change the legal basis for regulators' conclusions on this point in the *Google Spain* context.[69]

The deviation from standard notice and takedown processes here is significant, and dangerous for Internet users' expression and information-access rights.

One of the biggest issues with the GDPR process is Step 2: the immediate, temporary "restriction" of content from public view. There are arguments an intermediary could invoke to skip this step in special cases, but it is very unclear whether those arguments could prevail – and raising them would be an expensive risk for intermediaries.

The restriction provisions shift an important default: from a presumption that online expression is permitted until proven otherwise, to a presumption that its challenger is right. This conflicts with both standard legal protec-

[64] This authorization is not spelled out in the GDPR, but it re-uses language from the 1995 Data Protection Directive, which regulators have interpreted to establish these rules. *See* Article 29 Data Protection Working Party, *supra* note 59, p. 3, para. 9.

[65] Art. 17.3.

[66] Art. 17.1.

[67] Art. 17.2 and Art. 19.

[68] Art. 14.2(f) and 15.1(g).

[69] Article 29 Data Protection Working Party, *supra* note 59, p.3.

tions for free expression[70] and with our best knowledge about real-world RTBF requests - recall the 57% bogus notice rate reported by Google. An allegation made in secret to a private company should not have such drastic consequences. The GDPR's "restriction" requirement might make sense when applied to back-end data stored and used by companies. But where notice and takedown applies to third parties' online speech, that speech deserves far better protection.

The GDPR also creates considerable procedural unfairness in Step 6, in most cases preventing the user who posted the disputed content from knowing that it has been removed or delisted. Notice to the affected user is important to deter over-removal in the GDPR context, particularly for smaller intermediaries with scant legal resources. One of the main purposes of such notice is to let affected users correct the *intermediary's* errors, as well as the notifier's errors. Routinized notice puts the opportunity for error-correction in the hands of the person best motivated and equipped to use it: the content's publisher. Leaving the determination entirely in the hands of a technology company simply cannot substitute for involving the publisher as a mechanism to reduce improper removals.

From a pure data protection perspective, leaving the accused publisher out of the loop makes a sort of sense: if an individual has the right to make the company stop processing data about her, which should also preclude their talking to the publisher about it. This "when I say stop, I mean stop" reasoning may be sensible for stored, back-end data. But when the free expression rights of another individual are at stake, systematically depriving that individual of any opportunity to defend herself is a serious denial of fairness and due process.

Finally, the GDPR's seeming requirement that intermediaries disclose personal data about accused speakers is remarkable. It, too appears to be an artifact of rules intended for back-end data, listing Controllers' obligations when they receive data about an individual from someone else. Controllers must tell the data subject "from which source the personal data originate"[71] and "any available information as to their source."[72] The GDPR makes no reference to subpoenas or other forms of valid legal process for Controllers

[70] In a notable exception, a pre-Marco Civil Brazilian ruling held that a hosting platform must, within 24 hours of receiving a notice, temporarily remove user content pending legal analysis of the notifier's claim. Superior Court of Justice, Third Panel, Google Brazil, Special Appeal No. 1323754/RJ, August 28, 2012.

[71] 14.2(f).

[72] 15.1(g)

who receive data in the form of users' speech to protect those users' own private data.

Presumably, such an obligation will look as unreasonable to privacy regulators as it does to civil liberties advocates, and they will find some way to avoid it. Notably, Latin American lawmakers would face the same issue, under their existing data protection law, if they followed the *Google Spain* precedent and treated intermediaries as data controllers for users' speech. Laws in Chile, Colombia, and likely other countries requires controllers outside the journalistic context to disclose the source of personal data.[73]

III. Questions about the Google Spain ruling for non-EU countries considering RTBF laws

These developments in EU data protection law have ramifications for countries outside the EU. Questions about following in the footsteps of EU law will be intensified as the GDPR comes into effect.

From a human rights perspective, this is a complex question. On one hand, EU law has been admirably robust and innovative in protecting Internet users' privacy rights. There are good reasons that advocates might want to emulate many of its choices. On the other hand, the way the RTBF has played out in Europe gives far shorter shrift to speech rights than many other legal systems would do. And, simply as a matter of doctrine and blackletter law, EU developments were driven in part by rules unique to Europe, with no corollary in Latin America. Below is a list of considerations relevant to policy development outside the EU.

III.A. Does the *Google Spain* ruling compel identical interpretation of other countries' legislation that resembles the Data Protection Directive?

Of course, national courts will interpret their own national laws, and not assume that the CJEU ruling makes sense for their own countries. However, to the extent that EU precedent is relevant, it is important to recognize that the CJEU's interpretation was by no means a foregone conclusion, even under EU law. The CJEU's own Advocate General for the case, in fact, recommended

[73] *See* DLA Piper, "Data Protection Laws of the World", 2016, available at: http://bit.ly/2fvYkMx. Interestingly, a Chilean appeals court identified data protection law as a reason not to disclose online speakers' information in a case rejecting defamation liability for an Internet host. Supreme Court, *Suazo vs Reclamos.cl*, 6/07/09, *supra* note 17.

the opposite outcome: that Google was not acting as a controller, and that in any case the Data Protection Directive did not support a right to delete public information based on personal preference.[74] Numerous data protection specialists criticized the court's analysis in the aftermath of the case. Criticisms based on Free Expression concerns may be the most important grounds for other countries to choose a different course, from a human rights perspective. However, purely doctrinal critiques are also relevant for countries with EU-like laws. For example, classing an intermediary as a data controller is difficult to reconcile with some key obligations of controllers – obligations that are effectively impossible for intermediaries to meet. For example, controllers must get consent or other special authorization before processing data about someone else's health, ethnicity, sexual orientation or other "sensitive" attributes. For open speech platforms accepting users' statements about other people, this is effectively impossible.[75] Requirements to give data subjects notice prior to "collecting" data about him are also nonsensical when the "collection" consists of letting a user freely post expression online.[76]

These concerns could readily support the legal conclusion that intermediaries are *not* controllers of user-generated content. Alternatively, it could support the conclusion that they become controllers, and take on removal obligations, only after adequate and substantiated notice. The Italian Supreme Court reached exactly this conclusion in a pre-*Google Spain* case.[77] Framing the issue this way would protect important privacy values. It would preserve entirely Internet users' data protection rights regarding back-end tracking or profiling data. Moreover, it would permit lawmakers to apply their existing notice-and-takedown frameworks, including free expression protections, to users' online speech.

III.B. What is the "Right to Be Forgotten"?

As discussed above, the right adopted by the CJEU in Google Spain was a right to be delisted from certain web search results. Whether some version

[74] Opinion of Advocate General Jääskinen, European Court of Justice, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD),* Case C-131/12, May 13, 2014, para. 20, available at http://bit.ly/2fbElQH

[75] *See* discussion in Peguera, *supra* note 50.

[76] Several Latin American Data Protection laws, including Mexico, Colombia, and Argentina, have versions of this requirement. *See* DLA Piper, *supra* note 73.

[77] Italian Supreme Court of Cassation, "*Milan Public Prosecutor's Office v. Drummond*", Judgment Nº 5107/14, December 17, 2013, available at: http://bit.ly/2efrUYY, at para.7.4 (informal translation).

of this right applies to other sources of information, including the websites themselves, is very much an open question. Extending the right beyond search results would have serious consequences. As advocates consider RTBF proposals in other countries, clarity about the scope of online or offline speech affected by any such right will be critical.

III.C. Should intermediary liability law shape RTBF outcomes outside the EU?

The connection between conventional Intermediary Liability law and RTBF Notice and Takedown practice is conceptually simple. The free expression considerations are the same, from the affected online speaker's perspective, regardless of the legal framework that suppresses her speech. In Europe, however, a major legal barrier complicates this question. The eCommerce Directive, which governs all other aspects of EU Intermediary Liability, says "[t]his Directive shall not apply to (…) questions relating to information society services covered by" data protection law.[78] This leads many – though by no means all - EU lawyers to conclude that RTBF falls outside of ordinary notice and takedown rules. That carve-out, if it exists, is uniquely European. It should not preclude countries outside the EU from drawing on their own Intermediary Liability laws.

A more complex issue is whether controllers' duty to erase personal data is truly a form of "liability" for third party content, or instead their own independent obligation. However, this question, too, is subject to different laws and considerations in different countries. For jurisprudence that frames Intermediary Liability rules as a form of speech protection there is little reason to vary that protection depending on legal conceptions of "liability."

III.D. Is the CJEU's analysis of fundamental rights consistent with human rights obligations and constitutional law in my country?

The CJEU suggested that privacy or data protection rights should, "as a rule," trump the public's rights of access to information. This conclusion was widely criticized by EU lawyers, but stands as law for RTBF removals under *Google Spain*. This prioritization of privacy rights over speech rights is clearly incorrect in some other systems, including the

[78] eCommerce Directive, Article 5.1(b), *see* also Recital 14.

Inter-American system of human rights. That difference is relevant for both of the RTBF's free speech issues: the scope of the substantive right, and the procedural rules for Internet companies as adjudicators of online speech. Differences could also arise from the way national constitutions define and delineate rights. Data protection, as a right distinct from privacy, is a fundamental right under the EU Charter. Latin American practitioners in countries with constitutional *habeas data* rights,[79] and in countries that constitutionally protect only traditional privacy rights, will face important questions about balancing these rights under their own constitutional systems.

III.E. Does existing national law already protect privacy and dignity rights online?

Where existing law already gives people instruments to protect their privacy, reputation, dignity, or honor, or to prevent discrimination based on personal information, it is important to question what would be added by adopting a RTBF.[80] Adding a new, ill-defined RTBF, untethered from the nuanced claims and defenses in existing laws, may only muddy the waters and increase frivolous claims and over-removal of online content.

If lawmakers do see shortcomings in existing law, it can be remedied with more tailored laws incorporating protections for free expression – without invoking the blunt instrument of EU-style RTBF laws.

III.F. Does the EU already apply its Data Protection law to online expression in my country anyway?

In the *Google Spain* case, one of the key rulings was jurisdictional – that EU law applied to data processing carried out outside of Europe by the American Google parent company, because of connections between web search and advertising sales carried out by the local subsidiary. Many experts believe the 1995 Directive also applies to foreign companies on other grounds.

[79] These include, with some variation, Argentina, Brazil, Colombia, Mexico, Peru, and Venezuela. Cerda Silva, *supra* note 3.

[80] Notably, in the wake of the *Google Spain* ruling, many existing claims to intermediaries and courts making claims under defamation of or other sources of law were refiled as data protection claims. Hurst, Ashley. "Data Privacy and Intermediary Liability: Striking a balance between privacy, reputation, innovation and freedom of expression", part 1. Available at: http://bit.ly/2fxRXXu. (Noting that using data protection claims in lieu of privacy or defamation avoids "lengthy debate about such terms as "reasonable expectation of privacy" and gives plaintiffs "a potential short cut")

Whatever the answer is under that law, the GDPR clearly expands extra-territorial application to Internet companies around the world – including both processors and controllers- as long as they "monitor" EU users.[81] "Monitoring" seems to encompass online accounts and standard web and app customization features, so the law reaches many online companies outside of the EU. In addition, regulators have asserted that these companies must delete content globally – including in countries where that content is protected by free expression laws. This assertion of jurisdiction puts both foreign companies and foreign lawmakers in an awkward position, as they wrangle with compliance choices and EU diplomatic and commercial relations.[82]

In practice, EU regulators presumably will not prioritize or dedicate limited resources to policing small and distant companies. However, the GDPR will be an issue for companies with growing EU user bases and presence in Europe.[83] They will need to think hard about their obligations under the Regulation overall – not just its RTBF requirements. (There is an interesting question about authority running the other way: should non-EU data processing laws, including potentially more liberal rules balancing free expression, govern European processing?)

III.G. Can administrative agencies adjudicate free expression rights under my country's legal framework?

By extending data protection law to cover public online expression, the Google Spain ruling moved considerable new authority into the hands of data protection regulators. These administrative agencies can decide whether certain information will be possible to find using search engines. If RTBF is extended to hosting platforms, the same regulators will determine whether expression appears online at all. Resting such power in the hands of administrative agencies, rather than courts, may be permissible under the EU's law and human rights framework. Policymakers in other countries, however, may reach other conclusions.

[81] Art. 3.2(b).

[82] Keller, Daphne y Brown, Bruce D., "Europe's Web Privacy Rules: Bad for Google, Bad for Everyone", *The New York Times*, April 25, 2016, available at: http://nyti.ms/2fpm3f2.

[83] Another new jurisdictional hook covers foreign entities "offering goods or services" in the EU. In a recital, however, this ground is cabined based on factors such as the national currency used for prices. R. 23. Recitals in the GDPR also evince a real frustration with claims that EU law does not reach the foreign corporate parents of subsidiaries established in the EU, saying "legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor" for determining "establishment" jurisdiction under Article 3.1.

Conclusions and recommendations

Grounding a RTBF in EU-style data protection law leads to imbalanced rules that under-protect Internet users' free expression rights. One remedy for this, in the EU and elsewhere, would be to incorporate significant new substantive and procedural protections for speech within data protection law. A simpler approach, however, is to recognize that obligations for intermediaries to erase online speech are very different from obligations for them to erase back-end user data. The issues raised by speech deletion, and the need for procedural rules that protect against over-removal, are already addressed in intermediary liability laws and in free expression jurisprudence.. Those rules can be brought to bear in protecting both speech rights and privacy and data protection rights.

Lawmakers concerned with protecting the full spectrum of rights have many doctrinal options under their own national laws. While these will vary by country, the considerations identified in this article can help lawmakers and human rights advocates in arriving at robust legal frameworks to protect the rights of Internet users.

Chapter Six

Right to Be Forgotten in Cyberspace? International Principles and Considerations about Latin American Regulations

Nelson Remolina Angarita[1]

Do people have the right to change their lives without being forever haunted by the ghost of the negative information about their past spread all over the Internet?
Nelson Remolina Angarita

Introduction

The expression "right to be forgotten" (RTBF) appeared in the legal scene decades ago. In the Republic of Colombia, it was first analysed under the Constitutional Court ruling T-414 on June 16th, 1992[2]. For a long time, the concept referred to the situation of people reported as debtors, people in arrears or individuals who had committed a crime. During the XX century, the subject was studied under the framework of the right to information, reputation and human dignity in relation to individuals, credit risk entities and the State.

Nonetheless, the debate in the early XXI century was enriched with new elements and circumstances. On the one hand, elements as Internet and freedom of expression were added. In addition, the right to be forgotten

[1] Nelson Remolina Angarita is associate professor at Universidad de los Andes (Bogotá, Colombia). Director of the Information Technology, Telecommunications, Electronic Commerce Task Force (GECTI) (http://gecti.uniandes.edu.co/2014) and of the Ciro Angarita Barón Observatory for the protection of personal data in Colombia (http://habeasdatacolombia.uniandes.edu.co). He holds a Summa Cum Laude Ph.D. in Legal Sciences from the Pontificia Universidad Javeriana and a Master of Laws, The London School of Economics and Political Sciences. Specialist in Commercial Law and Lawyer (1994) at Universidad de los Andes (Bogota, Colombia). This paper only reflects the author's opinion. Email: nremolin@uniandes.edu.co. This article is an English translation of the Spanish original.

[2] *Cfr.* Constitutional Court, ruling T-414 on June 16, 1992. MP. Ciro Angarita Barón. The text can be accessed at: http://bit.ly/2h0v2Wi

(RTBF) may be exercised on indeterminate subjects, such as any person who posts information on the Internet.

The ruling issued by the European Union Court of Justice[3] on the Costeja case in 2014 has been the point of reference of the XXI century debate. We should not overlook, however, that while in the Colombian Constitutional Court's ruling of 1992 such right was explicitly addressed, in the legal decision issued by the Court of Justice, the RTBF was not expressly analysed. Nonetheless, this last ruling has been the reference for a series of comments, articles and reactions which caught the attention of the academia, businesses and regulators.

For instance, recently the right was expressly included in Costa Rica (right to be forgotten), Nicaragua (right to be forgotten online) and article 17 of the General Data Protection Regulation[4] (GPDR) of the European Parliament and of the Council under the name "Right to erasure («right to be forgotten»)", announced as one of the new inclusions into the Regulation[5].

The legal construction of the RTBF has encompassed the analysis of several rights and principles. The list includes the rights to privacy, personal data protection, reputation, freedom of expression, the right to give and receive information, among others. Principles include the principle of human dignity and the principle of technological neutrality in Internet.

Acknowledging the RTBF is primarily related to law. Real facts and concrete situations have been a determining factor to acknowledge and guarantee this right. Establishing how to guarantee the RTBF on the Internet has also been an interesting task. In other words, which measures will prevent negative information from being revealed to third-parties in cyberspace? In line with the above-mentioned, several mechanisms have been employed, ranging from the removal of information to "de-indexing", to anonymization, "robots.txt", "metatags" and other similar technical tools, which prevent revealing the information intended to be forgotten.

Within this framework, this paper pursues multiple objectives, namely: (1) to highlight the importance of the RTBF and its relation to human dignity; (2) to underscore the challenge faced by people and authorities to guarantee the

[3] *Cfr.* Court of Justice (Grand Chamber). Decision on May 13, 2014. Case C131/101. *Google Spain, S.L., Google Inc. and Agencia Española de Protección de Datos (AEDP), Mario Costeja González*. The text may be found at: http://bit.ly/2a332A6

[4] *Cfr.* European Parliament. Reform on data protection, "New rules adapted to the digital era" (press article). Published on April 14, 2016, available at: http://bit.ly/1XxhgJc

[5] *Cfr.* Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, in relation to the protection of natural persons with regard to the processing of personal data and the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation).

RTBF in cyberspace; (3) to emphasize that the RTBF is part of the right to erasure and part of the right to objection from the legal perspective of the right to the protection of personal data, and (4) to specify that search engines are the main responsible for processing personal data worldwide and that information indexing is the main trigger of data mass dissemination on the Internet.

Our conclusions are not immune to criticism, which is welcomed. As a matter of fact, a whole paper could be written with totally different starting point and conclusion. That is natural, since there are various perspectives (business, academic, public policy, among others) and interests (economic, human rights) on the subject-matter.

Hence, our first thoughts are a mere academic invitation to continue discussing more cases in the light of the specificities of each factual situation, as well as the legal tools, rulings or administrative decisions in each country.

I. Cyberspace as a challenging scenario for the effective guarantee of the RTBF

The level of effective guarantee of the RTBF depends, among other things, on the context where protection should be applied. It may be, for example, at a physical, local, electronic and international level, depending on the case. Claiming the RTBF to a local credit risk data bureau or a physical newspaper is not the same as claiming the right before a person – "Internet users"- or a business, that publishes information about others on Internet.

In the first case, it is more feasible to identify those responsible and suppress the information through the RTBF. In the second case, it is very difficult to attain the complete "suppression" of information on Internet, since it may be published or replicated online by millions of people, and due to the complexity and ignorance of the changing and innovative technological world, that is not fully understood by many of us, by some judges, public servants or regulators. Therefore, we will briefly refer to certain matters about cyberspace and Internet that, we believe, reflect the society and the reality of the XXI century that we must face.

I.A. From cyberspace to Internet

We are witnesses to the migration from the physical world full of borders to the technological and borderless "cyberspace". We live on a planet divided into territories where most of the activities are governed by national

regulations and authorities with territorial[6] (not cross-border) competence. At the same time, we observe a process of erosion and blurring of territorial borders and the emergence of a huge space where the number of people interacting in cyberspace progressively increases.

Cyberspace has been characterised for being a global scenario without geographical borders,[7] where activities unfold within the technological architecture of Internet, whose users are growing all the time. Here, the physical space finds no limits (as opposed to our homes or country territory), but an artificial or virtual undefined field where people interact. An important part of the interaction in the virtual world has legal implications and consequences in the real world.

(i) While there are various meanings of cyberspace, it is important to bear in mind that it is made up by the following elements[8]:
(ii) A technological infrastructure (technological resources) made of an endless number of devices (servers, computers, mobile phones, tablets, etc.) located in many parts of the world.
(iii) A worldwide platform of communications (worldwide communications web), information and interconnected networks (Internet) known as "global information infrastructure"[9].

Millions of people of various nationalities, located in countries with different legal systems that use technology, communications and information to interact with other people from any part of the world or use the services available on Internet.

Internet[10] is the technical part of cyberspace connecting Internet users

[6] We can assert that the legal world is currently a mixture of (i) local regulators with a territory-defined field of action; (ii) territory-based regulation, and (iii) settlement of disputes generally conducted by judges or authorities with territory-restricted competence.

[7] *Cfr.* Gilden, Michael, "Jurisdiction and the Internet: the Real World Meets Cyberspace, in: *ILSA Journal of International & Comparative Law*, No. 7 (1), 2000, p. 150.

[8] For some features of cyberspace and the challenges to law, refer to: Johnson, David and Post, David, "Law and Borders: the Rise of Law in Cyberspace", in: *Stanford Law Review*, No. 48, 1995-1996, pp.1.367-1.402.

[9] Reidenberg refers to it as "*the global information infrastructure* –GII– "(Reidenberg, Joel R., "Governing Networks and Cyberspace Rule-making", in: *Emory Law Journal*, No. 45, 1996, p. 912.)

[10] According to the *English Oxford Living Dictionary*, Internet is "a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols". Available at: http://bit.ly/2gPJ2V4

("cybernauts") from all parts of the world. It is said that Internet is the "world-wide network that connects the whole world"[11], where all the computers and mobile devices can be linked globally to share their universal field of action and the international nature of the many activities that take place on Internet.

The Internet Society[12] points out that "Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard to the geographical location". And adds that "the Internet today is a widespread information infrastructure".[13] In other words, Internet is even more ubiquitous as it remains present in almost all parts of the world.

I.B. Search engines are the primary responsible for processing personal data worldwide

Search engines carry out the mass, global and cross-border processing of personal data from trillions of people worldwide. They conduct many operations on personal data, such as searching information on Internet, indexing, analysing and, in general, using data for various purposes. This is the reason why there is no doubt that search engines are responsible for processing personal data.

In that sense, the Colombian data protection authority concluded that the indexing performed by the mentioned search engines was part of information processing. In fact, the Superintendence of Industry and Commerce, through a statement on March 3rd, 2015, declared that the processing of personal data includes "the collection, storage, *indexing*, preservation, *analysis*,

[11] Cassin, Barbara, *Googléame: la segunda misión de los Estados Unidos*, V. Goldstein (trans.), Buenos Aires, *Fondo de Cultura Económica*, National Library, Tezontle, 1st ed. in Spanish, 2008, p. 15.

[12] The Internet Society was founded in 1992, with the mission "to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world" (Internet Society. Mission. http://bit.ly/2h4sGsb). It is self-defined as "a global cause-driven organisation governed by a diverse Board of Trustees that is dedicated to ensuring that the Internet stays open, transparent and defined by you" (*cfr.* Internet Society. "Who we are". http://bit.ly/1T127zC). The Internet Society has an Advisory Council composed of academics, researchers, service/equipment suppliers, content providers, government and international organisations and public interest groups (*cfr.* Interent Society, Organisation Member Advisory Council (OMAC). http://bit.ly/2heRuhG).

[13] Leiner, Barry, Cerft, Vinton *et al*, "Brief History of the Internet", Internet Society, 1997. http://bit.ly/1jBhWfC. The authors of this texts are: Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff.

use, circulation, transmission, transfer, *dissemination*, *access*, consultation, suppression, and purging of personal data".[14] In this way, there is no doubt that search engines process personal data and, therefore, they should fulfil the obligations imposed by regulations as responsible for the processing of huge amounts of data from trillions of people worldwide.

I.C. *Indexing* as the limitless multiplier of personal data in cyberspace

Search engines are not the creators of the information published by third parties (such as mass media or Internet users); however, they are primarily responsible for disseminating the data online massively and instantly. *Indexing* is the triggering factor of the unlimited dissemination of personal data in cyberspace. If we consider *indexing* as "good" or at least "normal", then the question remains why *de-indexing* is something "bad" or "abnormal"? Indexing is the trigger of the limitless multiplication of personal data on Internet. That is why de-indexing should reasonably mitigate the effects caused by indexing in relation to the dissemination of negative information for which the RTBF may be applicable. Ignoring the multiplying and global effects of search engines and indexing means overlooking the existence of the Internet.

De-indexing does not fully erase the posted information, but locating such information will not be as easy and fast as with the intervention of the search engine. Therefore, it is important to consider the massive impact of the instant and global dissemination made by search engines, which can find and organise data relating to an individual in a matter of seconds.

If search engines did not index the information available on Internet, it would not be so easy to find the data about a certain person. Is it perhaps not reasonable then to ask those responsible for "indexing" and facilitating the dissemination of information on Internet to "de-index" and help prevent the spread of specific negative information in certain cases?

We agree on the importance and need to guarantee freedom of expression on Internet, but we should not forget that such freedom is not absolute and must be analysed in the light of the specificities of each case, bearing in mind its coexistence with other rights, such as data protection[15]. On this point, it

[14] *Italics* was made by us. For more information, *see*: Remolina Angarita, Nelson, "*Autoridad colombiana de protección de datos concluye que sí es competente para investigar a Facebook*", 2016. Available at: http://bit.ly/2gGzmh5

[15] In relation to this, the opinion of the Peruvian data protection authority is important: "The claimant's personal data (first and last names) has been blocked, i.e. any information or publication related to the dismissal of case No. 39452-2009 (305-09)-CMV that appears

may be worth mentioning the following statement from the Peruvian data protection authority:

> As the fundamental right to protect personal data shares the same hierarchy as any other fundamental right, in general and abstract terms, no other right shall be considered above it. Each case should be individually weighed and evaluated.
> As a matter of fact, freedom of expression coexists with other rights, and our obligation is to protect them all, since no fundamental right should affect any other fundamental right, therefore, the setting of limits between one and the other should not be presented, as intended by the claimant, as a matter of "conflict" or "incompatibility", but as the definition of forms of "coexistence" between both rights. Hence, arguments favouring freedom of press may be true and plentiful, but by no means do they justify the annulment of the right to personal data protection[16].

De-indexing is not a prior check method, but a way to solve problems caused, among other things, by the massive and indiscriminate indexing of information on Internet. De-indexing does not mean that the search engine is responsible for the content. By indexing information, the search engine facilitates data dissemination and localisation. That is why, in justified cases, de-indexing is appropriate so that the engine stops disseminating any negative information that affects a person.

De-indexing is a reasonable measure to help forget certain negative information aimed at guaranteeing human rights and, ultimately, vindicating human dignity in certain cases.

---

in the results from Google Search engine, understanding by blocking –in this case- the processing of publications to prevent them from being available for subsequent searches or indexing based on name search criteria". This means that no Internet user may be prevented from accessing the content located in the URLs of the Internet websites listed on the claim when using Google Search, but they will only be able to reach said content as long as they use search criteria other than the claimant's first or last names. Consequently, the DGPDP (General Directorate for Personal Data Protection) considers that: "The reference to freedom of expression on Internet by website administrators or webmasters is inappropriate, since the data subject to claims remains unchanged on the source web pages."

"The reference to freedom of expression by Internet users is also inappropriate, since access to the information subject to claims is maintained due to the use of other words in search criteria (concepts, facts, subject-matter, number of resolution, dates, among others)", Republic of Peru, Directorate Resolution No. 026-2016-JUS/DGPDP on March 11, 2016. Available at: http://bit.ly/2fBFWR6).

[16] *Ibíd.*

I.D. "Internet of Corporations" and the protection of human rights in cyberspace

"Internet of Corporations"[17] (IoC) is another expression I suggest should be considered as was the "Internet of things". In my opinion, this is no minor issue since "Internet of Corporations" largely summarises what has happened with the regulation of Internet. The IoC has shaped the fate of Internet and its users since it was hyper-regulated by businesses, who use its "legal notes" or "terms and conditions" to establish the rules that, as of July 2016, govern the destiny of over 3.42[18] billion people worldwide.

IoC refers to the rules set by business people to do business or offer their services on Internet. It contains the guidelines business people consider reasonable under their business model in order to make profit. Ultimately, it is the Internet that businesses want to make money. These regulations may be called "business laws", that are part of the binding corporate rules (BCR). Since the middle of 2016, these regulations have been governing over 1.70 billion Facebook[19] users, or those who perform over 2.85 billion Google[20] searches every day and, in general, people accessing roughly more than 1.05 billion web pages[21] available on Internet.

As you can see, we are facing a huge reality that involves the "digital economy" and the effective protection of human rights of billions of people on Internet. This situation also depicts the "power on Internet" and the "fragile protection of human rights in cyberspace" because, in practice, the scope of human rights on Internet depends, largely, on what is defined by business laws. For instance, the following question may be raised: does the owner of a search engine recognise the RTBF or not? If yes, then there would be no problem de-indexing the data affecting the individual. But if the business fails to acknowledge the RTBF, then that individual would have to resort to the local authorities to reach his/her goal and force the search engine to de-index the information to protect the rights of the person in a concrete situation.

[17] This section summarises part of the following article by the autor. *See* Remolina Angarita, Nelson, *"Internet de las empresas" ["Internet of Corporations" –IoC–]: una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (Parte 1)*, published on June 28, 2016, available at: http://bit.ly/2gi9wfl

[18] *Cfr.* http://bit.ly/1cWKuda, last access: July 29, 2016.

[19] *Cfr. idem.*

[20] *Cfr. idem.*

[21] *Cfr. idem.*

The IoC has colonized most Internet activities. In view of that, the States have issued laws that influence the activities performed by businesses on Internet. These state regulations have been made for several reasons, namely: the protection of general interests, the protection of human rights of citizens, the protection of e-commerce consumers. Many of the objectives of the State regulation are summarised under the EU-US Joint Statement on Electronic Commerce, on December 5, 1997[22].

The goals of businesses and the objectives of States explain the purpose of their rules. While the goal of a business is to make money, the mission of the State is, in general, "to serve the community, promote general prosperity and guarantee the effectiveness of the principles, rights and duties enshrined in the Constitution".[23] The objectives of businesses are written down on their social bylaws and are unilaterally set by the businessmen, while the goals of the State are set within each country's Constitutions and are agreed upon a democratic basis.

As is observed, businesses and States have several goals and objectives. However, they are not discriminatory. Business and the due protection of human rights are very important matters for some companies. The same is true for innovation and human rights.

Big data, cloud computing and Internet of things are creations of the Internet of Corporations. Each concept is underlain by a business model aimed at making profit, which is legitimate. What should be determined, among other things, is the following: Are business laws consistent with constitutional mandates and international documents on human rights? Do companies do enough to guarantee the rights of people on Internet? Do foreign companies doing business on Internet honour local regulations on human rights issued by the States? Should foreign companies doing business on Internet and not residing in a given country collaborate with that country's local authorities to guarantee the protection of the rights of people on Internet? Should foreign companies doing business on Internet and not residing in a given country follow the rules of that country's local authorities to guarantee the protection of the rights of people on Internet? Should foreign companies doing business on Internet be subject to local laws, or should national authorities be subject to the "Internet of Corporations"?

The questions above are of utmost importance for the future of the protection of rights and, some authorities have already started to make comments

[22] The text of this statement may be found in Spanish at: http://bit.ly/2ggzjW6

[23] *Cfr.* Article 2 of the Colombian Constitution.

in that regard. In a recent case, for example, the Data Protection Authority of the Republic of Peru concluded that:

> Admitting the defence arguments of Google – under Google Inc. or Google Perú S.R.L.- would be admitting that it may perform activities in Peruvian territory, use Peruvian media, process information from Peruvian citizens and market advertising for the Peruvian market, regardless of what is ordered by the Political Constitution of Peru, the LDPD and its regulation, on the right of each Peruvian citizen to protect personal data[24].

I.E. Challenge of the effective protection of rights in cyberspace

In 2001, the Colombian Constitutional Court spoke, among others, about the scope of the constitution in view of the regulation of matters related to the exercise of activities through Internet[25]. The Court believes that information is very important and plays a key role "in the development of today's society" and, that Internet has been a scenario where many "information and IT storage systems" operate. From the very beginning, the Court promptly stated that:

> The information shared on Internet leaves a fingerprint that, (…) enables to track and identify everything done by a person in the virtual world, the sites visited or consulted and the products consumed through the web. The collection of this data may be used to create profiles based on the likes, preferences, search and consumption habits of the people using Internet (as mere users or economic agents carrying out their activities through this means).[26]

On the other hand, the Court also recognised the importance "within a global system of communications, as Internet, of rights and liberties as important to democracy as (…) intimacy and *habeas data* (article 15 C.P.)".[27] Additionally, the corporation ratified that scientific and technological

[24] *Cfr.* Republic of Peru, *supra* note 15

[25] *Cfr.* Constitutional Court, ruling C-1147, October 31, 2001, MP, Manuel José Cepeda Espinosa.

[26] All parts or phrases between inverted commas are taken from ruling C-1147 of 2001.

[27] The other important rights quoted by the Court are: right to equality, freedom of conscience or religion, freedom of expression, free exercise of a profession or occupation, professional secrecy and the exercise of political rights allowing individuals to be part of the decisions affecting them (Constitutional Court, C-1147, 2001).

breakthroughs "have always posed a challenge to the rights", because they exert an influence "in the exercise of a person's fundamental rights", among others, and therefore, "demand various answers from the legal system".[28]

According to the Court, Internet is one of those breakthroughs "whose effects at a trans-national level pose various constitutionally significant problems"[29] because, among other things, we are dealing with an important reality of our society upon which the current legal tools may turn out to be insufficient. In fact, said corporation believes that "the existence of a new worldwide communications network and of information paths that are of easy access to citizens for multiple purposes (…) at a global scale, is not a legally harmless reality" and "*since the technology used in Internet, the ingenuity and creativity of many of its operators evolves at a very fast pace, legal precepts issued in order to regulate the activities developed through these means of communication may be harmless to reach some of the goals pursued*". [30] That is why, the Court concludes, in those cases where "the existing regulation is unable to reach the goals for which it was created, due to technical breakthroughs", the legislative branch "is responsible for making the corresponding decisions".[31]

Even though the Internet's field of action goes beyond national borders, the Court considers that the new technological scenario and the Internet activities are not excluded from the respect for constitutional mandates.[32] And concludes that "*there may be a virtual reality on Internet (...), but that does not mean that rights, in such contexts, are also virtual. On the contrary, they are not: these are explicit guarantees whose effective enjoyment in cyberspace should also be protected by a constitutional judge*".[33] It also underscores that "no one can argue that just because it is Internet, users may see their constitutional rights diminished".[34]

Considering the previously mentioned, the Right to Be Forgotten will be analysed below with illustrative hypotheses of its application.

---

[28] Missing italics in source text. All parts or phrases between inverted commas are taken from ruling C-1147, 2001.

[29] *Loc. cit.*

30 Missing italics in source text.

[31] *Loc. cit.*

[32] As a matter of fact, the Constitutional Court highlights that "the mandates expressed in the Political Charter gain substantial relevance, requiring protection by the constitutional judge of the rights recognised to all people, since these are guarantees also applicable in this setting" (Constitutional Court, C-1147, 2001).

[33] Missing italics in source text.

[34] All parts or phrases between inverted commas are taken from ruling C-1147 of 2001.

II. RTBF as part of the right to erase and the right to object: notes on the first Latin American and European regulations

The fundamentals[35], the definition and the scope of the RTBF shall depend on the wording of regulations and on legislative interpretations or the decisions or statements of each country's authorities.

To date, we find that this right has been expressly incorporated since 2012 in Latin American countries (Nicaragua and Costa Rica) and, later on, in Europe (2016). These regulatory references are the first on the subject. The analysis in each country will depend on its legal framework. Hence, we recommend not to generalise the subject in abstract terms, but rather analyse it in the light of each State's regulations.

Section 10 of Law No. 787/2012[36] from the Republic of Nicaragua is called "Right to be forgotten online", with the following content:

> The data owner has the right to request social media, browsers and servers to suppress and block his/her personal data on the files.
> In the case of data files from public or private institutions that offer goods and services and, that due to contractual reasons, store personal data once the contractual relation is over, the data owner may request the erasure and blocking of all the personal data that was recorded while he/she was still a user of a service or buyer of a good.

As noted, the RTBF is used as a synonym of the right to take down or suppress data, as part of the *ARCO* rights, expressly referred to by some Latin American regulations, like those of Mexico[37]. The first paragraph does not specify the reasons or circumstances under which the RTBF proceeds in the social media, browsers and servers. Hence, they will be the same when it comes to requesting data erasure or blocking. In the case of a contractual relationship with public or private institutions, the RTBF may be exercised

[35] In relation to the fundamentals of the RTBF, refer to: Leturia, Francisco, "*Fundamentos jurídicos del derecho al olvido. ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos fundamentos?*", on: *Revista Chilena de Derecho de la Pontificia Universidad Católica de Chile*, Vol. 43, No.1, Santiago, School of Law, April, 2016. Available at: http://bit.ly/2flFo0Z

[36] Personal Data Protection Law. Passed on March 21, 2012 and published on *La Gaceta*, No. 61, on March 29, 2010. Available at: http://bit.ly/2flybOn

[37] *Cfr.* Remolina Angarita, Nelson, "*Los derechos de acceso, rectificación, cancelación y oposición en la ley de datos personales y su reglamento*", *La protección de datos personales en México*, México, D.F., Tirant Lo Blanch, 2013, pp. 181-205.

from the moment the relationship is over.

Section 11 of Decree No. 37.554/2012[38] from the Republic of Costa Rica, under the name "Right to Be Forgotten" establishes: "The preservation of personal data, that may affect its owner, shall not exceed ten years, from the occurrence of the facts registered, except otherwise stated by a special regulation or set forth by an agreement between the parties that would establish a shorter a term. If preservation is necessary, beyond the agreed term, the owner's personal data shall be removed". As shown, the section relates the RTBF to the current validity of the personal data whose information may affect him/her. To this end, it sets a general term as a point of reference.

The RTBF was also included in article 17 of the General Personal Data Protection Regulation (GPDPR) (EU) 2016/679[39]. While it is mentioned as such – "RTBF"- it is not a new, autonomous and independent right, but a synonym of the right to erasure, which already existed under Directive 95/46/EC. Nonetheless, the new regulations have expanded the hypotheses where the erasure of personal data shall apply.

In effect, in accordance with Directive 95/46/EC article 12 paragraph "b", the data subject has the right to request the controller the "erasure or blocking of data" when processing fails to comply with the provisions of this Directive, particularly when data is incomplete or inaccurate. The term "blocking" may refer to de-indexing of data in a way that prevents access to given information. Due to the erasure of the data, the owner also has the right to force the controller to notify the erasure of the information previously disseminated.

Now, if erasure is a synonym of the "RTBF", we should note that this right is not new in international documents, addressing the processing of personal data, whose main references are highlighted in the following table:

[38] Regulation of the Law for the Protection of Personal Data Processing, on October 30, 2012. The text of the decree can be found in Spanish at: http://bit.ly/2gy3JFl

[39] *Cfr.* Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, in relation to the protection of natural persons with regards to the processing of personal data and the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation).

	Right to erasure or blocking
OECD Guidelines from 1980 and 2013	"Principle of individual participation. An individual should have the right: (…) d) to challenge data relating to him/her and, if the challenge is successful to have the data erased, rectified, completed or amended" (paragraph 13).
Convention 108 from 1981	"Article 8. Additional safeguards for the data subject. Any person shall be enabled: (…) c) to obtain, as the case may be, rectification or erasure of such data if this has been processed contrary to the provisions of domestic law the basic principles set out in Articles 5 and 6 of this Convention effective".
UN Resolution 45/95 (1990)	"4. Principle of interested-person access. Everyone who offers proof of identity has the right to (…) have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries".
Directive 95/46/EC	"Article 12. Right of access. Member States shall guarantee every data subject the right to obtain from the controller: (…) b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort".
APEC Privacy Framework (2004)	"VIII. Access and Correction. 23. Individuals should be able to: (…) c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted".
Directives of the Ibero-American Data Protection Network (2007)	"5. Rights of access, correction and cancellation held by the data subject. The data subject whose data is processed may perform the following, by clear, expedite, free or affordable procedures: (…) 5.3. To require, when appropriate, correction or cancellation of the data that might be incomplete, inexact, inadequate or excessive, as provided in these directives. 5.4. To require notification to third parties whom data were provided on all rectifications or cancellations per the preceding paragraph."
Madrid Resolution (2009)	"17 Rights to rectify and to delete 1. The data subject has the right to request from the responsible person the deletion or rectification of personal data that might be incomplete, inaccurate, unnecessary or excessive. 2. Where justified, the responsible person should carry out the rectification or deletion requested. The responsible person should also notify this fact to third parties to whom personal data had been disclosed, where they are known".

Table No. 1. Right to erasure or blocking in international documents. Source: Created by the author40

[40] *Italics* made by us.

Erasure means, among other things, "the removal of all traces of something".[41] In other words, it refers to the elimination, removal, eradication or destruction of personal data. Erasure is like the blocking of the ARCO rights. According to some international documents[42], blocking occurs in situations where the veracity of personal data is questioned. In view of such situations, the data subject may choose to request the rectification or blocking (erasure). The first assumes a correction of the information and its processing, while the purpose of the latter is to end the personal data processing due to bad quality information.

We believe the data subject may request the removal or blocking of data when:

- Data processing is forbidden.
- Data were illegally obtained.
- Information is false or does not comply with the requirements under the principle of veracity or quality.
- The time limit for personal data processing has expired (in cases where said limit exists on the regulation).
- The data collected is inappropriate, unnecessary or excessive in relation to the purpose of processing.
- The purpose of processing has been met.
- When, in specific and unjustified situations, the fundamental rights of the person are affected. In this case, there is real information about a person's past that in a special and exceptional context, should be forgotten.

In some cases, this is related to the right to object, also mentioned in some international documents as shown below:

[41] Definition taken from the *English Oxford Living Dictionary.*

[42] *Cfr.* (i) Ibero-American Data Protection Network. Directives for harmonization of data protection in the Ibero-American community (2007), and (ii) International Standards on the Protection of Personal Data and Privacy, favourably welcomed by the 31st International Conference of Data Protection and Privacy Commissioners, held on November 5, 2009, in Madrid.

	When the right to object is appropriate
Directive 95/46/EC	Art. 14: Right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him. Objection is also justified when processing serves prospection purposes.
Directives of the Iberoamerican Data Protection Network (2007)	Art. 6.2: "(…) in cases not excluded by virtue of the law, due to the concurrence of an exceptional, legitimate reason arising from his specific personal situation". Art. 6.3: "(…) the processing of personal data with regards to which the controller is to perform activities related to advertising and commercial prospecting".
Madrid Resolution (2009)	Art. 18: "(…) where there is a legitimate reason related to his/her specific personal situation".

Table No. 2 Cases where the right to object is appropriate per international documents. Source: Created by Nelson Remolina[43]

To summarise, in view of the lack of a universal definition of the RTBF, we believe this is not only the classical right to information removal, but also it is related to the right to object, which allows people, under exceptional circumstances, to request the negative and real erasure of their past.

In line with that, next we shall refer to article 17 of the new European Personal Data Protection Regulation.

II.A. Article 17 of Regulation 2016/679 (EU): right to erasure ("RTBF)

The European Regulation on personal data processing has influenced the standards of Latin American countries to such an extent that the legislation found in many Latin American countries is the same or similar to the European provisions. Additionally, the new Regulation expressly refers –for the first time- to the right to be forgotten, contributing to our understanding of what it is about. This reveals the importance and relevance of knowing the scope of the recent European regulation.

Before we elaborate on the content of article 17, it is important to point out that the right to be forgotten assumes a time limit to personal data processing. The general rule is that data processing should not last forever. In this sense, the regulation enshrines the principle of "storage limitation" under which data shall be used "for no longer than is necessary for the purposes

[43] Italics was made by us.

for which the personal data are processed".[44]

The regulation addresses the RTBF as a synonym of the right to erasure, previously existing not only in Directive 95/46/EC but in other international documents as well. Besides erasing data, the controller shall adopt reasonable measures to inform the controllers which are processing such personal data to erase it.[45]

II.A.1. Cases where the right to erasure or the "right to be forgotten" are appropriate

As a rule, article 17[46] establishes that the data subject has the right to

[44] *Cfr.* GRPDP article 5 paragraph "e".

[45] *Cfr.* GRPDP article 17 paragraph 2. On this regard, the list of reasons included in the Regulation states the following: "66. To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account the available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request. (67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system".

[46] The list of reasons in the GRPDP reads as follows: "65. A data subject should have the right to have personal data concerning him or her rectified and a "right to be forgotten" where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the Internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims".

request the erasure of his personal data and the controller, on its part, "shall have the obligation to erase personal data without undue delay where one of the following grounds applies":

a) the personal data *are no longer necessary in relation to the purposes* for which they were collected or otherwise processed[47].

In this case, it is essential to determine when personal data are no longer necessary in relation to the purposes for which they were collected. Think, for instance, when data are processed with the purpose of personnel selection, to fill a position in a company. Once the process ends, the history data from the people who were not hired to work at the company should be erased.

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), *and where there is no other legal ground for the processing*[48].

The regulation states, inter alia, that processing is legitimate if the data subject authorised[49] the collection and use of his or her information for one or several specific purposes[50]. Likewise, explicit consent is required from special and sensitive data[51] subject. If the data subject withdraws his or her consent, data should be erased, except that there is another legal ground preventing such erasure.

c) the data subject objects to the processing pursuant to Article 21(1) *and there are no overriding legitimate grounds for the processing*, or the data subject objects to the processing pursuant to Article 21(2).[52]

[47] Italics was made by us.

[48] Italics was made by us.

[49] Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. (GRPDP Article 4(11)).

[50] *Cfr.* GRPDP Point (a) of Article 6(1).

[51] It refers to personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural's person sex life or sexual orientation" (GRPDP Article 9(1)).

[52] The text in *italics* was made by us.

As is the case with other international documents, the GRPDP ratifies that in the cases of objection to processing, data erasure may be feasible. According to Article 21 of the Regulation, the data subject has the right to object "on grounds *relating to his or her particular situation*, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions".[53] *Particular situation* refers to the cases explained in part 2 of this text. In case of particular situations, "*the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject,* or for the establishment, exercise or defence of legal claims".[54] This shall be the determining factor to decide whether in the cases of this Article's point 2, the right to be forgotten or to erasure are applicable or not.

Last, as in other international documents, the right to object is also applicable when the purpose of personal data processing is direct marketing.

d) the personal data have been *unlawfully processed*.[55]

Processing is unlawful when it is not based on any of the assumptions of Article 6 of the GRPDP.

e) the personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been *collected in relation to the offer of information society services* referred to in Article 8(1).56

Article 8(1) refers to the conditions applicable to the consent of children under 6 years of age in relation to the information society services.

II.A.2. Cases where the right to erasure or the "right to be forgotten" are not appropriate

The right to be forgotten is not absolute and may not be applicable in a series of cases listed in Article 17(3), which is transcribed below:

[53] The text in *italics* was made by us.
[54] *Idem.*
[55] *Idem.*
[56] *Idem.*

a) for exercising the right of freedom of expression and information.

On this regard, it should be noted that Chapter IX of the GRPDP sets forth exclusive rules for specific processing situations. Freedom of expression and information are part of those specific situations.

Under article 85 of the GRPDP, States shall by law set guidelines to reconcile "the right to the protection of personal data" with "the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression".

Particularly, the article provides for the creation of exemptions or derogations necessary for processing with journalistic purposes or the purpose of academic, artistic or literary expression, to reconcile the mentioned rights, in relation to that provided under the GRPDP on "Chapter II (principles), III (rights of the data subject), IV (controller and processor), V (transfer of personal data to third countries or international organisations), VI (independent supervisory authorities), VII (cooperation and consistency) and IX (specific data processing situations)".

As observed, the subject-matter is restricted to the intervention of each member State's regulator.

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2 as well as Article 9(3);

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

Based on the considerations above, the following lines refer to the first case on the subject found in Latin American law, which we consider important to highlight as the main fundamentals of this right.

III. RTBF from the Latin American law perspective and its relation to human dignity

The right to be forgotten appeared in the Colombian law in 1992[57]. Back then, the Constitutional Court reviewed a writ for the protection of the constitutional rights of a person reported as debtor in arrears at a financial information agency despite the fact that four years had passed since the monetary obligation had legally expired. From the beginning, the Court referred, inter alia, to what was then called the "soul's prison and the right to be forgotten"[58] asserting that "the soul's imprisonment, in today's society dominated by the image, the information and the knowledge, has proven to be a more expedite mechanism for social control than the traditional imprisonment of the body. In this way, the potential effects on the rights of the people generated by the perpetual spread of negative information about them were already foreseen.

In ruling T-414, of June 16, 1992, the Constitutional Court concluded that there was a breach of:

> The claimant's intimacy, personal liberty and dignity through the abuse of information technology and of the right of and to information. The infringement of said fundamental constitutional rights is materialised in the reluctance on the part of the Colombian Banking Association to remove his name from the list of debtors in arrears and to immediately update the information on their computerised data bank, knowing that upon the duly executed sentence of April 27, 1987, a judge from the Republic declared that Mr (…)'s obligation to *Banco de Bogotá* expired.

The Court considered that the RTBF "was openly denied to the claimant" by deciding "without a trial, and sentencing him to the indefinite exclusion from the credit system". That is why the Court ordered "the immediate removal of the claimant's name (…) from the list of debtors in arrears at the Information Agency".

[57] An analysis of the Colombian case jointly with a comparative analysis of the RTBF may be found in: Manrique Gómez, Valentina, "*El derecho al olvido: análisis comparativo de las fuentes internacionales con la regulación colombiana"*, in: *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, No. 14, Los Andes University, December, 2015. Available at: http://bit.ly/2f2QCMF

[58] Constitutional Court, ruling T-414 of June 16, 1992, MP, Ciro Angarita Barón.

It is very important to highlight the following statements set forth by the Court in the mentioned sentence:

- The personal data processing "has a limited valid term".
- "Sanctions or negative information about a person should not last forever and, consequently, after some time, such persons hold a true right to be forgotten".
- "With the express recognition of human dignity as the supreme value of the Social Rule of Law, (article 1 of the Charter, 1991), intimacy –one of the most concrete and direct manifestations of said dignity- has acquired a privileged position in the set of constitutional fundamental rights. Once more, this implies that, *in case of an eventual insuperable conflict between the right to information and the right to intimacy where balance or coexistence are not possible, intimacy shall prevail"*.[59]

In later decisions, the Court highlighted the link between the right to be forgotten and human dignity, underscoring that information, even if true, should not be published eternally when that affects the person's dignity. Thus, for instance, through ruling T-022 in 1993, that corporation stated that:

> Truth is not the miracle key that opens said wall –intimacy- and exposes the subject to a merciless observation, like a fish in a crystal bowl. No. Truth yields the way to the person's dignity and to the expected risks of self-determination and maturity in exercising freedom. As was repeatedly pointed by the highest authorised legal doctrine and the philosophical school of thoughts that consider the person as their vital pillar, for barely obvious reasons, *exceptio veritatis*[60] is not applicable.

On its part, in ruling T-592 of 2003, the Court concluded that:

[59] Italics was made by us.

[60] Original underline from the sentence wording. *Cfr.* Constitutional Court, ruling T-022 of January 21, 1993, MP, Ciro Angarita Barón. In this ruling, the Court concluded the following: "This corporation believes it appropriate to warn that the right to intimacy is not build in all cases with material taken from the quarries of absolute truth or kindness, but with the humblest ones pertaining to human behaviour in all of its complex manifestations. Therefore, neither *exceptio veritatis* nor the alleged or actual existence of a misbehaviour are sufficient to ignore the right to intimacy, with all the scopes set by the Constituent in article 15 of the Charter. Hence, kindness, integrity and intimacy operate in areas not necessarily consistent or equal" (underlined in original text).

> For the purpose of restoring reputation, the right to be forgotten is not the only aspect that matters in setting the valid terms that negative information shall remain on data files, but also the debtor's dignity claim that the review of his behaviour be performed considering his human condition, in view of which people may, at all times, have their good name and intimacy repaired after correcting their behaviour.[61]

Based on the afore-mentioned, the following criteria may be considered for future cases involving situations related to the RTBF:

- As a rule, personal data processing is not perpetual.
- Even though a person's processed data may be truthful, he cannot be condemned to having his negative information disseminated indefinitely.
- Neither privacy nor the right to information are absolute. Both are important in a democratic society. Human dignity, however, is a determining factor to making decisions when facing specific situations discussed before judges. It is not sensible to favour, *per se*, one right or the other, because the specificities of each case deserve special analysis.

In sum, a constitutional doctrine on the right to be forgotten emerged in 1992 in Colombia. It is important to recognise that negative information, whether it be true or not, should not always be published in an unlimited and indefinite manner. There are cases where it is necessary to limit said publication for a matter of human dignity or for other reasons resulting from specific cases.

Conclusions

The right to be forgotten has gained special relevance in view of Internet publications of real facts from a person's past, who now wish to have the data fully erased on personal grounds. At the same time, cyberspace is the stage where these situations take place, which makes it very difficult for the RTBF to effectively materialise in such digital, cross-border scenario, which is uncontrollable due to the number of Internet users and the global, open and easy-access network design of Internet.

On June 16, 1992, Colombia witnessed the birth of the right to be forgotten, as a result of the work done by the Constitutional Court. The purpose of

[61] Constitutional Court, ruling T-592 of July 17, 2003, MP, Álvaro Tafur Galvis.

that right is to stop the publication or dissemination of negative and truthful information about a person's past, in specific and legitimate situations. It is not reasonable, in some cases, to publish negative information in an unlimited and indefinite manner, since it is imperative to restrict such publication for a matter of human dignity or for other reasons resulting from specific cases. Therefore, it is necessary to define, in each situation, whether in the case of the person objecting to the processing of his past data, or for some other legitimate reasons to continue processing that information.

The right to be forgotten is important for those who want to change their lives in relation to their past: Does a sexual worker have the right to change her job, rethink her life, get married, have children, study and live her present and future life without having people know about her past? Should people be condemned for life due to their past? Do people have the right to choose a different way of living without being haunted by the negative ghost of their past? If the answer is *yes*, how will that person change if his negative past is being disseminated through Internet, on the news, on videos or in the film industry? Probably answers will vary on a case by case basis, but it is important to define, inter alia, whether a person's negative past is of public interest and socially relevant so as to continue with its dissemination in the present and the future.

Many people consider it transcendental to acknowledge and recognize the right to be forgotten. Maybe that is the only way for them not to be stigmatised or eternally condemned for true but negative facts of their past.

The first regulations expressly referring to the right to be forgotten are from Latin America (Nicaragua and Costa Rica in 2012) and then, from Europe (2016). In the former, the RTBF is associated to the time limit of information and its erasure or blocking.

In relation to the recent European regulation on the RTBF, gaps prevail in its definition, since this is not the classical right to erase information, but it is related to the right to object, under which people may request the removal of information about their negative and true past under exceptional circumstances. Also, time is an additional and important factor to establish that we are addressing this right, because normally, law deals with negative and true information of a person's past.

The right to be forgotten is not absolute. Its protection shall depend on the analysis of the variables arising from the special characteristics of specific and real cases. However, it should not be forgotten that people have the right to change their lives without being permanently and indefinitely haunted by the negative ghost of their past.

Search engines do not generate the information, but they are responsible for massively and instantaneously disseminating it on Internet. Overlooking the multiplying and global effects of search engines and of indexing is like ignoring the existence of the Internet.

We should not forget that indexing, which is performed by search engines, facilitates the search of information on Internet. Search engines help disseminate a person's outdated information.

Indexing triggers the limitless multiplication of personal data in the net. It calls the attention that some people blindly and uncritically assume that it is "normal" to index information, but that it is "terrible" or "very serious" to de-index it in order to protect human rights or human dignity.

Finally, this paper concludes with the same quandary used at the very beginning: Do people have the right to change their lives without being forever haunted by the ghost of the negative information about their past spread all over the Internet? If your answer is *yes*, then you have understood the importance of the Right to Be Forgotten.

Towards an Internet Free of Censorship II

Perspectives in Latin America

The Center for Studies on Freedom of Expression and Access to Information (CELE) was founded in 2009 at University of Palermo Law School with the overarching goal of promoting freedom of expression and access to information through targeted research and capacity building. CELE's goal is to develop useful studies, guides and papers for civil society organizations, journalists, and governmental and academic institutions working on the defense and the promotion of the rights to freedom of expression and access to information, primarily in Latin America.

CELE was created to respond to the need for spaces for the debate on the importance, the content and the limits of the rights to freedom of expression and access to information in the Latin American region. The Center intends to dialogue and collaborate with other academic entities in Argentina and Latin America.

In this framework, CELE's specific objectives are:

- To develop studies, guides and recommendations capable of shaping and changing public policies affecting the rights to freedom of expression and access to information.
- To foster a deeper study of these issues together with other academic entities and disciplines.
- To raise awareness on the importance of the rights to freedom of expression and access to information in democratic societies, especially among the younger generations.

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información
Mario Bravo 1050, 7° P. (C1175ABT) Buenos Aires | Tel.: (54 11) 5199-4500 int. 1213
www.palermo.edu/cele