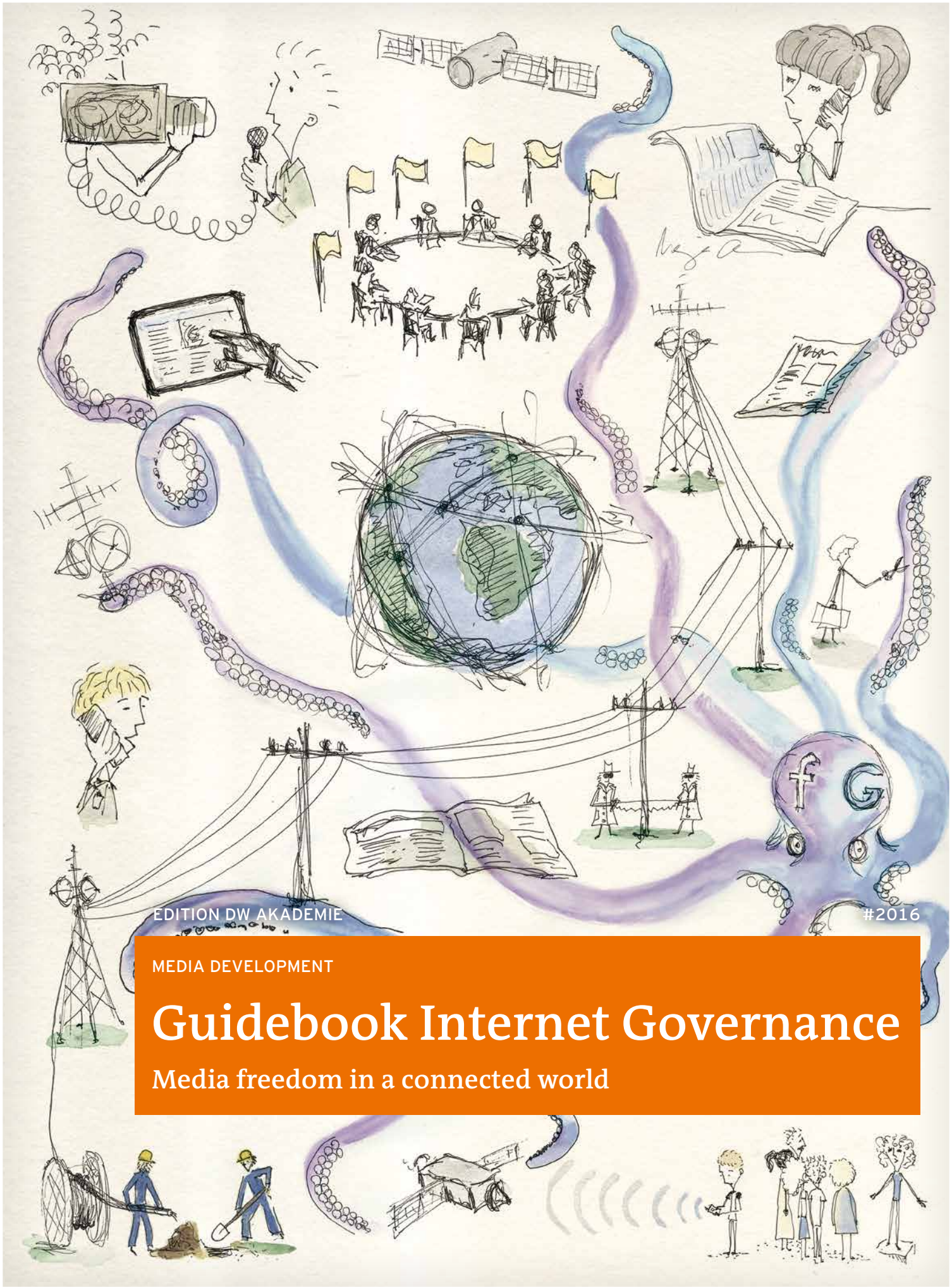
DW Akademie

Made for minds.



EDITION DW AKADEMIE #2016

MEDIA DEVELOPMENT

Guidebook Internet Governance

Media freedom in a connected world

EDITION DW AKADEMIE #2016

MEDIA DEVELOPMENT

Guidebook Internet Governance

Media freedom in a connected world

Barbara Gruber, Lorena Jaume-Palasí, Steffen Leidel, Matthias Spielkamp (eds.)

Imprint

PUBLISHER
Deutsche Welle
53110 Bonn
Germany

RESPONSIBLE
Petra Berner

AUTHORS
Enrico Calandro
Helani Galpaya
Lorena Jaume-Palasí
J. Carlos Lara
Matthias Spielkamp

EDITORS
Barbara Gruber
Lorena Jaume-Palasí
Steffen Leidel
Matthias Spielkamp

EDITORIAL OFFICE
Ralf Grötker

ILLUSTRATION
Cover, pages 20, 24, 28
Manja Ehemann

PUBLISHED
June 2016

DW Akademie

With financial support from the

BMZ Federal Ministry for Economic Cooperation and Development

Cooperation Partner

iRIGHTS lab

Table of contents

Foreword

Foreword

DW Akademie is an international media development organization active around the globe in promoting the right to freedom of expression—in the digital as well as in the physical world.

The Internet has become a global tool for freedom of expression. From a filmmaker uploading a banned documentary on Youtube to a journalist using Whatsapp to file reports from a rural area, or a migrant worker rating their experience of their recruiter online, the Internet allows people to exchange, and engage with, ideas and information in ways they never could before.

And this online freedom of expression, in turn, supports informed public participation in democratic processes as well as social, cultural and economic development. In fact, the Internet is now considered so fundamental to development that the United Nations' new Sustainable Development Goals pledge to increase affordable access to the Internet in the least developed countries.

Capturing the potential of the Internet for development requires certain conditions though, such as the free flow of information. Citizens must be aware of their digital rights and know how to use, understand and create digital content. They must also have access to all of the Internet.

A free and open Internet, however, is increasingly under attack.

In 2015, Internet freedom decreased for the fifth year in a row, according to the US advocacy group Freedom House. In many developing countries, governments are pushing to control the Internet. Censoring content is a growth industry, and Internet and social network shutdowns in response to civil unrest are on the rise. Online surveillance is exploding and people are being increasingly intimidated or detained because of their online activities.

At the same time on an international level, there is disagreement about how the Internet should be governed. Many nations are lobbying for states to have a stronger role in managing the Internet, a move that could give governments new mechanisms for controlling the Internet of the future.

Pressure from commercial interests to monetize or prioritize parts of the web pose an additional threat to Internet freedom.

When state or commercial entities unduly determine what people can and cannot view and do online, this curtails people's fundamental human rights to express themselves and to seek and share information.

Therefore, it is vital for all of us, and in particular civil society and the media, to work together to shape the Internet of the future and ensure it remains in the service of democracy. Civil society has a crucial role in advocating a human rights-based understanding of the Internet, opposing threats to Internet freedom, and representing Internet users in relevant forums, such as the Internet Governance Forum. Journalists are needed to report on digital rights and the effects of proposed Internet regulation. And informed citizens can play an active role in pushing for Internet freedom.

The publication of this Guidebook Internet Governance seeks to give these actors a greater understanding of Internet governance from the perspective of the Global South.

The guidebook's authors explore some of the most pressing Internet governance issues facing the Global South. DW Akademie would like to thank iRights.lab and the contributors for their cooperation and expertise in producing this publication.

Petra Berner
Head Strategy and Consulting Service DW Akademie

01
Introduction

Internet governance and the media—a call to action

Lorena Jaume-Palasí, Germany; Matthias Spielkamp, Germany

To many in the media, Internet governance seems to be an issue far removed from their daily life and work. This misconception can have substantial consequences. The Internet is fast becoming the infrastructure for all communications between media and citizens. If journalists and media freedom activists do not get involved in the debates about how to govern the net, it will be left to governments and private companies to define the rules for our public arena.

When a journalist in Nairobi uploads a news video to an Internet platform like Youtube, for a user in Colombo then to watch it, the data will not just cross several national borders on its way. It will also travel via diverse kinds of public and private infrastructure, from a state-owned telephone network to a privately operated satellite link, to, maybe, a community-run Wi-Fi network.

It will be steered through this array of interconnected lines by open source applications, processed by patented and copyrighted software code, directed on its way by standardized protocols an international community of engineers has agreed upon. Along this entire journey, governments and civil liberty organisations try to assess whether international telecommunications agreements, national must-carry regulations, and fundamental rights—like the one to freedom of information or privacy—are adhered to.

Governing the Internet means governing the media

These, then, are the complexities of what we talk about when we use the expression "Internet governance." At the same time, the example makes quite clear that regulating the Internet means regulating media and journalism. Which means that journalists, publishers, and media freedom activists have to get involved in this process to make their voices heard.

Media are more affected by Internet governance then by any other kind of regulatory framework. The reason: Distribution of traditional media—television, radio, and newspapers—is migrating to the Internet: newspapers still call themselves newspapers but reach a much larger share of their audience via their websites, radio programs are streamed over the net, television is not broadcast via airwaves any more but either streamed as IP-TV (Internet protocol television) or watched on-demand by users on the stations' websites. On top of all this, much of the content journalists produce is consumed on platforms that do not even belong to traditional media companies: Youtube, Facebook, Renren, Twitter, Vkontakte, Weibo, Instagram, Whatsapp, Wechat, and others.

Fundamental rights still apply—but how to enforce them on the net?

On the one hand this means that media regulation we are accustomed to—like broadcasting laws—are becoming less relevant, whereas questions of interoperability of technologies or network neutrality gain enormous importance. But this is only true for what experts call the "physical" and the "logical layers" of the Internet: the physical infrastructure—phone lines, submarine cables, telecom satellites, mobile networks—and the standards that make computers understand each other.

On the other hand, principles that have been guiding Internet governance from the very beginning are more or less identical to those principles that have shaped the regulation of the media sector: freedom of speech and information, copyright protection, privacy, and more. And concepts like intermediary liability—the question of who is responsible for content published on Internet platforms—acquire enormous importance (see J. Carlos Lara's analysis "Don't Shoot the Messenger" on p. 22).

So if someone publishes a controversial comment on Facebook or Twitter, is the company responsible for determining whether it is libellous or in line with the law of the respective country? If not, how can people in Chile or Bangladesh enforce their rights vis-à-vis a company that operates under the laws of a foreign country but makes the content available globally?

Questions like these are amplified in a situation where the legality or decency of content is regarded very differently around the world but the content is accessible everywhere via the Internet, as was seen in the case of the publication of depictions of Mohammed—completely legal as free speech in most countries, an illegal act in many Muslim countries.

New stakeholders, new conflicts—a new power balance?

So it should come as no surprise that governing the Internet is a complex process with many entities involved. As a consequence, in the course of the last decade a large array of stakeholders have become involved in the governance process: governments, the private sector (companies), academia, the technical community, civil society (and, in some regions, youth representatives have most recently been added). This approach is not only supposed to represent a diverse range of views, demands, expectations, and ideas in the process. It also means tangible outcomes in the form of codes of conduct and technical standards can result from it.

But that is not all. At the heart of the attempt to govern this international "network of networks" there lies a dilemma: Many stakeholders have an interest in exerting control over the net, e.g. a government's effort to enforce privacy protection for its country's citizens, without at the same time jeopardizing the free and trans-border flow of information that makes the Internet the revolutionary—and tremendously valuable—development that it is.

If, for example, a country like China decides to block certain web traffic, it has to live with the fact that valuable information may not be available to China's scientists. If a company like Yahoo decides it wants to offer Nazi memorabilia, like swastika flags, in a country where the sale of these is prohibited by law, e.g. France, it cannot be stopped technologically from doing it. But it has to live with the fact that it will be held accountable: Its assets in France might be frozen and its French employees may end up in court.

It is not an empty phrase: No single entity, not even powerful governments like those of the United States of America, China, Russia or India can single-handedly regulate the Internet, let alone control it. The same is true for—admittedly enormously powerful—companies like Amazon, Apple, Facebook, Google, or Microsoft.

Internet governance and the media in practice

So how does Internet governance work in practice, then? The image on pages 30 and 31 (Kenya) provides a good example of the specific stakeholders involved in the process. Government entities, like ministries and the Communications and Multimedia Tribunal, together with self-regulation bodies like the Media Council of Kenya, private companies, and civil society organisations like ICT4Democracy, along with the technical community, try to negotiate the best way for information to travel, be disseminated and regulated in Kenya. And Enrico Calandro's article, "Undermining privacy and freedom of expression in guise of cybersecurity?" (p. 26) is a concrete example of how regulation in one area of the Internet can have sweeping consequences in other areas.

Another prominent example of governance impacting the media is Facebook's recent squabble over a service called "Free Basics." The company wanted to offer Indians access to its social network and a very limited choice of other websites (as it does in many countries around the world). Although the company has a large user base in India and spent billions of rupees on a campaign supporting Free Basics, there was a huge backlash against the service, led by users' rights groups, academics, and activists. In the end they convinced the Indian government to oppose the proposal. Because in order to offer the service to Indians Facebook had to team up with a telecom provider that is regulated under Indian law, the government was able to halt Facebook's attempts by outlawing the service. (For a discussion of the pros and cons of Free Basics and similar ideas, see Helani Galpaya's contribution to this guidebook, "Access for all—or end of the Internet as we know it?" on p. 18)

But even though the Indian government and activists can claim victory in this case, India cannot keep Facebook—located in the United States—from processing data of its Indian users with the purpose of targeting ads to them or even giving the US spy agency NSA access to Indian citizens' data.

Our public arena is at stake

What is at stake in these discussions is the structure of the public arena where we share and discuss our ideas. In democratic societies, a long history of regulation—resulting from a combination of law-making, court decisions and public debate—has led to a rather elaborate understanding of what behavior is legal and seen as ethically sound. Under authoritarian regimes, at the same time, censorship and blocking of content are usually imposed without any consultation with the citizens and without due process. What makes the Internet so disruptive for everyone is that it challenges both approaches.

The decentralized structure of the underlying technology of the Internet and the trans-border character of the flow of data mean that national legislation is losing importance. To democracies, this presents a challenge because democratic rule rests on the idea that the nations' citizens decide—in a mediated process of elections and representation—what rules they want to be governed by. If the nation state cannot control what is shared and published on the communication infrastructure, part of that process is lost. To authoritarian governments, the challenge is even greater because their rule rests on the control the regime is exerting over the citizens. Information suppression and control has always been one of the most important pillars of such a system.

If we assume that free media is a good thing, it is easy to see why the governance of the Internet is such an enormous and complex challenge. It also becomes clear why the global and regional governance of the Internet matters at a national level too: Governments have a harder time than ever enforcing restrictions on communication. This happens at a time when—even among democratic societies—there is no consensus on what has to be tolerated and where lines have to be drawn. Companies find it increasingly difficult to abide by regulation governing communication if they want to serve customers in many different countries. In some cases, activists have a harder time advocating their demands because they may conflict with the demands of other activists from other countries. The technology community face greater difficulties because they need to take into account the demands of a growing number of stakeholders.

Journalists have to make their voices heard

Does this mean, then, that all attempts at governing the Internet are futile? Quite the contrary. Because none of the stakeholders can realistically determine the future of a globally networked media society alone, they all have to get together and negotiate what route to take. In the process of these debates, ideas of how best to govern the Internet are proposed, contested, discarded, adjusted, brought in again, discussed again, and—sometimes—adopted. There is a lot of wheeling and dealing going on, companies try to further their business interests, governments try to assert their regulatory powers, civil society advocates demand fundamental rights be guarded, the technical community wants to keep standards workable—and so on and so forth. Most of the time this results in compromises that make no one happy—but leave no one out in the cold, either. Ideally, we witness the power of the better argument.

What is important is that as many voices as possible are represented and heard. Because views not present at the table (i.e. the national, regional and global Internet governance forums) will not be taken note of. This is why it is essential that civil society stakeholders from all countries, including in the Global South, engage in this governance process.

Lorena Jaume-Palasí
heads the secretariat of the German IGF. She is also Director for Communications and Youth Engagement at the European IGF (EuroDIG) and a researcher on philosophy of law and politics at the Ludwig Maximilians University, Munich. Her research is centered on the contemporary idea, dynamics and ethics of digital publicness and privacy. She engages pro bono at the Internet & Society Collaboratory helping in the development of technical applications such as the offlinetags <http://www.offlinetags.net/en/> and occasionally writes for iRights.info on data protection and digitalization.

Matthias Spielkamp
is co-founder and publisher of the online platform iRights.info, reporting on Internet Governance issues in Germany, and managing partner at the think tank iRights.Lab. As a board member of the German section of Reporters Without Borders, he is responsible for the organization's policies regarding information freedom on the Internet. In the steering committee of the German IGF he acts as co-chair for the civil society/academia group. He currently heads an Internet governance program in cooperation with APC and LIRNEasia.

02
What activists say

Africa

Internet governance is trending as the most important global policy issue today. This is because globally, we have become dependent on the Internet in every sphere of life—education, financial transactions, freedom of expression, and access to information of vital public interest. The Internet therefore needs to be a globally accessible and democratically governed communication medium and secure developmental tool. This can only be achieved through implementation of policies that recognize the intrinsic democratic importance of transparent and accountable Internet governance frameworks.

Koliwe Majama is a journalist and media rights advocate. She currently works at the Media Institute of Southern Africa's Zimbabwe Chapter (MISA-Zimbabwe) as the program officer for broadcasting and information communication technologies.

It is only through Internet governance that Internet freedom can be guaranteed through a multi-stakeholder model, which allows for consensus building and identification of ways to safeguard the freedom of expression and access to information. In my opinion, these goals are the most important ones, if one bears in mind the specific challenges faced in different situations or governance systems.

Kamufisa Manchishi is a program officer at the Media Institute of Southern Africa Zambia Chapter. He runs a program on the Freedom of Expression and Access to Information, which seeks to address challenges affecting media freedom and freedom of expression, including Internet freedom.

Internet Governance is more about governing human behavior in a single world, without borders and amidst diversity, than about the Internet as a messenger and open space. One expectation is that just as the Internet has changed world markets, it will also make possible a bottom-up, multi-stakeholder approach which transforms global governance itself.

Prof. Nii Narku Quaynor is widely acclaimed as the "father of the Internet in Africa." In 1994, he established the first Internet service provider in Ghana and West Africa, operated by Network Computer Systems Ltd. He then assisted in implementing Internet access throughout sub-Saharan Africa.

Latin America

Internet governance is about shaping the evolution of a key resource. It is the way to influence decisions, trying to ensure that the Internet remains open and managed in the public interest. It is about making policy in a way that protects the rights of users and fosters innovation. It is about bridging the digital gap as well as the current political gap, so that actors from developing regions become equal decision-makers in an inclusive global discussion. The stakes are high and active participation is fundamental to achieving these goals.

Marilia Maciel is a researcher and scientific coordinator at the Center for Technology and Society of the Getulio Vargas Foundation in Rio de Janeiro. She serves as a member of the ICANN Non-commercial Users Constituency and is a member of the Advisory Board on Internet security, created under the Brazilian Internet Steering Committee.

Internet governance is a broad concept. However, as a principle for the information society that came from the WSIS process, I agree that "the international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations." For countries in the Global South it is key that one defends and strengthens this principle in a way that any decision on Internet regulation is not taken only by one country, nor only by the government, nor only by one sector.

Dr. Eduardo Bertoni is the director of the Center for Studies on Freedom of Expression and Access to Information at the Palermo University School of Law, Argentina. He was the executive director of the Due Process of Law Foundation and the special rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights at the Organization of American States.

Internet governance seems to be esoteric and a problem of the developed world. This impression only lasts until, as a nation, one becomes aware that governance can't manage spam, phishing, domain names, intellectual property, and privacy. Soon, one will discover that the costs of not acting are far higher than those of acting. "Access first, governance later" is a false dichotomy, as much as "development first, Internet later". Harmonic growth is the most effective growth.

Dr. Alejandro Pisanty was selected to be a member of the Working Group on Internet Governance (WGIG), set up during the World Summit on the Information Society (WSIS). He promoted the multiple-stakeholder model for Internet governance, in face of demands for stronger government controls by other parties. He has continued these activities as a member of the Internet Governance Forum's Advisory Group.

Asia

In India, providing access to the Internet and fostering the ability to use it is about more than bridging the digital divide—it is an opportunity to address existing economic and social inequalities. How can we translate the mobilizing technology of the Internet to address the disparities we see in the real world? This is a tough challenge that is yet to be figured out, an area where our choice of rules, regulation, and decision-making processes will increasingly play a crucial role. Internet governance is fundamental to the evolution and preservation of the Internet as a communication medium that fosters equality, freedom of expression and innovation, where individual networks cooperate, form affinities and construct their identities through their collaboration with others.

Jyoti Panday is program officer at the Centre for Internet and Society, working on Internet governance and on issues related to the role and responsibility of intermediaries in protecting user rights and freedom of expression.

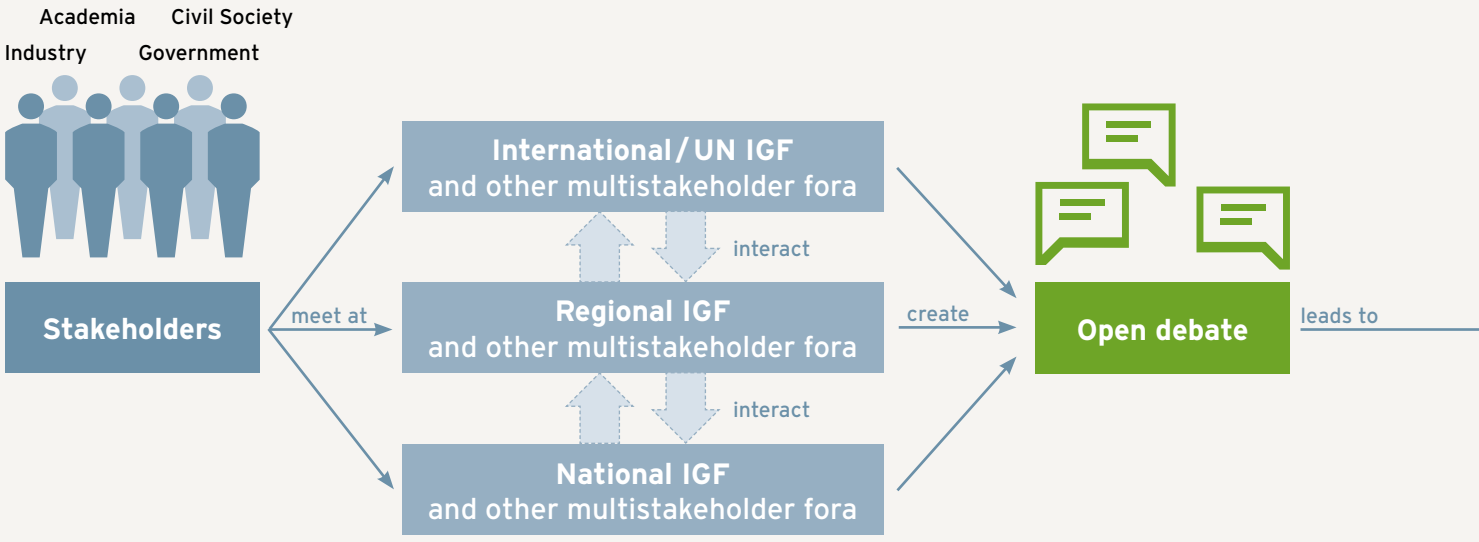
In precarious democracies like Pakistan, the Internet offers the possibility and the hope for alternate discourse and empowerment. Internet governance matters because policies governing the technology seek to do much more than regulating the business of the Internet. Internet governance policies also regulate and effect social, economic and human development in a world that is now shaping up as an information-based economy. By virtue of the pace of technological development and its truly global, boundary-less nature, Internet governance also offers us the chance to explore new and progressive ways of creating governance models by introducing multi-stakeholderism and initiating the debate on human rights' intersection with what was previously seen as simply technological advances.

Sadaf Khan is program director at the citizens' media watchdog initiative Media Matters for Democracy, Pakistan. She works with civil society organizations on media and internet policy advocacy, media ethics, journalist safety, and data and digital journalism.

Many voices count

Internet governance seen from a Stakeholder Perspective

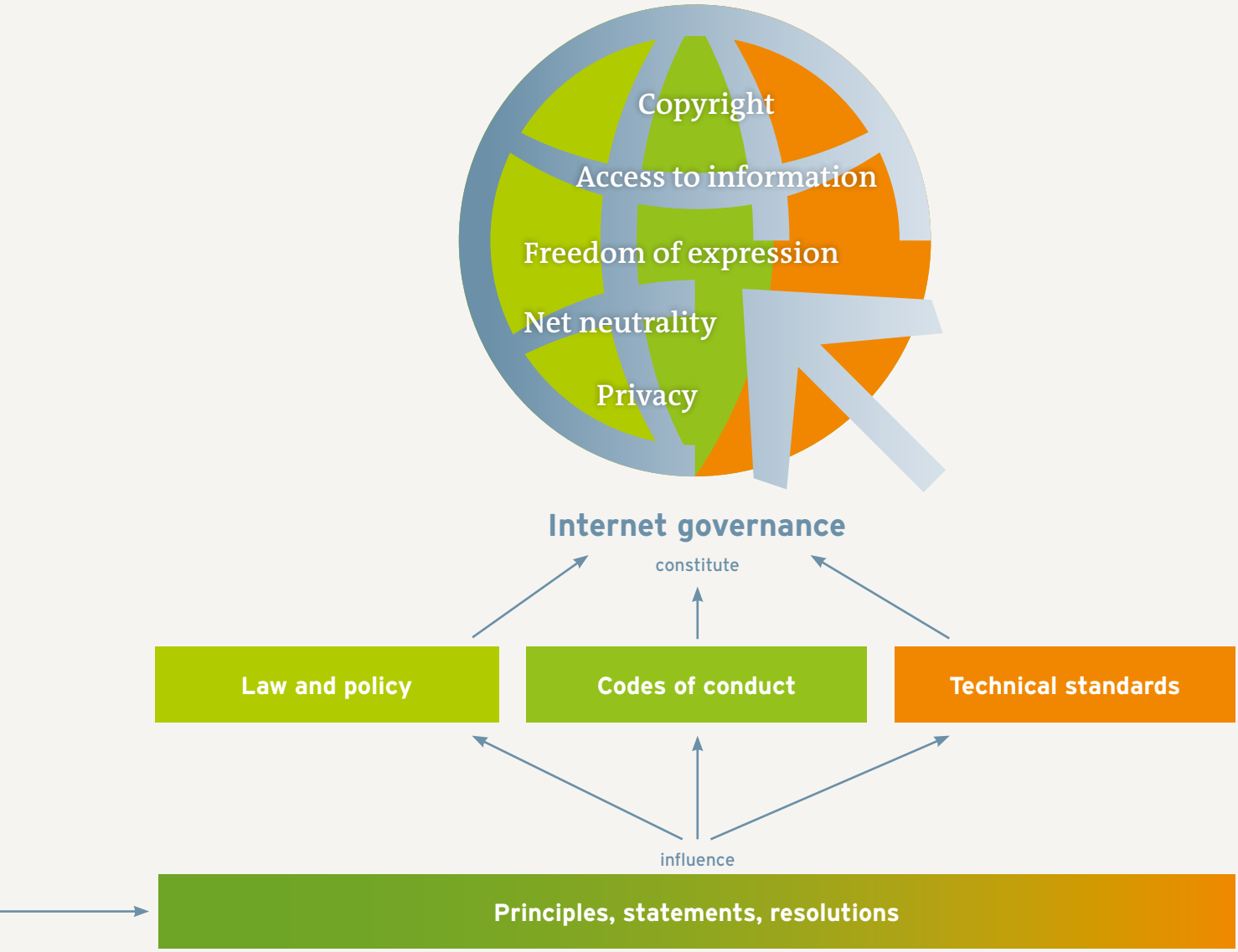
The decentralized character of the Internet and the effortless flow of data across national boundaries have led to the emergence of a new political regime: multi-stakeholder governance. This diagram shows the mechanisms by which stakeholders from the different parts of society contribute to rule-setting in Internet politics.



Stakeholders include a wide array of actors from civil society, government and the industry.

Regional and National Internet Governance make it possible to deal with issues of Internet policy at many different levels of concreteness.

On the **international stage**, processes like the UN-mandated Internet Governance Forum and its many independent regional and national equivalents offer platforms for political deliberation on how to govern the net and give the process legitimacy.



Law and policy: Of course, national governments also have a say in this. See p. 30 for the case of Kenya.

Codes of conduct: One example for this are common practices to deal with the problem of spam.

Technical standards: The World Wide Web Consortium, for instance, decides upon HTML-standards.

Principles, statements, resolutions: Important resolutions were the Tunis Agenda (2005) or the NETmundial Multistakeholder Statement (2014). Another example: The Manila Principles. See p. 25.

Internet governance comprises a vast field of different topics. Among these: cybersecurity; copyright; the digital divide; open data; online anonymity; eHealth; eLearning; broadband-development and intermediary liabity, to mention just a few.

03
Access for all—or the end of the Internet as we know it?

Policy proposals for regulating zero rating in emerging Asia

Helani Galpaya, Sri Lanka

Zero rating could be the mechanism through which millions of citizens in emerging economies are introduced to the Internet. At the same time, zero rating could well lead to the destruction of the open Internet as we know it. But the choice is not a matter of either-or. With proper regulation mechanisms in place, benefits of zero rating can be reaped while possible harm can be effectively mitigated.

Emerging Asia—high mobile phone penetration, low Internet use

In emerging Asia, high levels of competition and innovative business have resulted in nearly everyone (even the poor) calling and texting on their mobile phones. But less than 20 percent of the population in most emerging Asian countries is online (while the majority of Asians who are using the Internet are doing so via mobile devices). Low prices for online connectivity by themselves don't seem to change the situation: Some Asian countries even meet the "under 5 percent of income" target (Galpaya 2015) set by the UN's Broadband Commission (2015) and have payment mechanisms (pre-paid, small value re-charges) that help people on low incomes manage their expenditures.

Zero rating is a practice where Internet service providers do not charge customers on data for select applications and content. One example: Facebook's service FreeBasics. Free Basics is a text-only version Facebook with selected content. Access to FreeBasics is toll free, but viewing videos or clicking on links outside of Facebook incurs charges at the normal rate set by the telephone company providing Internet access. India has recently banned FreeBasics because the service violates the principle of equal access to all online content (net neutrality).

Zero-rated content entices users to go online

In this situation, zero rating is an attractive way to accustom users to the experience of Internet services. This is how zero rating functions: Most citizens in emerging Asia consume mobile Internet on a capped and metered basis. A specific volume of data can be downloaded or uploaded for a given value (or per month); anything above this data cap is paid for separately (often at a premium). Zero-rated content refers to content that doesn't count towards the users' data cap. Telephone companies (in joint agreement with content providers such as Facebook) offer different flavors of zero-rated content, but broadly, users (who may be subscribers of a base-rate data package or are non-subscribers) are offered free (unlimited or limited) consumption of certain zero-rated content. Facebook, Whatsapp, and some music services are often zero-rated.

Zero rating is popular: In 2014 at least 45 percent of the world's mobile operators offered one zero-rated app (Morris 2015). By 2015, zero rating plans were available in every Latin American country (Internet Governance Forum 2015). For telephone companies, it's an opportunity to entice users to experience the Internet in the short term, with the hope users become fully paying consumers in the long term. For the user it is an opportunity to consume their favorite content (usually social media or instant messaging) for free or for a much lower price than otherwise.

At the same time, though, zero rating is also a threat to the open Internet, as it lures users into so-called "walled gardens," where commercial services like Facebook can basically dictate both rules of communication and the selection and prioritization of content (cf. MacKinnon 2012). For example, in countries where most people access the Internet through the zero-rated service Facebook on their mobile phone, activists who seek to reach a large number of people are practically forced to go via Facebook. This, in turn, implies that they have to submit to the content management practices and other rules imposed by Facebook on its users. Far from being neutral, Facebook terms of service may pose severe problems to people living in countries subject to political oppression. For instance, Facebook's rules demand that users register with their real name—something which human rights activists in certain countries would rather not risk. A case in point is the recent example of the Saudi Arabian blogger Raif Badawi who was sentenced to 10 years in jail and 1,000 lashes as punishment for starting a website as a forum for social and political debate. Using a pseudonym would not solve the problem, given Facebook reserves the right to arbitrarily take down content, according to its terms of service. This would mean that our activist's efforts to gain popularity on Facebook would be, in the end, fruitless.

Regulatory and policy options to mitigate harm

From an Internet governance perspective, zero rating is both a chance and a risk: Zero rating could be the mechanism through which millions of citizens in emerging economies are introduced to the Internet. But it could also be the worst thing

"Walled gardens": Commercial services dictate both rules of communication and the selection and prioritization of content.

that could happen to the open Internet. Fortunately, zero rating is not a matter of either-or. With proper regulation mechanisms in place, benefits of zero rating can be reaped, while harm can be mitigated. Here are some proposals[1]:

- **Make transparency mandatory to enhance competition:** In zero rating models where a content- or app provider pays the Internet service provider (usually: the telephone company) to be inside the walled garden, the service provider has incentive to throttle content outside, creating a two-tiered Internet. One option for a transparent regulation would be to make publication of speeds for all types of content mandatory for service providers. In sufficiently competitive markets (such as in Asia) transparency may suffice to mitigate the harm.

- **Protecting net neutrality:** Net neutrality refers to the concept that on the Internet, every packet is treated the same, irrespective of its content, sender, or receiver. Zero rating can violate this principle, but there are ways to make it more palatable, based on principles of non-discrimination and non-exclusivity. Variations of the following are already being implemented:

  - **One-click-away zero rating:** Where a popular app (e.g., Facebook) is zero-rated, but so is the first URL users click through to, outside of the app.

  - **Time-limited zero rating:** Internet service providers are only allowed to offer a zero rating package to any given SIM (or user) for a specified, limited period (e.g. 3 months). After this, continuing users pay normal rates and have access to all content at that rate.

  - **Equal Rating:** Users are asked to watch 5 minutes of advertisements, in return for getting 10 minutes of free access to the open Internet.

  - **Zero rating 2G access:** Internet access on 2G is automatically zero rated, while 3G access is charged as normal. This has the benefit of getting free (albeit slow) access to the Internet for citizens.

  - **Anyone can zero rate:** In theory, anyone who negotiates with the Internet service provider is able to zero rate their content. This requires the service provider to publish a "reference zero rating price list" to start with. It also requires non-discrimination of similarly-classed apps and non-exclusivity (e.g., one music app can't prevent another from entering the walled garden).

  - **Matching data offer:** An Internet service provider may give users some amount of free content, as long as the same amount of data use is given for using the unrestricted Internet.

- **Innovation harm:** Innovative mobile app developers who don't have funds to zero rate their content inside the walled garden can be at a disadvantage because users who don't like to pay won't discover them. Or they aren't allowed to enter the walled garden at all, because another (competing) app has locked the Internet service provider into an exclusive contract. The latter harm requires ex-ante regulation, where zero-rated platforms are banned from discriminating against applications of a similar class of service.

Conclusion

Zero rating promises to increase Internet access in emerging economies such as Asia, while at the same time posing severe risks to the open Internet. From an Internet governance perspective, the proper reaction to this should be to define broad ex-ante rules. Such rules should follow the principle of non-discrimination of similarly-classed content or apps ("Anyone can zero rate"). Beyond that, regulators should monitor markets and user behavior and be ready to act if necessary (such as negotiating with Internet service providers to include offers like "One-click-away zero rating" or "Matching data offer" in their service). In order to make monitoring possible, service providers should be bound to transparency regarding the conditions of access to zero-rated and non-zero-rated content within their area of service. Transparency also has a further benefit: Strongly competitive markets at ALL points of the Internet value chain is the best defence against zero rating harm.

[1] *In fact, countries like Chile, Canada, and Slovenia have already installed regulations of the kind proposed above. See Christopher Yoo (2016).*

Helani Galpaya
is CEO of LIRNEasia, a pro-poor, pro-market think tank working on ICT policy and regulatory issues in the Asia Pacific. She researches and engages in public discourse on issues related to net neutrality, policy and regulatory barriers in Internet access, e-Government, broadband quality of service, and how knowledge and information can improve inclusiveness of agriculture value chains and of small/medium/micro enterprises. She is currently carrying out an impact evaluation of mobile phone rollout in Myanmar.

04
Don’t shoot the messenger

Internet intermediary liability and what must be done in order to protect democratic opinion formation

J. Carlos Lara, Chile

Excessively strict liability rules set incentives for Internet intermediaries to proactively restrict content which might pose risks for liability, without yet being proven to be legally problematic. This poses severe threats to freedom of expression and restrains the free flow of information.

Those in charge of the enabling technologies that make the Internet what it is (and growing into what it can be) are called Internet intermediaries. Between each person behind an act of expression or information and their potential audience, there are intermediaries providing services that allow or aid that expression to reach an audience either technically (by transferring or blocking data packages) or as a content platform (where the new digitalized audiences gather). Content producers, whether a blogger, a journalist, or the media that publishes them, use intermediaries to host and propagate their content, to provide easy access to them in search engines, or to reach their audience via social media.

Social media platforms such as Facebook or Youtube, search engines, as well as telephone companies which provide internet access, act as Internet intermediaries. Whereas traditional media such as newspapers or TV stations are mostly responsible for content which they distribute, Internet intermediaries aren't: It is, to some extent, still an open question in how far they should be legally liable for third party content distributed over their channels. Strict liability would make it impossible for most social media to offer their services. Zero liability, on the other hand, would allow for unrestricted copyright violations or harmful content such as sexual harassment. However this dilemma could be solved: Liability regimes should be designed in such a way that Internet intermediaries are not incentivized to restrict access to content in an arbitrary way, thus violating freedom of expression and restraining democratic opinion formation.

From a media policy perspective, it is a central question how intermediaries facilitate or remove either harmful or beneficial information. This is where governance becomes important: Should intermediaries be made accountable for illegal content uploaded by someone else? What happens if the content itself is a legitimate act of expression, protected speech, or is otherwise not illegal? What happens if content is considered illegal in a non-democratic country or is challenged by an oppressive regime? Intermediary liability regimes try to solve the problem, establishing when an Internet intermediary is indeed liable for third party content, and also establishing when they must restrict or remove third party content to avoid being held liable.

Internet intermediaries are to be found throughout the whole chain of online communication. First, there are connection intermediaries such as Internet service providers (e.g., telephone companies), providing access (connection, routing, and transmission of information) to the Internet at large. Then, there are content intermediaries, such as those that provide hosting of information for users (cyberlockers, cloud computing, and domain hosting services), social networks and online forums, and others like search engines.

While there are several possible ways to design intermediary liability, the legal regimes in many countries have opted for systems where a content intermediary is held liable only if it fails to remove or restrict the content after receiving notice of its illegality. The nature of that notice and the resulting rights and obligations for both intermediaries and content creators vary from country to country[2].

What makes the case problematic is that several of the biggest Internet companies operate from countries where their legal duties put them firmly on the side of censorship for certain types of content. This is the case of the notice and takedown system implemented in the U.S. through the Digital Millennium Copyright Act. The Copyright Act holds an intermediary liable for the copyright infringement of its users unless infringing content is removed following just a private notice—regardless of whether or not it is deemed to be illegal. This regulation has already allowed for the removal of millions of links to copyrighted content without due evaluation of its legal status[3]. By so doing, it has generated acts of censorship of legitimate and harmless content[4], and even political censorship outside of the U.S. (e.g., in Ecuador), based on alleged copyright violations[5]. Because this kind of scheme is favored by powerful industries in the U.S., it is also promoted internationally through free trade agreements, such as the Trans-Pacific Partnership TPP, thus affecting several

[2] *The law may adopt one of different types of liability for third party content: absolute immunity for intermediaries (as long as they do not interfere with the content), conditional immunity (by which they are not liable if they perform an action, such as removing content), and strict liability (which makes them liable with few or no defenses), with some variations.*

[3] *A long list of cases of link removals on copyright grounds without proper consideration of other legitimate interests can be found at Project Lumen (formerly Chilling Effects), available at https://projectlumen.org*

[4] *In the Lenz v. Universal case, a long battle in courts ensued to determine the fair use nature of a Prince song appearing as part of a home video which was taken down from Youtube, essentially calling a home video illegal.*

Just messengers: Too strict liability for social media platforms and search engines could restrain democratic opinion formation.

countries from the Global South in Asia and Latin America which are adopting similar regulations[6]. Especially intermediaries operating internationally may have an interest in this legal export and harmonization.

As a result, to avoid liability intermediaries may enforce rules without taking into account the free speech rights of content authors, or overenforce the rules that exist in order to avoid legal consequences, proactively taking contents away from the eyes of the people, and influencing whether some outlets or producers of content will have greater visibility (Meléndez-Juarbe 2011).

What is to be done? First among the challenges is the need to create a balanced system to deal with illegal or harmful content. Considering the legitimate interests of the creators or uploaders of content, and the legitimate interests of those who oppose its availability (copyright owners, offended individuals, or society in general) is a delicate balancing act. Also intermediary liability regimes introduce the business interests of intermediaries in that equation, regardless of the disproportionate nature of erasing acts of expression. One has to keep in mind that abuse may come not only from private interests, but also from state powers that can demand not only censorship, but further 'collaboration' with state institutions. Whether motivated by excessive or unfair intermediary liability regimes, or by a need to cooperate with institutions of power, the power of an intermediary can be wielded against public interest. This is especially true in the cases where, based on content deemed illegal or dangerous, or just politically inconvenient, a complete service or website is blocked or removed. This was the case of two Internet service providers who blocked the parody website of a Paraguayan newspaper (ABC Color) in 2014 (Avila 2014). The fact that intermediaries hold information from their users in the form of IP addresses is also a cause of privacy and anonymity concerns: Intermediaries may be compelled to give up information about their users, even without legal standing to do so, to allow prosecution for acts of speech or access to information.

Unbalanced intermediary liability regimes put all of society at risk of privatizing the control of legitimate acts of expression and public discourse itself, either in favor of state power or disproportionately protecting private interests. To protect freedom of expression and the free flow of information, intermediaries "need to follow international standards of transparency, necessity, proportionality, legitimate purpose, and due process in order not to engage in violation of rights," as Internet-activist Rebecca MacKinnon puts it[7]. States must also ensure those standards are enshrined in law.

The Manila Principles on Intermediary Liability represent a list of such standards, with careful consideration for interests involved[8]. They were developed by a group of public interest NGOs and academics from all continents out of a need to define and refine the mechanisms to deal with content online, both for states and for intermediaries themselves. The Principles were created within the context of comprehensive free trade agreements that tend to include provisions for content removal close to the US model (such as TPP), and questionable content restrictions worldwide. The Principles aim to influence the legal requirements for content removal or for liability of intermediaries not only at the state level, but also to promote responsibility, transparency and due process among intermediaries. Implementing such standards will ensure we can keep the Internet as a space for free expression.

Manila Principles on Intermediary Liability

1. Intermediaries should be shielded from liability for third-party content.
2. Content must not be required to be restricted without an order by a judicial authority.
3. Requests for restrictions of content must be clear, be unambiguous, and follow due process.
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
5. Laws and content restriction policies and practices must respect due process.
6. Transparency and accountability must be built into laws and content restriction policies and practices[9].

[5] *The Spanish law firm Ares Rights has been sending takedown notices for years under the DMCA on behalf of Ecuadorean government officials against contents critical of them, targeting "documentaries, tweets, and search results that include images of those officials, alleging copyright infringement". See Sutton (2014).*

[6] *A comprehensive analysis of the US strategy of exporting its intellectual property system through free trade agreements to, among others, the Global South and underdeveloped countries, can be found in Flynn et al. (2012).*

[7] *Fostering Freedom Online: The Roles, Challenges and Obstacles of Internet Intermediaries. 2014.*

[8] *Available at https://www.manilaprinciples.org*

[9] *www.manilaprinciples.org*

J. Carlos Lara
is a Chilean lawyer, and works as manager for the public policy and research team at Derechos Digitales, a non-governmental organization based in Santiago de Chile, promoting and defending digital rights in Latin America. He has been a research assistant at the Centre of Studies in Information law at the University of Chile. J. Carlos leads research on data privacy, freedom of expression, and access to knowledge online.

05
Undermining privacy and freedom of expression in guise of cybersecurity

Post-9/11 policy in contemporary South Africa

Enrico Calandro, South Africa

The securitization of the Internet governance debate poses a threat to the open net in general, and to media and journalism in particular. Under the guise of so-called cybersecurity, governments enact legislation that broadens control and imposes draconian penalties on journalists and whistleblowers. A case study from South Africa.

The South African digital media environment, including the Internet, can generally be considered free and open. There is a culture of freedom of expression online with varied content available. The online environment remains diverse and active in South Africa. Marginalized communities are expected to benefit from new access initiatives over time. However, recent sector developments, especially regarding Internet regulation, pose a serious threat to freedom of expression and would violate basic human as well as constitutional rights. At the same time, South Africa is at an impasse from an Internet policy implementation point of view: making very little progress on aspects related to broadband policy, privacy protection, and cybersecurity legislation.

Broadband for all: little progress

To start with broadband policy: Over the last few years, the ICT sector has suffered from leadership discontinuity in the Executive with a rotation of six different Ministers of Communications since 2009. In May 2014, the Department of Communications was split into two separate departments. The split has disrupted other initiatives to extend broadband to all parts of the country as envisaged in the National Development Plan through the national broadband policy and plan: "SA Connect".

One of the main objectives of SA Connect was to provide every citizen with access to a broadband connection at a cost of 2.5 percent (or less) of the average basic monthly income by 2020. The national broadband policy echoes the declaration of the UN Human Rights Council by acknowledging that fast, reliable, and cheap access to the Internet enables human rights. Despite the positive international and domestic response to the policy, very little is known about SA Connect's progress and implementation, except that the members of the national broadband advisory council resigned after failing to get the newly appointed Minister, Siyabonga Cwele, to meet with the Council.

In the spirit of post-9/11

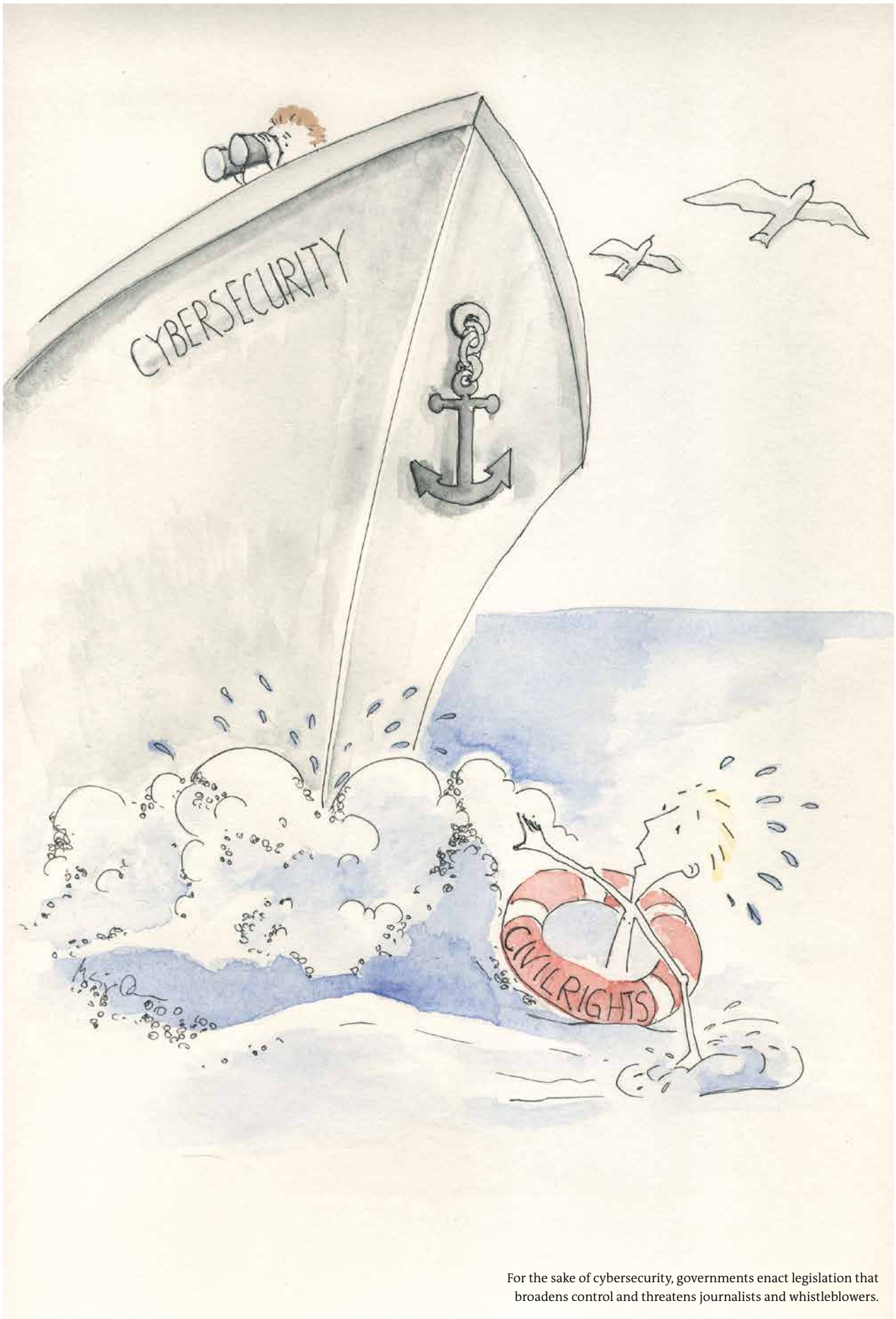
The new Minister, the former Intelligence Minister, has however been active in the area of cybersecurity. Although South Africa does not face particular threats to its national security, especially terrorist threats, the country has adopted a plethora of post-9/11 measures to counter terrorism and other forms of crime (Duncan 2014). One example: In 2013, the South African Government passed two acts which threaten to restrict people's rights to information and freedom of expression. The first one is the Protection of State Information Bill (POSIB) or the so-called "Secrecy Bill," which criminalizes reporting on classified state information and intentionally accessing leaked information, thereby restricting the constitutional right to access public sector information. The second is the General Intelligence Laws Amendment Act or the so-called "Spy Bill," which authorizes state security agencies to intercept "foreign signals intelligence" without judicial oversight.

The "Secrecy Bill" seeks to implement a system of classifying state information and places harsh restrictions on the possession or distribution of classified state information with penalties up to 25 years in prison. Individuals who intentionally access leaked information, including Internet users, would be held criminally liable and face up to 10 years in prison (Freedom House 2014). The act was adopted by the National Assembly in November 2013 but it was sent back for revision since it faced constitutional challenges. The main concerns about the "Secrecy Bill" are related to the fact that the current version seems to undermine basic rights of freedom of expression and the right of access to information protected by the Constitution.

More recently, in order to put in place a coherent and integrated cybersecurity legislative framework to address various shortcomings which exist in dealing with cybercrime and cybersecurity in the country, the Minister of Justice and Constitutional Development published a Draft Cybercrime and Cybersecurity Bill. The Draft Bill has been highly criticized as it undermines constitutional rights which South African citizens are expected to enjoy offline and online (Right2Know Campaign, 2015). Its definition of hate speech seems to be significantly broader than the one contained in the Constitution. The South African Constitution imposes restrictions to freedom of expression related to "a. propaganda for war; b. incitement of imminent violence; or c. advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm." The Draft Bill, though, extends the grounds for hate speech beyond race, gender, ethnicity, or religion. Also, its definitions of harmful content are much broader than the restrictions on freedom of expression defined by the national constitution.

Guidelines for good Internet governance

The South African Internet policy and regulatory framework on cybersecurity appears fragmented, open to abuse and, in



For the sake of cybersecurity, governments enact legislation that broadens control and threatens journalists and whistleblowers.

some instances, also unconstitutional. A government's ability to control content that is available online has profound implications for freedom of expression and censorship. Beyond the more obvious negative impact on users' civil and political rights, information control could also have a negative impact on Internet use and access. This again could be particularly harmful for the economic development of low- and middle-income countries such as South Africa. In addition, risks of Internet control by semi-authoritarian (or authoritarian) regimes are more realistic in these countries. The same is not be expected, for instance, in France or Germany.

The main objective of government should be to preserve the Internet as an engine for social and economic development through the creation of a trusted and secure environment for citizens and business. Thus, an Internet policy should encourage and facilitate an open and competitive online landscape, reaffirming users' rights to free speech and expression and access to information.

Enrico Calandro (Ph.D. BA UCT)
is a senior researcher at Research ICT Africa, an ICT policy think tank based in Cape Town. Prior to joining Research ICT Africa, he worked as a technical advisor for the ICT program of the SADC Parliamentary Forum in Namibia, within the UN technical cooperation framework. He is a recipient of the OTF fellowship on Information Controls, of the Amy Mahan scholarship award for the advancement of ICT policy research in Africa and of the UNDESA fellowship for international cooperation.

Think globally, act locally

Kenya: stakeholder shaping internet regulation on a national level

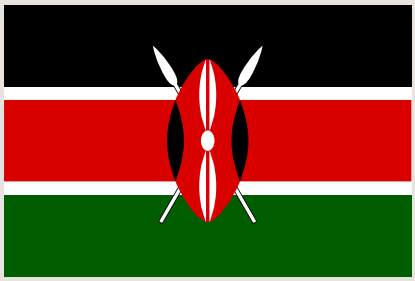
A wide variety of different stakeholders are involved in Internet governance at a national level. Even a single one of these actors can significantly change the rules of the game. For example, in December of 2015, the Communications Authority of Kenya announced that it would enact regulations that make it mandatory for anyone accessing the Internet to submit a personal ID. Users will be required to register using their national identity card, passport or birth certificate. Government authorities will closely monitor the identification process. Unregistered use of internet services will be fined with imprisonment of up to seven years. Digital rights organisations have protested the law and it may end up in court[10].

Regulation / Ministries

- **Ministry of Information, Communications and Technology**
  - Communications Commission of Kenya
  - Communications Authority of Kenya
    - Computer Incidence Response Team (CIRT)
- **Ministry of Defence**
- **Ministry of East African Affairs, Commerce & Tourism**
  - State Department of East African Affairs
  - Directorate of Commerce
- **Ministry of Education, Science & Technology**
- **Ministry of Finance (National Treasury)**
- **Ministry of Foreign Affairs & International Trade**
- **Ministry of Industrialization & Enterprise Development**
- **Ministry of Sports, Culture & the Arts**
  - Department of Film Services
- **Ministry of Transport & Infrastructure**
- **National Cohesion and Integration Commission**
- **Office of the Attorney General & Department of Justice**
- **National Courts**
  - Communications and Multimedia Tribunal

Multistakeholder dialogue

- **Kenya Network Information Centre**
- **Kictanet**
  - Kenyan IGF
- **African Peer Review Mechanism**
  - National Commission
  - National Governing Council



Internet governance in Kenya

Self-regulation / Codes of conduct / Technical standards

Technical community

- Information Systems Audit and Control Association (ISACA) Kenya
- Computer Society of Kenya
- Centre for Informatics Research and Innovation (CIRI)
- ISOC Kenya Chapter
- iHub

Private sector

- Information and Communication Technology Authority (gov. owned)
- Telecommunications Service Providers Association of Kenya (TESPOK)
- Safaricom
- Vodacom
  - M-Pesa
- Airtel Kenya
- The Information Communication Technology Association of Kenya
- Kenya IT & Outsorcing Services (KITOS)
- Media Owners Association

Civil society

- Bloggers Association of Kenya
- Kenya Monitor (citizen journalism)
- Kenya Human Rights Commission
- Kenya Media Editors Guild
- ICT4Democracy
- Mzalendo
- Ushahidi
- Huduma Kenya
- Msema Kweli.
- African Women's Development and Information Network FEMNET

Academia

- Masseno University
- Kenya Education Network
- Multimedia University of Kenya
- Strathmore University Business School
- Kenya College of Communications Technology
- University of Nairobi
- Kenya Institute of Mass Communication
- Kenyatta University
- Kenya Institute for Public Policy Research and Analysis (KIPPRA)

Media Council of Kenya

[10] *Shiundu, Alphonce. 2016. "New Law Tightens Noose on Online Hackers". Standard Digital News. http://www.standardmedia.co.ke/mobile/article/2000186538/new-law-tightens-noose-on-online-hackers. Archived by WebCite under http://www.webcitation.org/6fNqrQDdU*

06
No balancing exercises!

How to deal with conflicts between basic civil rights

David Kaye in interview with Lorena Jaume-Palasí

David Kaye, UN Special Rapporteur on the freedom of opinion and expression, talks about how codes of conduct for online behavior can be governed and about decision-making in cases where rights such as privacy and liberty of speech seem to be at odds with one another.

In the field of Internet governance, we often observe conflicts between basic human and civil rights. Is there really a clash of values?
If you read a bill of rights, for instance, the International Covenant on Civil and Political Rights, as a narrative, you can see how it moves from privacy to the rights to religious belief and conscience, to the absolute protection of opinion, to expression, and then on to political participation. These rights are interrelated. Together, they tell a story! That said: Naturally the full and genuine enjoyment of one of these rights has an impact on the others. Privacy, for instance, is integral to this framework but it is not the only infrastructure of human rights.

Nevertheless, balancing one right against another one often seems necessary. What could be a guideline for decision-making in these cases?
First of all, I do not like speaking about "balancing rights". Take, for instance, article 19 of the International Covenant on Civil and Political Rights. This article provides clear standards: Everyone enjoys certain rights to freedom of expression that may only be restricted when provided for by law, and necessary and proportionate to protect specific legitimate interests, such as national security, public order and the reputation of others. We don't need to undertake balancing exercises in order to evaluate particular limitations on expression.

How about other values and rights. Do they likewise have clear standards?
Take privacy, for instance, which is largely framed by cultural norms: Actually, there is some room in human rights law for taking into account what amounts to "unlawful and arbitrary" interferences with privacy in one's house or in correspondence. But, on the other hand, norms about freedom of expression are clear. From this perspective, allowances for privacy that amount to restrictions on expression must be subject to the standards of Article 19 International Covenant on Civil and Political Rights.

Let's talk about privacy and freedom of expression. For a long time, we have observed a trend which might be called the privatization of the public. Privately-owned shopping malls take over the function of public squares. Social media such as Facebook accommodate a large portion of the public discourse—which means that the rules and mechanisms shaping this discourse are decided upon by a private company. In this respect: Is the Global South any different from the North?
I don't think there is a north-south divide here. Clearly, online space is widely seen as public space, and yet it is privately held, by and large. How that space is governed, how what we express is commodified, and what is done with that as a commodity: These are among the most important questions that states everywhere are seeking to address.

Even if public space is privately owned: Shouldn't basic human and civil rights apply nevertheless?
In the context of expression in online space, we see an increase in codes of conduct for behavior online. Sometimes these are characterized as "community standards", as with Facebook. Often, those standards are contained in a company's terms of service. We can see that these standards aim to tamp down harassment, verbal abuse, misogyny and racism, to name a few of the ills that exist in both digital and physical space. But those problems are not typically prohibited by human rights law. Rather, corporate actors often seek to prohibit this kind of expression as harmful to those who use their platforms or damaging to the kind of space they are trying to create. This may be entirely appropriate, and may be evaluated based on the standards adopted. But we should acknowledge that this kind of regulation—traditionally the province of governmental authorities—is being conceived and implemented by private actors. Sometimes this happens with the guidance of human rights norms. But usually, it happens without such guidance.

David Kaye
is the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, appointed in August 2014. He reports to the UN particularly on issues such as the safety of journalists, restrictions placed on Internet access and the effects of electronic surveillance. Mr Kaye is professor at the University of California, Irvine's School of Law. He teaches international human rights law and international humanitarian law and directs the University of California's International Justice Clinic.

07
Internet governance in the Global South: central topics

How can freedom of expression be fostered?

As a fundamental right, freedom of expression and information has received special attention in the context of digital technologies. Freedom of expression is enshrined among others in article 19 of the International Covenant on Civil and Political Rights (ICCPR), where it is stated that rights to freedom of expression may only be restricted when provided by law and to protect specific legitimate interests (such as national security, public order, and the reputation of others).

Freedom of expression is threatened by censorship, be it by governments (see p. 26), by private companies acting as Internet intermediaries (see p. 22) (such as Internet service providers, search engines or social media platforms), but also by societies intolerant towards minorities. One possibly neglected threat to freedom of expression and information is the prioritization and misuse of concerns such as security (see p. 32) or privacy, which often leads to an illegitimate imbalance. Also, efforts undertaken in order to secure national digital sovereignty often prevent the free flow of information "regardless of frontiers" as convened in article 19 ICCPR.

What is zero rating about and how is it related to freedom of expression and information?

Zero rating is a business model of some Internet service providers and mobile (virtual) network operators. Under zero rating, certain applications or Internet services are exempted from the broadband or mobile data cap (see p. 18).

Cliff Edwards, Netflix spokesperson, sees a few potential threats of zero rating: "[Z]ero rating isn't great for consumers, as it has the potential to distort consumer choice in favor of choices selected by an Internet service provider." Also Internet pioneer Vincent Cerf is often quoted saying "[A]llowing broadband carriers to control what people see and do online would fundamentally undermine the principles that have made the Internet such a success." While the opponents of zero rating fear a deformation and misrepresentation of the information sought in zero-rated applications and services, companies offering zero rating see an opportunity to create and access information. These companies argue that this is the only way for consumers to have access to services they could not afford otherwise. Mark Zuckerberg, for instance, sees zero rating services as a first step for people entering the digital sphere.

How does the multi-stakeholder model of Internet governance work?

Internet governance refers to the regulation of the Internet. Internet governance was born in a context where the main stakeholders involved focused mainly on the technical layers of the Internet (physical and logical layers). Recurring topics were the assignment of globally unique identifiers on the Internet (domain names) or technical standards. Today, Internet governance includes also the many issues relating to the content side of online services. Examples are issues of intermediary liability (see p. 22), copyright, or cybersecurity. At the same time, Internet governance implies a multi-stakeholder process (see p. 16) which has experienced a geographical stratification: from the global level first, over the regional, to the local level (see p. 30).

The multi-stakeholder model of Internet governance has managed to establish itself as a successful model for democratic deliberation (see p. 12).

The Global South is still underrepresented in terms of Internet governance. Local networks are rare and not yet well established. In particular, American and European actors dominate the scene. Of 289 national actors counted in a survey by the NYU GovLab's "Crowdmap of 100+ Internet Governance actors," 125 come from the UK and the US.

Why does privacy matter?

Privacy is a key issue for digital communication in general. With regard to the formation of public opinion, one important aspect is the protection of private communication against intrusions that could reduce the options for political and social dissent, especially of minorities. Here, the protection of privacy has an instrumental value as a safeguard against an autocratic government seeking to eradicate social plurality (see p. 26).

Particularly the protection of journalistic sources, fundamental in order for the press to exercise their role as the "fourth estate" in an accountable and democratic government, may be at stake when national security, law enforcement and cybersecurity restrict privacy rights in a disproportionate way.

On the other side, privacy regulation may be misused to privatize information of public interest that may be unfavorable for governmental institutions and actors as well as other relevant figures of public interest in the business sector, academia or civil society.

References

Access for all—or the end of the Internet as we know it?

Broadband Commission for Digital Development. 2015. "Broadband Targets for 2015." http://www.broadbandcommission.org/Documents/Broadband_Targets.pdf. Archived by WebCite at http://www.webcitation.org/6fJRJGQT9

Galpaya, Helani. 2015. "Reducing inequalities to universal & affordable access to ICTs." http://lirneasia.net/wp-content/uploads/2015/06/2015-05-UNDESAGalpaya-FINAL.pdf. Archived by WebCite at http://www.webcitation.org/6fJQn88EP

Internet Governance Forum 2015 "Zero Rating, Open Internet and Freedom of Expression". https://www.intgovforum.org/cms/187-igf-2015/transcripts-igf-%202015/2932-2015-11-13-ws-79-zero-rating-open-internet-and-freedom-of-expression-%20workshop-room-8-finished. Archived by WebCite at http://www.webcitation.org/6fJRtuvJ2

MacKinnon, Rebecca. 2012. Consent of the Networked: The Worldwide Struggle for Internet Freedom. New York: Basic Books. Morris, Anne. 2015. "Report: 45% of operators now offer at least one zero-rated app – FierceWireless:Europe." http://www.fiercewireless.com/europe/story/report-45-operators-now-offer-least-one-zero-rated-app/2014-07-15. Archived by WebCite at http://www.webcitation.org/6fJRXUEAy

Yoo, Christopher S. 2016. Letter in response to Telecom Regulatory Authority of India consultation on Differential Pricing at http://trai.gov.in/Comments_Data/Others/Yoo.pdf. Archived by WebCite at http://www.webcitation.org/6fJS8Ypzi

Don't shoot the messenger

Ávila, Renata. 2014. "Golpe a la neutralidad de la red en Paraguay." http://pillku.org/article/proveedores-de-internet-bloquean-sin-autorizacion-/. Archived by WebCite under http://www.webcitation.org/6fMloEE4I

Flynn, Sean et al. 2012. "The U.S. Proposal for an Intellectual Property Chapter in the Trans-Pacific Partnership Agreement." SSRN Scholarly Paper ID 2185402. Rochester, NY: Social Science Research Network. Accessed June 2016. http://papers.ssrn.com/abstract=2185402

Meléndez-Juarbe, Hiram A. 2011. "Intermediaries and Freedom of Expression." In: An Internet Free of Censorship. Ed. by Eduardo Bertoni. Bueonos Aires: CELE. http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/04-Intermediaries_Freedom_of_Expression_Hiram_Melendez_Juarbe.pdf. Archived by WebCite at http://www.webcitation.org/6fMlaoBUO

Sutton, Maira. 2014. "State Censorship by Copyright? Spanish Firm Abuses DMCA to Silence Critics of Ecuador's Government." Accessed June 2016. https://www.eff.org/deeplinks/2014/05/state-censorship-copyright-spanish-firmabuses-DMCA

Undermining privacy and freedom of expression in guise of cybersecurity

Association for Progressive Communications (APC); Humanist Institute for Cooperation with Developing Countries (HIVOS). 2014. "Global Information Society Watch 2014. Communications surveillance in the digital age." Accessed June 2016. https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf

Department of Communications. 2013. South Africa Connect: Creating opportunities, ensuring inclusion. South Africa's Broadband Policy. No. 953, 6 December.

Duncan, Jane. 2014. "Protests and the Construction of National Security Threats in South Africa." http://forums.ssrc.org/african-futures/2014/07/01/protests-and-the-construction-of-national-security-threats-in-south-africa/.Freedom House. 2014. "Freedom on the Net". https://freedomhouse.org/report/freedom-net/freedom-net-2014#.Vrr1lvEUQz4. Archived by WebCite at http://www.webcitation.org/6fNuMoqMk

Gillwald, Alison, Mpho Moyo, and Christoph Stork. 2012. "Understanding what is happening in ICT in South Africa. A supply- and demand-side analysis of the ICT sector. Evidence for ICT Policy Action." Reseach ICT Africa, Evidence for ICT Policy Action, Policy Paper Nr. 7. Accessed June 2016. http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_7_-_Understanding_what_is_happening_in_ICT_in_South_Africa.pdf

Grobler, Marthie, Joey Jansen van Vuuren, and Louise Leenen. 2012. "Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward." In ICT Critical Infrastructures and Society, ed. Magda David Hercheui, Diane Whitehouse, William McIver Jr., and Jackie Phahlamohlaka, 215–25. IFIP Advances in Information and Communication Technology 386. Springer Berlin Heidelberg. Ms. Accessed January 2016 http://krr.meraka.org.za/~lleenen/Grobler_Final.pdf

Rich, Cynthia. 2015. "Privacy Laws in Africa and the Middle East." Bloomberg BNA Privacy and Security Law Report. http://www.mofo.com/~/media/Files/Articles/2015/06/150615BloombergPrivacyAfricaMiddleEast.pdf. Archived by WebCite at http://www.webcitation.org/6fNuvyX4u

Right2Know. 2015. "Hands Off Our Internet." Accessed June 2016. http://www.r2k.org.za/handsoffourInternet/

About us

iRights

is a non-governmental organization based in Berlin. Consisting of iRights e.V., a charitable non-profit, and the independent think tank iRights.Lab, we have been active at the intersection of digitization and society for more than ten years. Since 2005 we publish the iRights.info online platform, one of Germany's premier resources for information and discussions on copyright, privacy, media freedom and Internet governance issues. We develop joint projects and provide research and consultancy for a wide range of stakeholders: foundations and other NGOs, government and public entities, private companies, academic institutions and individuals. Our mission: To harness the opportunities of digitization for the promotion of democracy and the public good. Our approach: We offer our expertise and create spaces for the cooperative development of practical outcomes and solutions.

iRights.Lab
Almstadtstr. 9/11 | 10119 Berlin, Germany

T +49.30.893 70 103
m.spielkamp@iRights-lab.de

iRights-lab.de
@iRightslab

Made for minds.

DW Akademie

DW Akademie is Germany's leading organization for media development and Deutsche Welle's center of excellence for education and knowledge transfer. As a strategic partner of Germany's Federal Ministry for Economic Cooperation and Development we strengthen the universal human rights of free expression, education, and access to information.

DW Akademie
53110 Bonn, Germany

T +49.228.429-0
info@dw-akademie.com

dw-akademie.com
facebook.com/DWAkademie

facebook.com/DWAkademie

dw.com/newsletter-registration

@dw_akademie

#mediadev – dw.com/mediadev

dw-akademie.com