United Nations
Educational, Scientific and
Cultural Organization

IPDC THE INTERNATIONAL PROGRAMME FOR THE DEVELOPMENT OF COMMUNICATION

CI-14/CONF.202/Inf.4
10 October 2014

BACKGROUND DOCUMENTS
FOR THE THEMATIC DEBATE:

"ONLINE PRIVACY AND FREEDOM OF EXPRESSION"

IPDC INTERGOVERNMENTAL COUNCIL
(Twenty-ninth session)

UNESCO HQ, PARIS

20-21 NOVEMBER 2014

TABLE OF CONTENTS

Agenda item:

THEMATIC DEBATE: "**ONLINE PRIVACY AND FREEDOM OF EXPRESSION**"

CONCEPT NOTE

EXECUTIVE SUMMARY

The 57th meeting of the IPDC Bureau agreed on the topic of 'Online privacy and freedom of expression' for the thematic debate at the 29th Council Session in November 2014. There are issues related to protection of each of these two rights online. The topic connects to Resolution 52 concerning Internet-related issues, adopted by the 37th General Conference of UNESCO in 2013. Five invited experts will have the opportunity to present at the session, with Council Members discussing the issues raised. The debate will be referenced in the Internet-related issues study, which itself will be presented to the 38th General Conference in November 2015. Regional representation and gender balance have been taken into account when inviting experts.

BACKGROUND

UNESCO is the United Nations specialized agency with a mandate to defend and promote freedom of expression and its corollary freedom of information. By Resolution 52 of the 37th General Conference in 2013, UNESCO is mandated to conduct a comprehensive and consultative study on Internet-related issues within its mandate, including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society, the results of which should include options that inform the Organization's reporting to the 38th General Conference in 2015. The study explores freedom of expression and privacy, amongst other issues of concern, and within the UNESCO conceptual framework of "Internet Universality" which promotes that Internet should be (i) human **Rights-based** (ii) "**Open**", (iii) "**Accessible to all**" and (iv) nurtured by **Multi-stakeholder participation**.
United Nations Human Rights Council Resolutions 20/8 and 26/13 on "The promotion, protection and enjoyment of human rights on the Internet" affirm that the same rights that people have offline must also be protected online. These rights include freedom of expression, the right to information, and privacy, as also affirmed in the Final Statement of the World Summit on the Information Society (WSIS)+10 review event held at UNESCO in February 2013.

In consultations with UNESCO Member States on the Internet-related issues study during early 2014, the 29th Council session of IPDC was identified as one opportunity to take forward the research and discussion. The subject relates to IPDC's mandate, which includes securing a healthy environment for the growth of free and pluralistic media in developing countries. IPDC also works to promote freedom of expression as well as innovation with regard to trends in communication. The Council sessions always feature thematic debates, and this lends itself to providing Member States with new information. This year's Council session represents an opportunity for Member States to respond in a way that can be factored into the Internet-issues study report.

SCOPE

The key issue in this thematic debate is the place of the rights to freedom of expression and privacy in the online environment. Amongst the many issues around these are those of balancing these rights in relation to each other, and to other rights (such as the right to life, liberty and security of person; and the right to

development), how these rights can be protected across jurisdictions, and how balances can be established.

Five specific sub-topics of relevance to the Internet-issues study can be addressed in this regard. Elaborated below, these are: the "right to be forgotten"; privacy issues; post-2015 development, jurisdictional overlap and the multi-stakeholder model. Given the forum of IPDC, the focus will be especially on how these issues relate to media and to journalism.

As the concept note for the Internet-issues study noted, there is a complex balance between the two rights:

> UNESCO follows the Universal Declaration of Human Rights (UDHR) which states that human rights are indivisible, recognizing thereby that particular actions concerning the right to privacy can impact on other rights, such as the right to freedom of expression, and vice versa. As noted in 37 C/Resolution 52, "privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and […] such privacy should not be subject to arbitrary or unlawful interference". At the same time, as noted in the Discussion Paper prepared for the 37th General Conference, privacy may also not be used to shield violations of individual rights or to block the media from exposing these. Public interest must enter any calculation of reconciling rights, and Article 29 of the Universal Declaration of Human Rights sets out this test for the purpose and method required in this regard: "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."

These conditions for balancing all rights govern any legitimate limitation of rights, including in cyberspace. Particular aspects of cyberspace add further complexity to the equation of protecting rights against violations. Five specific issues can be identified that especially reveal this complexity:

(i) The 'right to be forgotten'

This issue was evident in the recent European Court of Justice decision[1] on a "right to be forgotten", which required Google to remove a link to an online newspaper archive, although it did not require that archive to remove the e-article. At the same time, the Court stated that its ruling to delete search results about a particular individual's history would not apply to other information where there was overriding public interest in being able to discover the relevant facts. This issue about protecting individuals' rights to privacy and reputation, without violating freedom of expression and public interest, is one that merits unpacking.

(ii) Privacy issues in the digital age

The Internet lends itself not only to expanded freedom of expression, but also to expanded electronic tracking, surveillance and data-mining by various actors which can intrude on personal privacy and thereby also, in turn, have a chilling effect on online expression. In this way, for example national security issues in the online environment may compete with online privacy

[1] European Commission. Factsheet on the "Right to be Forgotten" ruling. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

and/or free expression, whose balance international standards should help to inform. What this means in less general terms is not resolved. The UN General Assembly and the Office of the High Commissioner for Human Rights both underlined the importance of states reviewing their laws, policies, procedures and practices to enhance independent oversight and transparency. One debate is over more specific principles that could inform this exercise.

(iii) Post-2015 development and the Internet

Where free expression and the Internet fit into the post-2015 development agenda is a matter currently in debate. The extent to which these are background or extraneous issues, or whether they are fundamental to sustainable development is of global relevance. The 10-year review of the World Summit on the Information Society coincides with the process defining the post-2015 development agenda, thereby offering the international community an opportunity to consider the role of information and communication technologies and the Internet within the wider development agenda. Can development be conceived without specific reference to the rights to impart and receive information, and how does the Internet facilitate the right to development? How can "Internet development" be measured?

(iv) Jurisdictional overlap

Most of the Internet operates as a transnational information and communication space with many key Internet intermediaries operating in a cross-border manner. This frequently raises questions about competing jurisdictions where different interpretations and regimes exist concerning limits on privacy and/or free expression, but where actors within a given state may have access to content held or circulating outside that state. In this context, process-oriented options beyond a "clash of jurisdictions" can be explored which may provide for a balancing of rights according to local interpretation but also without any national limitation involved crossing the threshold and becoming violations.

(v) Multi-stakeholder model

Multi-stakeholder participation is a principle affirmed in the Final Statement of the WSIS+10 Review Event, which was endorsed at UNESCO's 37th General Conference in 2013. It is also part of the draft concept of Internet Universality, alongside human rights, openness and accessibility. There are debates about the meaning of multi-stakeholder model, and the realms to which it applies. One debate is whether the multi-stakeholder model of Internet governance apply not only to the governance of infrastructure and critical internet resources, but also to selected policy issues, such as those related to privacy and freedom of expression. The multi-stakeholder model may have a valuable place in establishing balances of human rights online.

FORMAT AND SPEAKERS

The format is that the moderator to introduce the Internet-issues Study and provide an update on its progress, and then the five experts will each tackle one of the topics above. Each speaker will have 10 minutes to present. Subsequently, Member States will take the floor, and at the end, speakers will each have 5 minutes to respond to points made.

HIGH COMMISSIONER FOR HUMAN RIGHTS' REPORT ON THE RIGHT TO PRIVACY

Mona Rishmawi, Chief, Rule of Law, Equality and Non-Discrimination Branch, Research and Right to Development Division, Office of the High Commissioner for Human Rights

In resolution 68/167, the General Assembly requested the High Commissioner for Human Rights to submit a report on "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale". This report was presented to the Human Right Council in Geneva last September and will be presented at the present session of the General Assembly in New York.[2]

Surveillance practices can have a very real impact on peoples' human rights, including their right to privacy, and their rights to freedom of expression and opinion, to freedom of assembly, to family life and to health.

As the High Commissioner's report makes clear, international human rights law provides a robust and universal framework for promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance; the interception of digital communications; and the collection of personal data. However, practices in many States reveal a sometimes deliberate lack of adequate national legislation and enforcement; weak procedural safeguards; and ineffective oversight. This contributes to widespread impunity for arbitrary or unlawful interference in the right to privacy.

The very existence of a mass surveillance programme regarding email communication and other forms of digital expression creates an interference with privacy, and the onus is on the State to demonstrate that its interference is neither unlawful nor arbitrary. The report notes that State surveillance of electronic communications data may be a legitimate law enforcement measure –if it is conducted in compliance with the law. But States must demonstrate that the surveillance is both necessary and proportionate to the specific risk being addressed. States have an obligation to ensure that individuals' privacy is protected by law against unlawful or arbitrary interference. All forms of communications surveillance must be conducted on the basis of publicly accessible law; and this law must in turn comply with the State's own constitutional regime and international human rights law. International human rights law is also explicit on the principle of non-discrimination. States must take measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity -- regardless of the ethnicity, nationality, location or other status of the people whose communications it is monitoring.

Procedural safeguards and effective oversight are crucial for safeguarding the right to privacy in law and in practice. A lack of effective oversight has contributed to impunity for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Moreover, States have a legal obligation to provide effective remedies for violations of privacy through digital surveillance, in judicial, legislative or administrative forms, with procedures that are known and accessible.

As regards the role of the private sector, Governments increasingly rely on corporations to conduct and facilitate digital surveillance. There may be legitimate reasons for a company to provide user data. However, when the request is in violation of human rights law, or where the information is used in violation of human rights law, that company risks being complicit in human rights abuses.

[2] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

LEGAL POSITION ON THE RIGHT TO BE FORGOTTEN

Ronaldo Lemos,[3] Director Institute for Technology & Society of Rio de Janeiro

The "right to be forgotten" is a legal conceptual construct, one that has not been yet recognized by international law. Even at regional or national levels, the "right to be forgotten" emerges in connection with only a few jurisdictions, and with regard to specific contexts of the law, such as the right to privacy and the field of data protection. Nonetheless, in May 2014, the European Court of Justice delivered a specific decision, based on the EU's 1995 Data Protection Directive, which materializes the "right to be forgotten" in more elaborate terms. The Court held that "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relation to that person[4]."

The Court also recognized that the "right to be forgotten" is not absolute, and needs to be balanced against other fundamental rights[5], such as freedom of expression and of the media. Several problems arise from the "right to be forgotten" as materialized by the Court's ruling. One of them is that such materialization of the "right to be forgotten" incentivizes the exercise of "privatized censorship": online service providers (OSPs) become day-to-day judges of what information is to be deemed, in the words referred by the Court, "inaccurate", "inadequate", "irrelevant" or "excessive", and therefore suppressed *ad limine* upon request.

In addition, the abovementioned criteria are highly subjective. There are no objective standards to determine the words held by the court: "inaccuracy, inadequacy, irrelevance or excess". Hence the only acceptable way to determine whether any of these criteria apply is through *due process of law*. Any form of private or expedite removal of speech on the grounds of the "right to be forgotten" that does not go through the full analysis of natural courts - respecting *procedural and substantive due process* - shall be considered as potentially undermining public liberties.

Moreover, other traditional remedies exist, and are less disproportionate than the "right to be forgotten". Historically, many jurisdictions have adopted legal institutes such as the "right of reply" and the "right of rectification". Both are preferable and more objective than the vague concepts underlying the "right to be forgotten".

Even those legal institutes, such as the "right of reply", have to be carefully balanced with freedom of speech, of the media and the press, especially in the online context. In this sense, Frank La Rue, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has stated in his report: "…*the Special Rapporteur emphasizes that due to the unique characteristics of the Internet, regulations or restrictions which may be deemed legitimate and proportionate for traditional media are often not so with regard to the Internet. For example, in cases of defamation of individuals' reputation, given the ability of the individual concerned to exercise his/her right of reply instantly to*

[3] Ronaldo Lemos is the director of the Institute for Technology & Society of Rio de Janeiro (ITSrio.org) and professor of law at the Rio de Janeiro State University. He has a master in laws degree from Harvard University, and a bachelor and doctor in laws degree from the University of Sao Paulo. He is one of the architects of the "Marco Civil da Internet", a bill of rights for the Internet passed into law in Brazil in April 2014 protecting freedom of expression and privacy online, as well as network neutrality. He is also a non-resident visiting scholar with the MIT Media Lab.

[4] http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

[5] "*the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive*"
http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

restore the harm cause, the types of sanctions that are applied to offline defamation may be unnecessary or disproportionate[6]".

If remedies to defamation cases are to be mitigated online because of the ability to reply instantly, the rapporteur's argument becomes even more in point regarding the "right to be forgotten". In this sense, the "right to be forgotten" often deals with requests to remove links to established facts or other forms of objective information. The interested individual continues at all times to have the possibility to counter the information he/she wants to suppress with more information, rather than requesting its removal. That is a more proportionate outcome under the general principles of law.

Moreover, Brazil has recently adopted the "Marco Civil da Internet" law, which is relevant to the present discussion. The applicable principle under the Marco Civil is that *due process* and *prior ruling by courts* cannot be rescinded. OSPs have no legal obligation to remove speech or links to speech motivated by private requests, including in regard of the "right to be forgotten". The Brazilian legislator has decided that OSPs enjoy a safe harbor against such private claims. In other words, the courts cannot be kept at bay whenever freedom of speech, of the media and the press are involved.

That emphasizes once again the need for *due process.* The decision and corresponding reasoning in support of suppressing links should be the registered by public court records. If links are suppressed privately, by means of decisions made by OSPs, no public records are produced. That is especially relevant in view of the vagueness of words such as "inaccurate", "inadequate", "irrelevant" or "excessive", which provide leeway for mistakes and abuse, which the transparency of public court records can curb.

Finally, the "right to be forgotten" also conflicts with the *right to a shared past*, something that should be of especial concern for the UNESCO Member States. That idea has been exemplified by Eduardo Bertoni in his article "The Right to Be Forgotten: An Insult to Latin American History[7]". Bertoni claims that "rather than promoting this type of erasure, [Latin American countries] have spent the past few decades in search of the truth regarding what occurred during the dark years of the military dictatorships." In contemporary societies that become increasingly digital, the "right to be forgotten" can open new avenues for undesired historical revisionism.

On a final note, I have argued on the side of Eduardo Bertoni's view, in favor of the need to preserve and promote the accessibility to digital archives, rather than their deletion or de-linking[8]. One significant example is the destruction in Brazil in the 1980's of the court files regarding a labor accident involving a machine worker called Luis Inácio Lula da Silva. The files were destroyed because they were considered "irrelevant" at the time. In 2001 that machine worker was elected president of Brazil.

[6] http://www2.ohchr.org/en
glish/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[7] http://www.huffingtonpost.com/eduardo-bertoni/the-right-to-be-forgotten_b_5870664.html
[8] http://revistatrip.uol.com.br/revista/205/colunas/salvem-a-memoria-do-orkut.html

PRIVACY ISSUES IN THE DIGITAL AGE

Nighat Dad, Executive Director Digital Rights Foundation

The internet and other technological advancements in the field of communication have provided individuals with new ways and means of communication, thus opening a new medium for freedom of expression, especially for dissident groups and human right defenders, and more generally for citizens wishing to engage in civic issues and connect with the world beyond their national borders. On the other hand, with the increasing and ubiquitous use of the internet, we are witnessing tighter control exerted by states around the world. Such practices have been well-documented thanks to the work of whistle-blowers and investigative journalists.

Whilst governments have a responsibility to protect all their citizens, and in fact all those present within their territory, from threats such as terrorism, they also have a positive obligation to respect and protect the fundamental rights and freedoms of individuals, both citizens and non-citizens. Certain rights can be legitimately restricted in narrow circumstances for reasons such as national security and public safety, in accordance with the law.

To achieve such a balance in which both human rights and national security concerns are respected, it is important to have guidelines that could help States develop an online environment that does not hamper individuals' privacy and freedom of expression.

Freedom of expression and privacy form a foundation for many other human rights that UNESCO is mandated to promote, including freedom of expression, access to information and knowledge, and education. An understanding of the right to privacy as a basic universal right is upheld by several UN treaties and conventions, as well as at the domestic level in national constitutions and laws.

As underlined in the July 2014 report by the UN High Commissioner for Human Rights, in view of the current practices in which States have been operating to conduct surveillance, there is a need for a review of the checks and balances of laws and regulations related to communications surveillance to ensure they adhere to international human rights law and adequately protect the rights to privacy and freedom of expression. The *International Principles on the Application of Human Rights to Communications Surveillance*,[9] developed by a coalition of civil society, privacy and technology experts, provide a useful framework to consider communications surveillance in the context of the internet. Some key elements include:

- In addition to clear and effective protection of privacy through constitutional protection, a robust data protection regime, and strong legislation, States should adopt specific regulations of communications surveillance by law enforcement and intelligence agencies that ensure effective oversight, accountability and transparency. These must be up-to-date, accessible to and understood by all

- Surveillance must be carried out in accordance with the law and meet the principles of legitimacy, legality, proportionality and necessity. Mass surveillance can never be proportionate in a democratic society because it fundamentally undermines the key tenants of the rule of law and hampers human rights. If a genuine national security concern arises leading to a request for targeted surveillance, it should be followed with non-discriminatory action towards the target after

[9] http ://necessaryandproportionate.org

having followed a transparent and open process by a competent judicial authority in order to provide justification for authorisations given to conduct surveillance.

- Communications surveillance by both state bodies and intelligence agencies should be subjected to effective oversight and accountability. There should be an increased level of transparency and oversight of their policies and practices.

- State practices and policies should not undermine a free Internet. On the contrary, governments must promote, not undermine, the security of online communications, by enabling free and secure access to tools that enable users to engage online freely, without fear, and anonymously. This would allow the internet to remain an open and secure space for individuals to enjoy their fundamental rights of freedom of expression and access to information.

- Lastly, any decision to conduct surveillance must be authorised by a competent judicial authority. The judiciary should oversee and give prior approval for communications surveillance to determine if a certain case will affect citizens' privacy rights, and to balance such a request with the public interest. Considering the judiciary to be an independent branch, it is best placed to decide if a request for surveillance is legitimate and if it is necessary for the investigation of a case.

POST-2015 DEVELOPMENT AGENDA AND INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTS)

Fatou Jagne Senghore, Regional Director ARTICLE 19 Senegal/West Africa

The right to development, although not entirely recognized universally, is particularly relevant to African countries. This perspective reinforces the significance of ICTs and freedom of expression for the continent's future, and the relevance of these matters to UNESCO's "Priority Africa". Freedom of expression incorporates the right to seek and receive information, and that in turn is linked to transparency. Against this background, and in the context, of the Post-2015 Development Agenda, the African Declaration on Internet Rights and Freedoms has been developed.

Why are access to information and transparency important?

Expression, transparency and the free flow of information reduce corruption and play a vital role in ensuring accountability at all levels. The availability and accessibility of information empowers people to assert their rights and their entitlement to public services. It also promotes accountability in development by facilitating monitoring by civil society, international bodies and others on how governments are meeting their commitments. A lack of access to means of expression and to public information has often been identified as a significant problem with achieving the Millennium Development Goals (MDGs). ICTS, and especially an Internet that is shaped by concerns about rights, are fundamental enablers for providing access to information, to voice, and to transparency.

UN process

Throughout the negotiations on the post-2015 development agenda, some civil society groups and Member States called for a specific Sustainable Development Goal related to good governance and for the inclusion of access to information, free speech, public participation and human rights were raised by civil society and member states. The final outcome document of the Open Working Group (OWG) included targets on access to information, but weakened the text on human rights, dropping explicit mentions of the freedom of speech, media, association and assembly.

Access to ICTs as a means of implementation of the post-2015 development agenda

Using ICT infrastructure can help speed up the delivery of services, provide access to crucial information and enable public participation in policy and implementation. Civil society organizations and public institutions like libraries can use ICTs to bridge the gap between national policy and regional implementation, ensuring that development is shaped by, and reaches, all communities.

By providing direct support to facilitate access, including by providing public information online, and by establishing community-based ICT centres and other public access points, States can provide public forums and space for wider civil society participation and engagement in decision-making. The latter recommendation is consistent with the recommendations of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and his August 2011 report on Access to the Internet.

Notwithstanding the clear linkages between development and freedom of expression, access to information, transparency and ICTs, these issues received little attention during the OWG discussions and

were not included in specific meaningful form in the final version.

African Declaration on Internet Rights and Freedoms

The potential of Internet and ICTs to contribute to development and democracy in Africa is encapsulated in the recently launched African Declaration on Internet Rights and Freedoms.

The 23 civil society organizations that developed this Declaration appreciate that UNESCO's Deputy Director-General welcomed the initiative of the African Declaration at the launch event during the recent Internet Governance Forum.

The Declaration must be a stepping-stone for understanding the link between the right to development and ICTs based on the protection of digital rights, including freedom of expression and the right to privacy online in Africa.

The Declaration seeks to provide guidance as to how these rights should be implemented or interpreted by policy makers and courts respectively, taking cognizance also of matters of special relevance to Africa such as access and multi-lingualism.

We see the Declaration as the first in a series of standard-setting instruments for the protection of human rights on the Internet in Africa, and for the potential of the Internet to contribute to the right to development. Whilst these principles are well-developed in other regions of the world, particularly Europe and increasingly the Americas, our regional mechanisms in Africa need to step up to provide guidance to policy-makers in the region to protect our rights online. Civil society will make use of the Declaration in dialogue with national and regional institutions across Africa, and we will also contribute it to the UNESCO Internet-Issues Study.

THE MULTI-STAKEHOLDER MODEL AND JURISDICTION

Bertrand de La Chapelle, Director Internet & Jurisdiction Project

Internet Governance[10] is a topic more present than ever on the international agenda and in the media. This brief document highlights key points as relevant to cross-jurisdictional issues. Transnational online spaces and services create unique social, political and economic benefits for mankind. However, as online interactions increasingly involve Internet platforms, technical operators, servers and users based in different physical locations, determining one single applicable law on the basis of traditional territorial criteria becomes difficult or even impossible. This is especially evident for user-generated content and in particular speech-related issues, for which national rules greatly vary. Collisions between these often incompatible national laws create increasing tensions between public authorities, Internet platforms or operators, and users across jurisdictions.

Jurisdiction and privacy:

- Surveillance, tracking and data-mining raise increased concerns now that individuals voluntarily post considerable amounts of data on social media - with the expectation that it will be kept for a long period of time - and that the amount of data automatically collected is growing exponentially.
- This qualitative transformation challenges the existing balance of most privacy regulations, and even sometimes the very concepts upon which they were built (consent, limitations on collection, retention, purpose or reuse), at the very time when the use and reuse of data increasingly appears as a main future source of social and economic value creation.
- In this context, two opposite trends are worrisome: extra-territorial extension of sovereignty in access to user data and "data localization". The former breaches the very principle of sovereignty. The proliferation of the latter, beyond its technical impracticality, would harm innovation and the very benefits of a cross-border infrastructure.
- Faced with the risk of unbridled legal competition between countries and the proliferation of uncoordinated unilateral decisions in the name of security, more attention should be given to 1) the creation of transborder frameworks ensuring due process and oversight mechanisms, and 2) the development of a balanced privacy regime that both protects the rights of individuals and allows for social and economic value creation.

Jurisdiction and the "Right to be forgotten":

- The Court of Justice of the European Union (CJEU) decision is more of a right for a specific link to be de-indexed in a search on someone's name than a full "right to be forgotten", which is a broader concept.
- Although the decision was in relation to Google and on the basis of a European Directive, the decision is already being applied by other search engines and in other regions.
- This issue is not simply a regulatory or business matter but touches upon social dimensions in the digital age regarding identity and memory at both the individual and collective levels.
- Most importantly, the CJEU decision has given to a particularly important category of private actors (search engines) a quasi-judiciary role to determine a delicate balance between fundamental rights (privacy on one hand and, on the other, freedom of expression or the right of the public to know).

[10] The now famous 2005 definition of Internet Governance in the WSIS Tunis Agenda is : "*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*"

Although they did not ask for this responsibility, it behooves companies to exercise it with a great attention to due process and transparency.

- This issue touches a very diverse set of actors including: search engines and theirs users, but also various Ministries inside each government, Data Protection Authorities, hosting companies, publishers and webmasters, NGOs and a broad range of academic sectors.
- Several processes are currently under way among these different groups, potentially leading to incompatible sets of criteria and procedures. Auditions by the Data Protection Authorities (DPAs) and the Advisory Council set by Google demonstrate the need for a multi-stakeholder dialogue process to define a comprehensive and balanced implementation framework.

On Jurisdictional overlaps:

- Jurisdictional overlap is not a flaw in the Internet but the natural and unavoidable consequence of its most useful feature: its enabling of communications and services that connect humans across borders.
- The tension created by the collision of national laws cannot be resolved by a rigid imposition of the Westphalian geographic criteria of sovereignty. Traditional conflict of laws rules currently produce a legal competition among states and this has negative unintended consequences for all, threatening the benefits of the network itself.
- Sovereignty remains the core foundation of the international order but its exercise in the digital age imparts governments a responsibility to take into account the transboundary impact of national decisions.
- In situations where substantive harmonization is not a credible perspective, including many aspects of freedom of expression, procedural interoperability and mechanisms for disputes are among the few avenues to alleviate tensions and solve the jurisdictional conundrum. Maintaining transnational spaces requires coordinated efforts. However, traditional modes of inter-state legal cooperation are not adapted: MLATs, when they exist, are limited in scope and scalability, while a global harmonization of content-related national laws appears unworkable. In this context, requests by authorities for domain seizures, content takedowns and access to user data are increasingly sent directly, i.e. transnationally, to Internet platforms or operators in other countries. This solution however currently lacks clear procedures and transparency
- To ensure due process in the management of such transborder requests, agreed procedural interfaces are needed between states, platforms and operators, as well as users to enable the coexistence of diverse laws in shared cyberspaces. The Internet & Jurisdiction Project seeks to develop such a transnational due process framework in a multi-stakeholder process.

On the multi-stakeholder model and jurisdiction:

- In 2013, participants in the global dialogue process facilitated by the Internet & Jurisdiction Project identified six fundamental building blocks for such a transnational framework: Authentication, Transmission, Traceability, Determination, Safeguards and Execution.
- Numerous consultations with stakeholders around the world have since then defined corresponding operational components related to the phases of request submission and request handling
- For the way ahead, the Internet & Jurisdiction Project will engage in intensive stakeholder interactions and outreach to further refine and validate the draft framework.
- It will also engage in detection, documentation and formalization of emerging procedural norms and standards, and definition of dispute management channels and procedures.
- The Project will also prepare pilot implementation with a core group of entities

More information about the Internet & Jurisdiction project: www.internetjurisdiction

THE POTENTIAL OF THE MULTI-STAKEHOLDER MODEL TO ENSURE POLICY ISSUES AND SUSTAINABLE DEVELOPMENT

Moez Chakchouk PhD.: Internet & Media Governance Expert, Chairman and CEO of the Tunisian Internet Agency

The "multi-stakeholder" governance model which evolved out of the World Summit on the Information Society is a difficult concept to implement, but it is also a unique opportunity for countries to develop not only their economies but also social relations and many other benefits.

This governance model strengthens the relationships between the different actors, representing the driving force that can lead a country towards sustainable development. The multi-stakeholder model is an alliance of all parties related to information and communications technologies (ICTs). Therefore, we have to define, and not limit, their roles and operating processes.

Government's role needs consideration, as the discussion about governance and the Internet cannot be left to governments alone. Especially after the Snowden leaks on surveillance, governments should open the debate on internet policies to the public.

Governments have a primary role in providing an inclusive and equitable framing for Internet governance policy discussions. Openness is vital to build or restore the trust between different actors in cyberspace and beyond. Even on defined issues where governments have the final decision-making, which should not be all areas of the Internet, multi-stakeholder consultation is valuable. Public debates give the sector a faster dynamic, and through interaction between actors we can reduce conflicts and promote innovation.

Within this framework, the private sector must also act in supporting innovative and consultative initiatives, including in making more efforts in protecting and promoting human rights online. An example is to avoid the current tension driven by the sale of surveillance technologies to repressive regimes. For their accountability too, companies need to make more efforts regarding transparency and users' privacy protection. For example, to adhere to the UN guidelines for business and human rights, and to consider affiliation to the Global Network Initiative that recommends publishing transparency reports. They should be practice multi-stakeholder consultation around these issues, and be active in multi-stakeholder dialogues more broadly.

Representatives of civil society, as bearers of voice, have a huge effort to make in encouraging individuals to engage in Internet governance debates. They also have a role in monitoring the Governments' and companies' actions.

International NGOs and coalitions as UNESCO, ITU, Council of Europe and the Freedom Online Coalition, exist to foster cooperation through inter-action and advance global efforts towards expanding access and protecting human-rights principles for the Internet.

Together all these actors, through the multi-stakeholder model, can face several threats on the Internet, such as cybercrime issues. If we do not adapt our policy, not only towards more national openness and multi-stakeholder engagement, but also internationally through more cooperation, we will risk disconnection, and we could fail in our counter-terrorism battle and other existing risks.

The Internet has changed the way we express our ideas, in addition to the fact that access to information and to an affordable Internet is a top global priority. We know also that the Internet can be a catalyst of

growth in any economy, especially in developing countries, and a contributor to the post-2015 development agenda.

It is in this context that multi-stakeholderism stands as the best model for ensuring the Internet is a factor for human rights promotion, social cohesion and sustainable development. It is therefore essential that the Internet to be governed by all and that they share its benefits.