CONFERENCIA INTERNACIONAL

DERECHOS HUMANOS EN LA ERA DIGITAL

Program

0800 – 0900	Registration
0900 – 0910	Opening Ceremony
0910 – 1000	**Keynote Conference:** ***Opportunities and Challenges for Human Rights Protection in Digital Environments*** Toby MENDEL, Executive Director, Centre for Law and Democracy, Canada
1000 – 1030	Refreshments break
1030 – 1200	**Plenary Session 1:** ***National, Regional and International perspectives on human rights issues on the Internet*** **Moderator:** Amalia TOLEDO, *Karisma* Foundation **Panelists:** • Toby MENDEL, Executive Director, Centre for Law and Democracy, Canada • Ramiro ÁLVAREZ, Director of Access to Information Department, *Asociación por los Derechos Civiles*, Argentina • Andrea BONNET, Intellectual Property Counsel, Ministry of Foreign Affairs, Colombia • Fabiola CARRIÓN, Policy Counsel, Access, USA
1200 – 1400	Lunch
1400 – 1530	**Plenary Session 2:** ***Exceptions and limitations as balance instruments of human rights in copyright legal framework*** **Moderator:** Luisa GUZMÁN, *Karisma* Foundation **Panelists:** • Juan F. CÓRDOBA, Law Professor, *Universidad de la Sabana*, Colombia • Carlos A. CORREDOR, Head of the Register Office, National Directorate of Copyright, Colombia • Mike GODWIN, Senior Legal Advisor on Global Internet Policy Program, Internews, USA • Peter Jaszi, Law Professor, American University, USA
1530 – 1600	Refreshments break
1600 – 1730	**Plenary Session 3:** ***Liability of Internet service providers and content removal procedures*** **Moderator:** Carolina BOTERO, *Karisma* Foundation **Panelists:** • Liliana ARIZA, Counsel of the Directorate of Foreign Investment and Service, Ministry of Commerce, Industry and Tourism, Colombia • Fabiola CARRIÓN, Policy Counsel, Access, USA • Carlos CORTÉS, Legal Advisor on media regulation, Internet and technology, Colombia • Francisco VERA, Senior Policy Analyst, Access, USA • Lorenzo VILLEGAS, Law Professor, *Universidad de los Andes*, Colombia
1730 – 1800	Closure

Simultaneous translation will be provided into the working languages of the conference (English and Spanish). The translation will be done by Mateo Reyes, frontera.traduccion@gmail.com.

Follow us on social media with the hashtag **#DigitalDDHH**.

This conference is organized by Karisma Foundation with support of Google, Universidad del Rosario, Foundation for the Press Freedom (FLIP, in Spanish), Open Society Justice Initiative, Access, Internews, American University and RedPaTodos.

CONFERENCIA INTERNACIONAL

DERECHOS HUMANOS EN LA ERA DIGITAL

Biographies

Toby Mendel is the Executive Director of the *Centre for Law and Democracy*, a Canadian-based international human rights NGO that provides legal and capacity building expertise regarding foundational rights for democracy, including the right to information, freedom of expression, the right to participate and the rights to assembly and association. Prior to that Toby was for 12 years Senior Director for Law at *Article 19*, a human rights NGO focusing on freedom of expression and the right to information. He has provided peak level expertise on these rights to a wide range of actors including the World Bank, various UN and other intergovernmental bodies, and numerous governments and NGOs in countries all over the world. This includes law reform work in 2012 in Bhutan, Egypt, Morocco, Myanmar and Tunisia. Before joining Article 19, Toby worked as a senior human rights consultant with Oxfam Canada and as a human rights policy analyst at the Canadian International Development Agency. He has published extensively on a range of freedom of expression, right to information, communication rights and refugee issues, including comparative legal and analytical studies on public service broadcasting, the right to information and broadcast policy.

Ramiro Álvarez Ugarte is an attorney from the *Universidad Católica de Argentina*. He holds masters degree in Journalism from the *Universidad de San Andrés*, and in Law (LL.M) from Columbia University, where he was a Fulbright and Harlan Fiske Stone Scholar. He has served as Legal Advisor at the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights. Ramiro has also worked as a journalist in a variety of media outlets in Buenos Aires. Since 2009, he works with the Argentina organization *Association for Civil Rights* in the area of Freedom of Expression and, currently, as Director of the Access to Information Department. Ramiro teaches Constitutional Law at the *Universidad de Palermo*.

Andrea Cristina Bonnet López is an attorney with a master's degree in Intellectual Property and Commerce from the International Studies Center on Intellectual Property, University of Strasbourg, France, and a master's degree in International Human Rights Protection from the *Universidad de Alcalá*, Spain. She currently serves as Counsel to the Colombian government in international intellectual property issues, especially those that are negotiated at the World Intellectual Property Organization. Andrea is the author of data protection articles; her most recent book, published last year in France, is entitled ***Profitability or Health: The challenge for developing countries***. She has lectured on data protection, right to privacy and traditional knowledge at Colombian universities.

Fabiola Carrión is currently Policy Counsel at *Access*, an international human rights organization that defends and extends the rights of Internet users at risk worldwide. In this role, Fabiola leads the digital due process initiative – protecting the right to fair trial in digital spaces. She has over ten years of experience in human rights, including access to telecommunications, women's rights and criminal justice. Fabiola has worked a consultant to nonprofit organizations in the United States and Latin America. Previously, she served as Director of Government Relations in a New York NGO and as Policy Adviser for state legislators across the United States. Fabiola began her legal career as a law clerk for Judge Joseph Maltese in New York's Supreme Court. She is a graduate of the University of California, Berkeley, American University, Washington, D.C., and the *Universidad Alfonso X*, Madrid.

Juan Fernando Córdoba Marentes is an attorney from the *Universidad de La Sabana*, Colombia. He holds postgraduate studies in Copyright from the *Universidad de Buenos Aires*, Argentina, and a master's degree in Law (LL.M.) from the University of Queensland, Australia. He is pursuing a Doctorate in Law (with emphasis on Intellectual Property) at the *Universidad Austral de Argentina* with a thesis on exceptions and limitations to copyright and the three-steps test. Juan Fernando is referee, university professor and lecturer in various academic forums, as well as having served as legal consultant for several legal firms in Colombia and Australia. He is also a member of the International Literary and Artistic Association and the Colombian Copyright Center´s Director Board. He currently works as professor and researcher at the Universidad de La Sabana's Faculty of Law and Political Science, as well as the Director of the Law Program.

Carlos Andrés Corredor Blanco is an attorney from the *Universidad Industrial de Santander*. He holds postgraduate studies in Commercial Law from the *Universidad Autónoma de Bucaramanga* and a master's degree in Business Law from the *Pontificia Universidad Javeriana*. He has been a fellow on various specialized courses on Copyright, Enforcement and e-Government by the Organization of American States, the World Intellectual Property Organization, and the Department of Justice in the United States, Seoul, Panama and Washington, respectively. Currently, Carlos serves as Head of the Office of the Register Officer at the National Directorate of Copyright, Colombia.

Mike Godwin is Internews' Senior Policy Advisor on the Global Internet Policy Project. Mike is an American attorney and author, who has worked on a wide range of Internet law and policy issues for more than 20 years. He was hired directly out of law school in 1990 to become the first staff counsel of the Electronic Frontier Foundation, where he worked for nine years, culminating in his work leading to and following the Supreme Court case Reno v. ACLU, which established free-speech principles for internet expression under American law. Mike is also famous (or notorious) as the creator of the Internet adage Godwin's Law of Nazi Analogies. In the later 1990s and early 2000s, Mike worked on intellectual property and technology policy issues for the Center for Democracy and Technology and for Public Knowledge, two Washington, D.C.-based NGOs. From July 2007 to October 2010, he was general counsel for the Wikemedia Foundation, and has remained a consulting attorney to Wikimedia/Wikipedia since then, notably advising WMF in staging the SOPA-protest blackout in January 2012. Mike has served on the Open Source Initiative board and on the Student Press Law Center board. He also has served as a contributing editor of *Reason* magazine since 1994, not only writing on political and legal topics, but also contributing book reviews and interviews with science-fiction authors.

Peter Jaszi teaches domestic and international copyright law at American University Law School, supervises students in its Glushko-Samuelson Intellectual Property Law Clinic and writes about copyright history and theory. With Craig Joyce, Marshall Leaffer and Tyler Ochoa, he co-authors a standard copyright textbook, ***Copyright Law*** (Lexis, 8th ed., 2010). He and Martha Woodmansee edited ***The Construction of Authorship***, published by Duke University Press in 1994. Their new collection, ***Making and Unmaking Intellectual Property*** (edited with Mario Biagioli), was published by the University of Chicago Press in Spring 2011. In 1994, Peter was a member of the Librarian of Congress' Advisory Commission on Copyright Registration and Deposit, and in 1995 he was an organizer of the Digital Future Coalition. He is a Trustee of the Copyright Society of the USA, and a member of the editorial board of its journal. Since 2005, Peter has been working with Prof. Patricia Aufderheide of the American University's Center for Social Media on projects designed to promote the understanding of fair use by documentary filmmakers and other creators. Their book, ***Reclaiming Fair Use***, was published last year by Chicago. In 2006-2007, Peter led an interdisciplinary research team, funded by the Ford Foundation, to investigate the connections between intellectual law and the traditional arts in Indonesia. In 2007, Peter received the American Library Association's L. Ray Patterson Copyright Award, and in 2009 the Intellectual Property Section of the District of Columbia Bar honored him as the year's Champion of Intellectual Property, and in 2011 he was recognized with an IP3 award from *Public Knowledge*. Peter currently serves on the board of Independent Televisión Service, an important founder of documentary film projects.

Liliana Rocío Ariza Ariza is an attorney from the *Universidad Nacional de Colombia*, specialized in Industrial Property, Copyright and Information Technologies from the *Universidad Externado de Colombia*. She currently serves as Advisor at the Directorate of Foreign Investment and Service of the Ministry of Commerce, Industry and Tourism. Among her responsibilities, Liliana coordinate the Intellectual Property table in negotiating trade agreements.

Carlos Eduardo Cortés Castillo is an attorney from the *Universidad de Los Andes*, Colombia. He served as Director at the Foundation for Press Freedom (FLIP, in Spanish), Legal Advisor at the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights and professor of Media Law at the *Universidad del Rosario's* Journalism and Public Opinion Program. He has worked as a journalist for different Colombian media outlets such as *Semana* and *La Silla Vacía*. Carlos holds a master's degree in Media Governance from the London School of Economics, London, UK. He also works as researcher at the *Universidad de Palermo*'s Center for Studies on Freedom of Expression in Argentina, and as consultant for Open Society Foundations' Digital Media project. In 2013, Carlos has advised *Karisma* Foundation and the Colombian collective RedPaTodos on copyright and Internet regulation.

Francisco Vera is currently Senior Policy Analyst for Latin America at Access, an international human rights organization that defends and extends the rights of Internet users at risk worldwide. He is specialized in intellectual property, data protection, criminal law and freedom of expression from a regulatory perspective. He also works as Project Direct at the Chilean NGO *Derechos Digitales*, a human rights and technology organization. Francisco has also worked as attorney in civil and criminal law in several law firms in Chile.

Lorenzo Villegas Carrasquilla is an attorney and political scientist from the *Unviersidad de los Andes*, Colombia. He holds masters degrees in Constitutional and in Economics of Public Law from the University of Paris 2; additionally, he is pursuing a Doctorate from the University of Paris 2. He has undertaken studies in high government and telecommunications regulation. Lorenzo has served as Director and Commissioner at the Colombia's Communications Regulation Commission, Freshfields Bruckhaus Deringer partner and Law Clerk for Judge Vladimiro Naranjo in Colombia's Constitutional Court. He is an expert attorney in Information and Communication Technologies, Computer Law and Internet Law. He is a university professor in ICT Law, Regulation and Arbitration. Lorenzo also serves as referee at Bogotá Chamber of Commerce. Currently, he is Director at Lorenzo Villegas Consultants, an expert firm in ICT and Internet law.

CONFERENCIA INTERNACIONAL

DERECHOS HUMANOS EN LA ERA DIGITAL

Documents

From Eagerness Only Remains Uncostitutionality: The Fall of the Lleras Law 2.0

Juan Fernando Córdoba Marentes

Juan is referee, university professor and lecturer at various academic. He currently works as professor and researcher at the Universidad de La Sabana's Faculty of Law and Political Science, as well as the Director of the Law Program.

The unconstitutionality declaration of Bill No. 1520 of 2012 (known as Law Lleras 2.0 by Internet user), which developed some commitments on copyright set out in the Free Trade Agreement with the United States, has ratified the view of many persons who criticized its hasty adoption. Indeed, according to confusing news reports, the key argument that was overlooked by the Constitutional Court to determine the norm's unconstitutionality is that there has been a breach of essential procedural requirements during the legislative process in Congress.

This would give the reason to various plaintiffs who argued that the law should have been discussed in the committees designated to study intellectual property issues and not on those dedicated to the international policy matters, as eventually happened, presumably to ensure more expeditious processing of the government initiative. In any case, the eagerness of the Government to show President Obama that Colombia was meeting FTA commitments was reflected not only in the law's formal errors but in its very substance. For instance, one of the items that was declared unconstitutional, Article 13, basically replicates provision 16.7.9 of the FTA by stating that "notwithstanding the State's option of providing limitations and exceptions to exclusive rights under the national legislation on copyright and related rights, it is not permitted the retransmission of television signals, whether terrestrial, cable, or satellite, on the Internet without the authorization of the right holder or holders of the content of the signal and, if any, of the signal."

It is remarkable that with this law, the opportunity to establish limitations and exceptions in this area was not leveraged, despite the fact that the FTA recognizes the power of the Parties to do so. This gave arguments to law's critics to claim that rights to information, education and culture were infringed. Didn't we have six years, since it was initially approved the FTA, to prepare laws that fully and properly develop what was agreed in the treaty? Developing internally the FTA terms, it was not merely to transcribe a provision, as happened in this case, but to go further and tailor the commitment to the local context, for example, by defining the cases in which the transmission prohibited would not constitute an infringement.

The United States has the same commitment set out in Article 13. The difference is that they did make their task of establishing exceptions and limitations. Moreover, they will always have the fair use doctrine, which allows a person defending himself/herself for infringement when certain criteria of reasonableness are met.

In any case, it should be reminded to the industry that have displayed powerful lobby to promote and defend a lightly prepared norm, as well as to those that have attacked it for political reasons, that the Court's decision did not kill copyrights or disappeared exclusive privileges of the rights-holders to reproduce and publicly communicate works and other protected materials, as provided by the current legal system. Therefore, it would be wrong to say that the unconstitutionality declaration automatically allows the retransmission of television signals over the Internet without the permission of rights-holders.

Beyond this current situation, there is a perceived need for understanding that globalization and the establishment of free trade agreements involve greater flexibility in those paradigms that govern our intellectual property protection system. It would be advisable not stay only with the heinous and imposing part of the U.S. system, but also learn from the way they have developed to balance the various interests at stake, such as fair use. Sure, this requires deep thought, incompatible with the moment's eagerness.

This article has been first published in the website of the Universidad de La Sabana. Available in http://www.unisabana.edu.co/nc/la-sabana/campus-20/noticia/articulo/del-afan-no-queda-sino-la-inexequibilidad-la-caida-de-la-ley-lleras-20-columna-de-opinion/.

Beyond Tech and Tactics

In the new world of Internet policy, online freedom hangs in the balance

Mike Godwin

Mike *(mgodwin@internews.org)* is Senior Policy Advisor for the Global Internet Policy Project of Internews, an international non-profit media development organization whose mission is to empower local media worldwide to give people the news and information they need, the ability to connect and the means to make their voices heard. Formed in 1982, Internews has worked in more than 90 countries, and currently has offices in Africa, Asia, Europe, the Middle East, Latin America and North America. Visit *http://www.internews.org*.

Leave it to the National Security Agency and the Foreign Surveillance Intelligence Court to put the "spook" back in "spooky." In recent weeks, the general public has learned what many of us specialists have long known, which is that vast swaths of the communications of ordinary citizens have been swept into intrusive dragnets, and, the legal framework for all this snooping is itself the product of a secret body of law generated by a secret special court. Yet these revelations of how much the US government has been spying on its population shouldn't be so shocking given that the underlying law – the Foreign Intelligence Surveillance Act – has been in place since 1978.

If the digital era has empowered ordinary citizens to do and say more online, it's also made us more vulnerable to privacy intrusions of all kinds – and digital technologies empower governments at least as much as they empower the rest of us. But that is precisely the silver lining to the NSA story. It has alerted the public that the law and policy shaping the Internet have significance for all of us, not just for lawmakers.

It wasn't always clear that cyberpolicy would loom quite so large in our daily lives. When I started practicing "Internet law" in 1990, traditional legal scholars doubted there was enough legal matter in cyberspace to even cause concern. At the same time, technologists often talked glibly about how tools like ubiquitous personal computers would make the need for resolving legal and policy issues a thing of the past; everybody would be empowered to participate in public dialogue, a kind of direct democracy leaving lawmakers and bureaucrats in the dust of irrelevance.

Both assumptions were wrong. Cyberpolicy is more relevant than ever, because cyberspace has rapidly become a central staging area for political participation in the modern era. For proof look no further than to Italy and the United States. In both countries in 2012, repressive legislation led Wikimedian activists to protest by temporarily shutting down access to Wikipedia. It also led to new dialogues between governments, Internet companies and civil society organizations. In both instances, legislators withdrew the proposed laws.

The NSA brouhaha and the Wikipedia blackouts have underlined the ongoing tensions modern governments face: how can governments safeguard security, intellectual property, and other rights of citizens while fully protecting online privacy and freedom of expression? To one degree or another, this is a drama that is now playing out in countries around the world.

In fact, we are at a pivotal moment in which many developing countries are hashing out their Internet and communications policies. While many nations are committed to online freedom – or at least say they are – quite a few are working to rein in free expression or to impose ubiquitous surveillance that exceeds even the NSA's ambitions. Both new nations and old ones are rushing to update their laws for the digital era; there is a narrow window of opportunity to shape the digital future before these Internet policy regimes are set into law. So this is precisely the time for policy activists in emerging and transitional nations to focus on building the legal

framework under which freedom of expression – both traditional and online – can play its proper role in a democratic society.

In developing and transitional democracies, it has become apparent that if you don't have a strong consensus about what it means to have free media, it doesn't matter how slick your digital tools are. Notwithstanding the so-called "Twitter revolutions," this is a hard fact that activists in the Middle East, Africa, Latin America, and East Asia are learning the hard way these days. We know social media and encryption are **not** the answer to every free speech and privacy problem. While governments often give lip service to a free press, freedom of speech, and political engagement, they may also simultaneously pass laws and enact policies that undermine those very values.

These policy threats can take many forms. Two critical examples: (1) sometimes a new government, feeling its own fragility, wants to build a widespread surveillance infrastructure into the country's internet services; and (2) sometimes politicians and wealthy citizens realize that newly empowered Internet users can use digital platforms and tools to criticize the powers-that-be, so they deploy defamation laws and court cases to chilling effect.

For better or worse, the hard work of policy development doesn't lend itself to street protests or tweets alone – and most policy problems can't be solved by staging a Wikipedia blackout in the absence of deep engagement in a sustained multi-stakeholder approach. It turns out that cyberpolicy advocacy is less like programming a computer or stringing a wire than building a marriage: it hinges on creating and maintaining trusted relationships and transparent dialogue. What it really takes is face-to-face meetings between citizen advocates and policymakers, reasoning together, and creating a shared understanding of what freedom and privacy should mean on the Internet, regardless of the tools we happen to be using.

In my work with Internews' Global Internet Policy Project, I help strengthen the ability of civil society organizations to work towards humane, progressive Internet policy in their countries. In policy discussions, these ordinary citizens and brave activists and lawyers are learning how to make their voices heard by their governments as well as by the institutional stakeholders who have traditionally had a monopoly on government's ears. I have seen firsthand that what emerges from a mature process of policy advocacy is dialogue and colloquy in which all stakeholders — including government ministries, Internet activists, journalists, bloggers, civil society groups, telcom and internet service providers — recognize the value of other points of view and find solutions.

A.J. Liebling famously said, "Freedom of the press is guaranteed only to those who own one." The key fact of the modern digital era is that, increasingly, everyone owns one. The citizens who capture violence in the street with a camera-enabled phone are practicing journalism. So are the bloggers who publish with only a laptop and a Tumblr account. And when I lived in downtown Oakland during the 2011 Occupy Oakland protests, I knew that people who were live-tweeting police movements and crowd actions were honoring the noblest tradition of journalism: to bear witness.

The rising tide of citizen journalism and a plethora of citizen voices makes many governments uncomfortable, especially those with a tradition of muzzling the press. Controlling your critics is easier with censorship, with the introduction of online media restrictions, and limited broadcast licenses. So when everyone is, effectively, a newspaper or radio station or reporter, a newer, more fragile, or simply nervous government may find reason to panic.

Here civil society plays an essential role in media policy: it's to stop governments from panicking and adopting repressive policies that undermine privacy and that squelch a free media of all kinds, (including any built by a blogger with a Facebook or Wordpress account). To nurture good

Internet policy, public protests or legal actions may be the start of the dialog, but they can't be the end of it. Instead, advocates of an open and free Internet need to learn how to keep governments calm in the face of rapid digital democratization. In effect, they must become their own kind of institutional resource for ensuring free expression and privacy online. In the process, civil society groups can legitimize the whole process of engagement, so that their governments see them as resources and partners, not just adversaries.

Success will mean that Internet governance is not just for the governors anymore, and that Internet policy is not just for policymakers. And it will underscore the plain reality that journalism is not just for journalists any more. In today's digital democracies, where each of us could play any of these roles, the most valuable help we can offer those who are advocating for good policy on our behalf is the recognition that we each have a direct personal stake in freedom of the press, which nowadays is as universal and individual as freedom of speech.

This means activists have to look beyond digital technologies and protest tactics to secure long-term policy frameworks that protect online expression and privacy. The sooner we achieve international social consensus about this, the sooner we will understand how to manage the complex blend of individual privileges and responsibilities that come with life in the digital age.

International Principles on the Application of Human Rights to Communications Surveillance
Final version 10 July 2013

As technologies that facilitate State surveillance of communications advance, States are failing to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. This document attempts to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. These principles can provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

Preamble

Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognized under international human rights law.1 Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.2

Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to State communications surveillance. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. The explosion of digital communications content and information about communications, or "communications metadata" – information about an individual's communications or use of electronic devices – the falling cost of storing and mining large sets of data, and the provision of personal content

through third party service providers make State surveillance possible at an unprecedented scale.3 Meanwhile, conceptualizations of existing human rights law have not kept up with the modern and changing communications surveillance capabilities of the State, the ability of the State to combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.

The frequency with which States are seeking access to both communications content and communications metadata is rising dramatically, without adequate scrutiny.4 When accessed and analyzed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications.5 Despite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, legislative and policy instruments often afford communications metadata a lower level of protection and do not place sufficient restrictions on how they can be subsequently used by agencies, including how they are data-mined, shared, and retained.

In order for States to actually meet their international human rights obligations in relation to communications surveillance, they must comply with the principles set out below. These principles apply to surveillance of a State's own citizens and conducted in its own territory as well as of its surveillance of others extraterritorially. The principles also apply regardless of the purpose for the surveillance – law enforcement, national security or any other regulatory purpose. They also apply both to the State's obligation to respect and fulfill individuals' rights, and also to the obligation to protect individuals' rights from abuse by non-State actors, including corporate entities.6 The private sector bears equal responsibility for respecting human rights, particularly given the key role it plays in designing, developing and disseminating technologies; enabling and providing communications; and – where required – cooperating with State surveillance activities. Nevertheless, the scope of the present Principles is limited to the obligations of the State.

Changing technology and definitions

"Communications surveillance" in the modern environment encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future. "Communications" include activities, interactions and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

Traditionally, the invasiveness of communications surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content," "subscriber information" or "metadata," stored data or in transit data, data held in the home or in the possession of a third party service provider.[7] However, these distinctions are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analyzed collectively, reveal a person's identity, behavior, associations, physical or medical conditions**,** race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location,

movements or interactions over time,[8] or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law.

In evaluating the invasiveness of State communications surveillance, it is necessary to consider both the potential of the surveillance to reveal protected information, as well as the purpose for which the information is sought by the State. Communications surveillance that will likely lead to the revelation of protected information that may place a person at risk of investigation, discrimination or violation of human rights will constitute a serious infringement on an individual's right to privacy, and will also undermine the enjoyment of other fundamental rights, including the right to free expression, association, and political participation. This is because these rights require people to be able to communicate free from the chilling effect of government surveillance. A determination of both the character and potential uses of the information sought will thus be necessary in each specific case.

When adopting a new communications surveillance technique or expanding the scope of an existing technique, the State should ascertain whether the information likely to be procured falls within the ambit of "protected information" before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism. In considering whether information obtained through communications surveillance rises to the level of "protected information", the form as well as the scope and duration of the surveillance are relevant factors. Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection.9

The determination of whether the State may conduct communications surveillance that interferes with protected information must be consistent with the following principles.

The Principles

Legality: Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

Legitimate Aim: Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Necessity: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

Adequacy: Any instance of communications surveillance authorized by law must be appropriate to fulfill the specific legitimate aim identified.

Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.

Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

a) There is a high degree of probability that a serious crime has been or will be committed;

b) Evidence of such a crime would be obtained by accessing the protected information sought;

c) Other available less invasive investigative techniques have been exhausted;

d) Information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and

e) Information is accessed only by the specified authority and used for the purpose for which authorization was given.

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

a) Other available less invasive investigative techniques have been considered;
b) Information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
c) Information is accessed only by the specified authority and used for the purpose for which was authorization was given.

Competent Judicial Authority: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be (1) separate from the authorities conducting communications surveillance, (2) conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights, and (3) have adequate resources in exercising the functions assigned to them.

Due process: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,10 except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to

justify retroactive authorization.

User notification: Individuals should be notified of a decision authorizing communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstances:

a) Notification would seriously jeopardize the purpose for which the surveillance is authorized, or there is an imminent risk of danger to human life; or

b) Authorization to delay notification is granted by the competent judicial authority at the time that authorization for surveillance is granted; and

c) The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

Transparency: States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

Public oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.11 Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

Integrity of communications and systems: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.12

Safeguards for international cooperation: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement

purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

Safeguards against illegitimate access: States should enact legislation criminalizing illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

(Endnotes)

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

3 Communications metadata may include information about our identities (subscriber information, device information), interactions (origins and destinations of communications, especially those showing websites visited, books and other materials read, people interacted with, friends, family, acquaintances, searches conducted, resources used), and location (places and times, proximities to others); in sum, metadata provides a window into nearly every action in modern life, our mental states, interests, intentions, and our innermost thoughts.

4 For example, in the United Kingdom alone, there are now approximately 500,000 requests for communications metadata every year, currently under a self-authorising regime for law enforcement agencies that are able to authorise their own requests for access to information held by service providers. Meanwhile, data provided by Google's Transparency reports shows that requests for user data from the U.S. alone rose from 8888 in 2010 to 12,271 in 2011. In Korea, there were about 6 million subscriber/poster information requests every year and about 30 million requests for other forms of communications metadata every year in 2011-2012, almost of all of which were granted and executed. 2012 data available at http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586.

5 See as examples, a review of Sandy Petland's work, 'Reality Mining', in MIT's Technology Review, 2008, available at http://www2.technologyreview.com/article/409598/tr10-reality-mining/ and also see Alberto Escudero-Pascual and Gus Hosein, 'Questioning lawful access to traffic data', Communications of the ACM, Volume 47 Issue 3, March 2004, pages 77 - 82.

6 Report of the UN Special Rapporteur on the promotion and protection of the right

to freedom of opinion and expression, Frank La Rue, May 16 2011, available athttp://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

7 "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers… I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

8 "Short-term monitoring of a person's movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *United States v. Jones*, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

9 "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." *U.S. v. Maynard*, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562; *U.S. v. Jones*, 565 U.S. __, (2012), Alito, J., concurring."Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8(1) of the Convention." (*Rotaru v. Romania*, [2000] ECHR 28341/95, paras. 43-44.

10 The term "due process" can be used interchangeably with "procedural fairness" and "natural justice", and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

11 The UK Interception of Communications Commissioner is an example of such an independent oversight mechanism. The ICO publishes a report that includes some aggregate data but it does not provide sufficient data to scrutinize the types of requests, the extent of each access request, the purpose of the requests, and the scrutiny applied to them. See http://www.intelligencecommissioners.com/sections.asp?sectionID=2&type=top.

12 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para 84.