

IGF 2016 Workshop Report Template

Session Title	No. 267 Surveillance and International Human Rights Law
Date	December 8, 2016
Time	60 minutes
Session Organizer	Luis Fernando García, Executive Director at Red en Defensa de los Derechos Digitales (R3D) Katitza Rodriguez, Electronic Frontier Foundation
Chair/Moderator	María Cristina Capelo, Public Policy at Google
Rapporteur/Notetaker	Luis Fernando García (R3D)
List of Speakers and their institutional affiliations	Amos Toh - Legal Advisor to the UN Special Rapporteur on Freedom of Expression Peter Kimpian - Data Protection Unit - Council of Europe Katitza Rodriguez - Electronic Frontier Foundation Arjun Jayakumar - Policy Director at SFLC Luis Fernando García - Executive Director at Red en defensa de los derechos digitales
Key Issues raised (1 sentence per issue):	<ul style="list-style-type: none"> - Legitimacy of surveillance in the context of universal and regional human rights systems - Principles of legality, legitimate aim, necessity, adequacy and proportionality in the surveillance practices of governments around the world - Authorities in some countries are developing activities of massive surveillance as requests of information to telcos,

	<p>metadata retention without any adequate legislation to be more accountable and with a clear framework of control.</p>
<p>If there were presentations during the session, please provide a 1-paragraph summary for each Presentation</p>	<ul style="list-style-type: none"> - Right to the freedom of opinion is an absolutely right and need to be protected. Objectives of surveillance need to be very clear, proportional, desirable, necessary to the objectives that are pursuing - Surveillance operations are extended to other targets as activist and organizations. How we can extend more protective measures to protect citizens and have more accountability the surveillance at an international level?. Laws of regulation in some countries are borrow and opaque and have very broad limitations, especially national security related reasons to allow surveillance - In some countries telecom companies are compliant with surveillance measures with no legitimate, clear and proportionate objectives. It's useless to have very clear laws if there's no one to check whether those laws are being complied with - When a vague new telecom law entered into effect in countries as Mexico, the number of authorities that asked for user data spiked. Latin American countries do not have precise laws regarding new forms of surveillance. Surveillance has to pursue legitimate interest and has to be necessary and proportionate.
<p>Please describe the Discussions that took place during the workshop session: (3 paragraphs)</p>	<p>Massive surveillance is frequently associated to National Security reasons to be done.</p> <p>Privacy are a process in that are involved big telecommunication companies and governments asking to them information requests.</p> <p>Data protection agencies are not scrutinizing requests of government information requests involved in digital environments and have issues to resolve as metadata collection and analysis, geolocalization capabilities of devices and services and their use in any kind of investigations.</p>
<p>Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3</p>	<p>Civil organizations around the world need to encourage to telecom companies to challenge orders of surveillance requested by governments and be more accountable in order to make the protection of people's privacy more effective</p> <p>It should be emphasized that the processes of internet governance consider the necessity and proportionality principles in the regulation of the operation of new technologies to be</p>

paragraphs)	<p data-bbox="496 188 1386 246">potential violators of the privacy of people</p> <p data-bbox="496 246 1386 492">Civil society organizations must be very attentive to emerging internet governance regulations relating to surveillance, the accumulation of personal data and all those processes that compromise privacy, as there are substantial differences between local laws and international reality, especially in data exchange.</p>
-------------	--