

## IGF 2016 Workshop Report Template

Session Title	<b>Direct Access and the Next Billion: Policy, Problems and Proposals</b>
Date	Thursday December 8
Time	16.30-18.00
Session Organizer	Privacy International
Chair/Moderator	Lucy Purdon
Rapporteur/Notetaker	Alexandrine Pirlot de Corbion
List of Speakers and their institutional affiliations	Edin Omanovic, Privacy International Collin Anderson, Independent researcher Adnan Chaudhri, Digital Rights Foundation, Pakistan Patrik Hiselius, from the Swedish telecommunications operator Telia Company, formerly TeliaSonera Luis Fernando Garcia, R3D, Mexico Carolina Botero, Fundación Karisma, Colombia Judith Lichtenburg, Global Network Initiative (GNI)
Key Issues raised (1 sentence per issue):	<ol style="list-style-type: none"> <li>1. Direct access is not a new issue, but it's not going away, and it's getting worse.</li> <li>2. There is limited or no transparency in terms of the policies and practices, and it's very difficult to get information. This is a challenge especially for NGOs who are trying to work on this topic to advocate for better privacy and human rights protects. They rely on rumours, transparency reports, leaked documents, technical research.</li> <li>3. Telecommunication companies are often prevented by law from disclosing when states practice direct access, but some try to put as much info as possible in transparency reports.</li> </ol>
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	<p><b>Edin Omanovic:</b> Edin explained that direct access is a that heart of state surveillance today. He described PI's previous work on direct access- Swift scandal of the 1990s, PNR records, and the Macedonia report that uncovered direct access interception by the security services, which included intercepting 20,000 politicians, opposition, activists etc. including during a general election.</p> <p><b>Patrik Hiselius:</b> Providing the perspective of telecommunication operators, Patrik described the challenges an operator faces- try to be as transparent as possible in transparency reports, but legal framework often prevents it. He said operators were against direct access as they wanted to retain control.</p>

**Judith Lichtenburg:** Supporting the private sector perspective, Judith noted that it's not just operators that are concerned about it, also internet companies. Snowden documents demonstrated direct access into companies' servers. She explained that practices such as direct access mean that telecommunications operators lose controls and are thus unable to be accountable to their users.

**Collin Anderson:** Collin explained that unlike some other surveillance technologies, technically, it's very difficult to uncover when direct access is happening. Even identifying the technical standards states use (such as ETSI or SORM) will not help uncover whether a state is practicing direct access. He explained that the nature of this practice prevented a democratic debate on surveillance. This emphasises the need for further transparency in terms of policies and practices from both governments and companies.

**Adnan Chaudhri:** Adnan described the difficulty of challenging the government on issues of surveillance in Pakistan. People take for granted it is happening, and civil society are called trouble makers. But now that other actors have stepped in, such as the Human Rights Committee, and are asking Pakistan questions on their surveillance regime, it is not just civil society. The international community are also putting pressure on the government. Adnan provided the example of Blackberry in Pakistan, where the company refused to give direct access to their encrypted messaging service, which resulted in Pakistan threatening to throw the company out of the country. The decision was reversed but nobody knows why.

**Luis Fernando Garcia:** Luis described the surveillance legal framework in Mexico and some of their findings in relations to direct access that have emerged from their research. He provided details that the Mexican government were the biggest purchaser of Hacking Team Malware, elements of which would require the telecommunications operators to provide direct access to enable the use of that software.

**Carolina Botero:** Carolina explained that government agencies are allowed by law a "backdoor" into telecommunication services, thus raising the suspicion there is direct access in the country. However, Carolina explained that the practice is unknown because of the lack of transparency. She mentioned that developing an evidence-base is crucial when conducting their

	<p>work advocating for privacy but raised the challenging for CSOs to document harm of surveillance when it is increasingly more covert. This is a real obstacle they face in conducting their work.</p>
<p>Please describe the Discussions that took place during the workshop session: (3 paragraphs)</p>	<p><b>Defining direct access:</b> There's no official definition, but It broadly describes situations where law enforcement, intelligence agencies and possibly others have a direct connection to telecommunications networks and obtain communications content and data, often without prior authorisation, a warrant, or the knowledge of the operator that runs the network.</p> <p><b>Direct access threatens human rights and prevent democratic debates on state surveillance:</b> In States that practice direct access, nobody knows that surveillance is happening, there is no opportunity for oversight, therefore it is very open to abuse. The UN and the European Court of Human Rights have recognised that this practice violates privacy, freedom of expression, and freedom of association.</p> <p><b>The difficulty for civil society</b> in identifying states that practice direct access, due to technical confidentiality, legal constraints, and a lack of forums for civil society to challenge, scrutinize or bring transparency to the practice hence challenging their ability to advocate for better protections for individuals.</p>
<p>Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)</p>	<p>Governments should be transparent as to whether they have direct access, in which countries, under what legal framework, and using what kind of technology. Civil society could explore further use of Freedom of information laws to gather information.</p> <p>Other companies that are involved in the network, such as IEPs and submarine cable providers, should be part of the research, analysis and targeted advocacy strategies. Investors are an important stakeholder and should be included in civil society advocacy.</p> <p>Transparency report could provide useful information and so further meticulous analysis of them could enable the identification of which states practice direct access. Also, Telecommunications License requirements should be transparent.</p>