

PRESS RELEASE

SURVEILLANCE ISSUES OVERSHADOW TALKS AT END OF INTERNET GOVERNANCE FORUM (IGF) 2013

Future of Internet could be shaped by global reaction to surveillance, participants say

Bali, Indonesia, 25 October 2013 - As a stream of surveillance revelations continues to seize the attention of governments and public opinion alike, the largest global multistakeholder meeting on Internet governance, known as the IGF, concluded today in Bali, Indonesia, by confronting surveillance as the major “emerging issue” of the year.

Referred to as “the elephant in the room” in the opening session, the issue of surveillance cast a long shadow over the discussions at the four-day forum – a UN-convened annual meeting that drew more than 1,500 representatives of governments, civil society, technical community and private sector from 111 countries, with hundreds more participating remotely.

A number of the IGF’s 135 workshops and focus discussions made reference to “restoring trust” in the Internet and the potential dangers of retrenchment from an open Internet by nations concerned about the security and privacy of their digital communications. During the final focus session, in response to a comment coming in on twitter, moderator Jovan Kurbalija, referred to the forum’s “serious determination and responsibility to do something useful for Internet as a whole, and for humanity, first of all to avoid the situation like this one with the NSA case, but also to prevent similar situations happening worldwide.”

U.S. State Department Representative Scott Busby said that the United States recognizes the many concerns on the issue of surveillance and “welcomes a discussion about privacy and security, and we are right now intensively having that discussion,” adding that the issue of surveillance global should “take into account the views and practices of everyone around the world.” Addressing the nexus between the surveillance and violations of human rights, Mr. Busby said that the U.S. “does not use intelligence collection for the purpose of repressing the citizens of any country for any reason, including their political, religious, or other beliefs,” adding that “individuals should be protected from arbitrary or unlawful State interference.”

The issue of trust was picked up by Ross LaJeunesse of Google, who said “if our users don’t trust us, they won’t use our products, and they’ll go somewhere else.” Part of maintaining that trust, Mr. Lajeunesse maintained, is “not provide direct access for any Government to our data, our servers, our infrastructure”, and not to accept “large, blanket-like Government requests for user data.” He urged participants to hold all governments accountable to the highest standards, including those “where journalists are beaten, bloggers are imprisoned and activists are killed.”

Speaking from a technical perspective, Jari Arkoo of the Internet Engineering Task Force (IETF), offered what he called a “do not panic” message, which included the view that surveillance is a widespread problem that has been around for a long time, but that given today’s challenges “once again Internet technology needs to evolve” to ensure an Internet that protects privacy concerns while remaining open and global.

To strengthen trust “the principles of rule of law, transparency, and also respect for Human Rights” must be reinforced according to Johan Hallenberg of the Foreign Ministry of Sweden, a country that has introduced constitutional framework protections in the digital privacy area. An equally important aspect to protecting rights and freedoms of individuals from abuse of others, is the ensuring that “the State itself does not violate rights and freedoms -- in other words, setting the limits for state power,” he said. Fundamental to this exercise, Mr. Hallenberg added, is to ensure the separation between “surveillance of electronic communication by law enforcement agencies” and “intelligence collection by security agencies.” At the recent Seoul Conference on Cyberspace Sweden’s Prime Minister Carl Bildt presented several fundamental principles to maintain respect for Human Rights when carrying out surveillance of electronic communications, Mr. Hallenberg said, stating that these include: “legality, legitimate aim, necessity and adequacy, proportionality, judicial authority, transparency, and public oversight.”

“Trust among Governments and in the major ICT and Telecom companies is completely broken” as a result of unauthorized data and metadata collection, said Joana Varon of the Centre for Technology and Society in Rio de Janeiro, representing civil society organizations, adding that was time to move forward with solutions. In this regard, Ms. Varon mentioned that the Civil Rights Framework for the Internet in Brazil ('Marco Civil') as “a model in terms of both content and process” that could provide a useful guide in an international scenario. Ms. Varon invited representatives of other countries to consider the “International Principles on the application of Human Rights to Communication Surveillance”, which in addition to some of the principles in Sweden’s seven-point list also include “user notification, transparency, and public oversight.”

Kicking off the comments from the floor, Amb. Benedicto Fonseca Filho of Brazil said he would “align” his statement with the one delivered by Joana Varon, reiterating Brazilian President Dilma Rousseff’s call to the international community to launch a process that would achieve principles and norms to guide use and operation of the Internet. The proposed Summit meeting in Brazil next year aims to accelerate this process while maintaining a multistakeholder approach, he said.

Additional comments included the notion that developing principles to deal with surveillance is “necessary but not sufficient,” and that what is needed is “due process and oversight.” Commenting that the damage done by unauthorized surveillance was much larger than was being acknowledged, one speaker said that “a cancer scare does not get treated with an aspirin.”

“Some individuals countries are carrying out large-scale surveillance over other countries,” said Mr. Ren Yishen of the Foreign Ministry of the People’s Republic of China, calling this “an infringement of sovereignty and privacy that also poses a threat to the safe operation of the Internet.”

While surveillance is troubling for governments and the public alike, some speakers emphasized that the reaction may also be “very troublesome,” as calls for “data sovereignty” could present extreme technical challenges and could stifle local industries. Demand for “keeping data local” would likely lead to blanket requirements that would harm innovation in the Internet, another speaker said.

A former member of Parliament from Germany questioned the treatment of people who encrypt their data as “potential terrorists.” He went on to describe the need, among other things, for international contracts to ensure that “friends don’t spy on friends,” and received applause when calling for encrypting all communication so that surveillance will not work. The session’s loudest applause was heard for a comment from a representative of the Center for Technology and Democracy: “I’ve not lost my trust in the Internet,” Matthew Shears said, “I’ve lost my trust in the institutions that use the Internet for the purposes of undermining my fundamental rights.”

Session Chairman Dr. Setyanto P. Santosa, Chief of the Indonesian Information and Communication Technology Association, called it “the top of the top sessions” at the IGF, and Mr. Markus Kummer of the Internet Society, who had chaired the IGF preparatory process, commented that by addressing such a sensitive issue the multistakeholder Forum had “proved its value and its worth.”

The four-day IGF 2013 meeting was capped by a closing ceremony that reaffirmed the participants' belief in maintaining and strengthening the multistakeholder approach to discussing governance on the Internet, as opposed to a government-led multilateral approach. It also focused with a wider lens on emerging issues in Internet governance, beyond the surveillance issue.

"New cybersecurity threats and revelations of widespread Internet surveillance are only two of emerging issues that the multistakeholder community must address," said Elia Armstrong of the United Nations Department of Economic and Social Affairs (UNDESA), underlining the need for these multistakeholder deliberations to also feed into the broader processes for global agenda for sustainable development post-2015 and the "WSIS +10" review.

Anne-Rachel Inné, Chief Operating Officer of AfriNIC, expressed the hope that the "open and collaborative spirit of Internet cooperation" of IGF 2013 in Bali would be maintained in future meetings and negotiations, noting that "it is needed for the further evolution of Internet governance in all discussions going forward."

"Now, more than ever, it is time to reenergize the concept and practice of consultative multistakeholder governance," said Mr. Virat Bhatia, Chairman, Communications and Digital Economy Committee, of the Federation of Indian Chambers of Commerce and Industry (FICCI) on behalf of the business community. "Business opposes a multilateral or intergovernmental approach to Internet Governance," he said.

Shita Laksmi, of HIVOS-Indonesia and part of the IGF 2013 Indonesian Organizing Committee, said it was important to recognize that "management of the Internet is not just a technical matter", and that "multistakeholder principles should be reflected in our work from the beginning to the end," including the Forum's organizational aspects. Acknowledging that 2013 IGF preparations had not been easy, Semmy Pangerapan of APJII and the IGF 2013 Indonesian Organising Committee said that the process demonstrated how "open dialogue and an open mind can serve a solid ground for multistakeholder Internet Governance practices, which we believe is a triumph for a future generation of Internet users."

On behalf of civil society, Keisha Taylor from Trinidad and Tobago said that "lesser developed economies and rural areas must continue to be discussed so that progress can indeed be made, and the next billion users from across the globe can also connect and not be left behind."

Dr. Ashwin Sasongko, Director General of the Ministry of Communication and Information Technology of Indonesia, closed the session with a reminder that Internet governance is a multistakeholder responsibility that in Indonesia's view "should be able to maximize the positive activities and minimize the negative activities in the Internet," to create a safe, secure and tolerant cyberspace.

For more information visit: www.intgovforum.org/cms/ follow @intgovforum #IGF2013

Issued by the United Nations Department of Public Information

