Internet Governance Forum
Baku – 2012

Workshop
Cloudy Jurisdiction: Addressing the Thirst for Cloud Data in Domestic Legal Processes

Workshop organized by Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), University of Ottawa (Canada) and Katitza Rodriguez, International Rights Director, Electronic Frontier Foundation (Peru)

Introduction
The objective of this workshop was to discuss the means by which privacy protection can be assured in an environment that exists in many jurisdictions at once and, hence, is subject to legal access by a wide variety of state entities. The panel was divided into two parts, the first focused on highlighting challenges to surveillance problems posed by the cloud, while the second focused on solutions. The hope was to adopt a practical, problem-solving attitude to these issues.

The Workshop
Chair: Katitza Rodriguez, International Rights Director, Electronic Frontier Foundation; (Peru) (Civil Society)

- Ian Brown, Senior Research Fellow, Oxford Internet Institute (EU) (Academic)
- Bertrand de la Chapelle, Program Director at International Diplomatic Academy (EU)
- Marc Crandall, Global Compliance, Google (US)
- Elonnai Hickok, Policy Associate, Centre for Internet & Society (India) (Civil Society)
- Sophie Kwasny, Head of Data Protection Unit, Data Protection & Cybercrime Division, Council of Europe (IGO)
- Bruce Schneier, Chief Security Technology Officer of BT (US) (Private Sector)
- Wendy Seltzer, Policy Counsel, W3C (US) (Technical Community)

Rapporteur:

- Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), University of Ottawa (Canada)

Remote Moderator:

- Paul Muchene, iHub Nairobi (Kenya) (Private Sector)

Workshop Report
Part I: Privacy Challenges in the Cloud

Many lines are blurring in a manner that confounds traditional privacy protections while exposing increasing amounts of data.

- **The Jurisdictional Challenge.** While the Internet is *technically* borderless, in reality, state actors impose their sovereignty onto online environments with increasing frequency. The operating of sovereignty over shared spaces can subject individuals to the laws of another country without any realization of having done so. This in effect transforms the surveillance efforts of one country into privacy risks for all the world's citizens, as an interconnected network places their personal data at the whims of many states. The cloud, which by its nature exists in multiple jurisdictions at once, exacerbates these jurisdictional problems, which are generally inherent in online interactions.

- **Lawful Intercept.** Governments appear to be in a race to outdo each other in terms of increasing surveillance capacity. Legislative efforts focus on Internet intermediaries and aim to maximize intercept capability and mandate retention of transactional data. The latter, in particular, is problematic as 'transactional' data is presumed to be less private. In reality, however, online transactional data can provide a very rich and broad picture individuals lives, activities and preferences. Yet on the basis of a false 'content/metadata' dichotomy, states do not offer this type of transactional data the same level of protection as is offered to 'real' content. As activities move to the cloud this becomes increasingly problematic, as each cloud interaction generates its additional metadata.

- **Voluntary Lawful Assistance.** The move to the cloud places a significant amount of personal data in the hands of third party entities – data that historically resided on the home computer now sits on a company's servers. At the same time, companies are increasingly facing political and legal pressures to assist governments in their surveillance efforts. Internet intermediaries can be pressured to domestically locate servers in order to bypass in-transit encryption or to hand over personal information of their customers upon request. There is minimal oversight over such voluntary cooperation, and, hence, its scope is not well-documented. The problem is worse in some developing countries, where there are minimal incentives for online intermediaries to fight government pressures and potentially rigorous penalties for not doing so.

- **Updated Surveillance Powers Meet Antiquated Privacy Protections.** Absent a few exceptions (such as encryption of communications), governments are in a rush to update surveillance laws. At the same time, they do not seem to approach the need to update privacy protections with equal determination and zeal. Many legal regimes intended to safeguard privacy against the states' overriding interest in surveilling its citizens are premised on space-based distinctions that simply do not apply in an online/cloud environment. Government surveillance regimes treat the same data that was once stored at home with far less respect simply because it is in the 'cloud'. Nor have privacy laws evolved to account for the increasing comprehensiveness with which it is now possible to monitor information such as real-time location, contact networks and other types of information. This lack of interest in updating privacy and due process protections occurs in *spite* of the fact that there are many benefits to ensuring such protections are in place. Some service providers may, for example, wish to avoid jurisdictions which impose heavy-handed and costly surveillance obligations altogether.

- **Lost Individual Control.** Another feature of evolving data ecosystem is that individuals have increasingly lower levels of control over their data. This has legal and technical implications. Legally, it challenges privacy norms that closely link protection with ongoing control over access to data. Technically, individuals are prevented from safeguarding their data with encryption and other techniques, or even from understanding how or to what extent the third parties who

control it are securing their data. These two sets of implications combine to pose a serious threat to privacy, as individual data is increasingly vulnerable on both a technical and legal basis. Worse – lawmakers seek to obligate technology to develop in a manner that facilitates greater surveillance, often minimal understanding of the broader technical and social implications.

- **Intelligence vs. Law Enforcement.** It is becoming increasingly difficult to separate intelligence efforts from law enforcement. Most of our privacy protections are most effective in a law enforcement context, but the line between the two is blurring. The increasing availability of 'public' data is a further challenge. It permits law enforcement to sweep up immense amounts of data and undertake forward-looking analysis, whereas our legal system seeks to check law enforcement powers primarily by preventing access to data expected to be private. No reasonable expectations apply to public data.

- **Difficulty Establishing User Trust.** Cloud-based companies attempt to take steps to safeguard customer data. These range from adopting security standards, to challenging legal data requests. However, while some mechanisms have developed to certify some of these safeguards in the enterprise context, it remains a challenge to convey these efforts to individual users. While there are legal limits to what providers can do in terms of protecting against state access, many cloud providers recognize the need to take these steps to secure customer trust. This is particularly important when asking people to invest their data in a new ecosystem such as that represented by cloud computing.

- **Data Minimization is Strained.** In this context, data minimization is strained in its attempt to limit state surveillance. The nature and utility of the online tools in question envisions users storing their data in the hands of another. Indeed, they should be able to do so – they should be able to trust online services – without needing to worry about exposing themselves to state surveillance.

- **Need Security and Privacy.** The real challenge is to facilitate legitimate and necessary security investigations while ensuring privacy protections. Security faces challenges as well in technological ecosystems, where encryption and anonymity are sometimes easier to achieve. It would be helpful to better integrate security and privacy policy-making. The challenge is that the balance we have established over centuries in the brick and mortar context is not easily grafted onto cyberspace.

Part II: How do we Secure Privacy in a Transborder Cloud?

- **New Governance Norms.** New legal and extra-legal paradigms that are tailored to the rapidly evolving online environment must be developed. Outdated laws must be updated so Courts can play their role in securing civil liberties, but more flexible approaches should be explored. Cooperative mechanisms that bring together representatives of responsible governments from over the world, platform operators and civil society and give them the capacity to monitor what surveillance is happening on an ongoing basis. However, it is not clear whether this type of multi-stakeholder auditing is enough on its own. While policymakers are often disproportionately susceptible to intelligence/law enforcement voices, and courts and legislatures struggle with the technical impacts of their policies and typically show up retroactively to clean up the mess, these institutions still have an important role to play in ensuring surveillance remains proportional and legitimate.

- **Multi-Lateral Treaties & Governance Instruments.** The use of regional or multi-lateral agreements might form a preferable basis for instilling some control over transborder access to cloud data. Mechanisms such as MLATs can be used to place restrictions on surveillance mechanisms. The Council of Europe's Cybercrime Convention, if bolstered with more robust human rights protections, can provide a legal framework that states can rely upon as a substitute for the application of political pressure to share information directly to private companies. Private parties are not well-placed to assess the legality or legitimacy of data requests. Often, they are not even given sufficient information to *attempt* such assessments. In this sense, strong legal protections and objective mechanisms for ensuring compliance are not only necessary, but once in place,

- **Transparency.** Transparency must be approached in a balanced manner. User notification is important, but should not be undertaken in a way that prematurely exposes and, hence, undermines legitimate investigations. Aggregate transparency, however, has no capacity to threaten an investigation and is necessary for informed policy making, and so that individuals can understand how their data is at risk from state access.

- **Cross-Pollination of Stakeholders.** It would be useful for businesses to increase hiring trends from civil society and law enforcement and for governments to increase hiring from civil society and from business. Additionally, more multi-stakeholder dialogue is useful to reach a common understanding of the issues and challenges involved.

- **Technologically Informed & Neutral.** It is critical to ensure laws and practices are not technology specific but, at the same time, they need to be greatly informed by a thorough understanding of their broader technical implications.

Background Reading:

The Draft International Principles on Surveillance & Human Rights:
http://necessaryandproportionate.org/

Global Network Initiative, "Principles on Freedom of Expression and Privacy",
http://www.globalnetworkinitiative.org/sites/default/files/GNI_-_Principles_1_.pdf

Brown & D. Korff, "Digital Freedoms in International Law", GNI 2012,
http://wsms1.intgovforum.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

J. McNamee, "Internet Intermediaries: The New Cyberpolice?", GIS Watch,
http://www.giswatch.org/sites/default/files/gisw_-_internet_intermediaries_-_the_new_cyber_police_.pdf

Escudero-Pascal & G. Hosein, "The Hazards of Technology-Neutral Policy: Questioning Lawful Access to Traffic Data", (2004) 47(3) ACM 77
http://web.it.kth.se/~aep/PhD/docs/paper6-acm-1905-reviewed_20021022.pdf

HRC, "Protect, Respect and Remedy: A Framework for Business and Human Rights", April 2008, A/HRC/8/5, http://198.170.85.29/Ruggie-report-7-Apr-2008.pdf

HRC, “Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy” Framework”, March 2011, A/HRC/7/31 http://www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf

ACLU, “New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance”, Sept 2012
http://www.aclu.org/blog/national-security-technology-and-liberty/new-justice-department-documents-show-huge-increase

State Surveillance and Human Rights Project
https://www.eff.org/issues/surveillance-human-rights

State Surveillance and Human Rights Camp
http://wiki.surveillancehumanrights.org/Rights_Camp_Brazil