DATA PRIVACY ON A GLOBAL SCALE: KEEPING PACE WITH AN EVOLVING ENVIRONMENT

A report from a roundtable organised by the Internet Society at the WSIS Forum on 16 May 2012 at Geneva, Switzerland.

INTRODUCTION

The WSIS Forum 2012 offered a timely opportunity to bring together insights and ideas from various initiatives presently underway across the world to review, modernise and/or develop new approaches to privacy to keep pace with the evolving global data environment. Building on that experience sharing, this roundtable explored potential gaps in current frameworks, issues surrounding interoperability, and some possible ways forward.

Background

In 2009, the 31st International Conference of Data Protection and Privacy Commissioners ("Conference") produced a *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data* ("the Madrid Resolution"). In 2010, the 32nd Conference adopted a *Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data*.

In 2011, the Organisation for Economic Co-operation and Development (OECD) published *The Evolving Privacy Landscape: 30 Years After The OECD Privacy Guidelines* plus terms of reference for the review of OECD guidelines, and started its review. The Asia-Pacific Economic Cooperation (APEC) adopted the APEC Cross-Border Privacy Rules System. The UN Educational, Scientific and Cultural Organization (UNESCO) also commenced research on a global survey of Internet privacy laws and regulations.

In 2012, the Council of Europe released proposals for the modernisation of Convention 108. The European Commission "proposed a major reform of the EU legal framework on the protection of personal data" that would "… strengthen individual rights and tackle the challenges of globalisation and new technologies".[1]

Further, at the national level, many countries introduced new privacy laws (e.g. Mexico and Peru) or proposed changes to their existing legal frameworks (e.g. US – where the Obama Administration recently released the *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* report).

At the same time, considerable work is happening in other spheres – business,

[1] http://ec.europa.eu/justice/data-protection/index_en.htm

technical, academic, civil society, users etc. – aimed at providing better solutions and guidance for online privacy.

The panellists

- Joesph Alhadeff, VP Global Policy and Chief Privacy Strategist, Oracle
- Michael Donohue, Senior Policy Analyst, Organisation for Economic Co-operation and Development (OECD)
- Petru Dumitriu, Head of the Council of Europe Office in Geneva and Permanent Observer to the United Nations Office and other international organizations in Geneva
- Christine Runnegar, Senior Policy Advisor, Internet Society (on behalf of the Asia-Pacific Economic Cooperation Electronic Commerce Steering Group Data Privacy Sub-Group)
- Cristos Velasco, Founder and Director of the North American Consumer Project on Electronic Commerce (NACPEC) and Founder and Director of Protección Datos México (ProtDataMx), México
- Rigo Wenning, Staff Counsel and Privacy Activity Lead, World Wide Web Consortium (W3C)
- Mika Yamanaka on behalf of Ms. Xianhong Hu, Division for Freedom of Expression and Media Development, Communication and Information Sector, United Nations Educational Scientific and Cultural Organization (UNESCO)

The moderator

Christine Runnegar, Senior Policy Advisor, Internet Society

PERSPECTIVES FROM THE PRIVACY ROUNDTABLE

UNESCO

On behalf of my colleague Xianhong Hu who is not able to be present, I would like to thank ISOC for inviting UNESCO to be part of this very proactive reflection on privacy.

UNESCO, as enshrined in its Constitution, promotes the "free flow of ideas by word and image", and has accordingly committed itself to enabling a free, open and accessible Internet space as part of promoting comprehensive Freedom of Expression online and offline. It is within this context that UNESCO started to explore Internet privacy, as one burning human rights issue impacting on Freedom of Expression in terms of following aspects:

- First of all, the right to privacy can support freedom of expression and freedom of information on social media, if we can ensure that an individual or activist has a right of anonymity, and a right to leave and be "forgotten".

- Secondly, right to privacy is already seriously challenged since users of social media have lost full control over their personal data and messages, which are being easily monitored and used by governments and businesses across the world.

- Third, the danger exists that actions and mechanisms to protect online privacy

could be abused by governments or corporations to infringe legitimate freedom of expression in general and the democratic roles of journalism in particular.

To further explore all these burning issues, UNESCO has initiated a global legal survey on Internet privacy, aimed at mapping the current regulatory landscape in the U.S., the EU, Asia, Latin America, Arab States and Africa in relation to Internet privacy and how it impacts on freedom of expression issues. The end result is to provide a set of recommendations arising out of our analysis of the existing legal protections, self-regulatory guidelines, challenges, and cases relating to the issue that will seek a balance that protects both rights and wards off any ways in which protection of privacy measures could be used to violate free speech. The research is to be completed by September and will be launched at forthcoming 7th IGF in Baku in November 2012.

All in all, we don't think there is a quick solution to address those challenges on protecting Internet privacy and freedom of expression. The biggest challenge of applying these rights exists in the discrepancy of the legal frameworks between online territory and the real one, given Internet's transnational diffusion. UNESCO will continue to explore the subject from a global and holistic perspective, and promote the exchange of good practices including developing criteria of good practices, as well as and international collaboration through multi-stakeholder approach within the global WSIS and Internet governance process.

Q. Are you able to draw any preliminary conclusions at this stage? To date, have there been any surprising results?

Throughout this preliminary stage of research, there four core principles we would like to draw and inform the future development of privacy standards, which would be constructive in protecting and not compromising freedom of expression:

Notice/Awareness – Users should be given notice of an entity's information practices before any personal information is collected from them.

Choice/Consent – Users should be given the choice of whether their information is collected, and how it may be used. Two common forms of consent are opt-in and opt-out.

Access/Participation – An individual should be able to access data about him/herself and to contest that data's accuracy and completeness.

Integrity/Security – There should be appropriate means to enforce privacy standards through the courts or meaningful informal, self-regulatory mechanisms.

There is also a need to develop principles around anonymity, which is a complementary issue to both privacy and freedom of expression. Such principles would advocate for very narrow limitations to the right to anonymity, as well as due process in regard to implementing any limitations.

OECD

One word about the broader context

At the OECD, we situate our thinking about privacy within a spectrum of policies that aim to feed economic and social progress and wellbeing.

In December 2011, the OECD Council adopted a new Recommendation outlining a set of *Principles for Internet policy-making*.

- They highlight the importance of strengthening privacy.

- But, that is one among a constellation of considerations aimed to ensure that policy frameworks provide the right conditions to maintain an open and dynamic Internet that continues to bring benefits to economies and societies.

Recommendations are the instrument of choice at OECD – certainly in the Internet space – where are members can agree on high-level principles that are non-binding, but represent a political commitment. That are usually technically neutral, ensure whole of government perspectives, and embody the measure of flexibility that enables diverse membership to come to agreement in a reasonable time frame on principles that will not likely be overtaken by the latest technology tomorrow.

OECD has a Working Party on Information Security and Privacy that looks at privacy together with cybersecurity issues, Identity Management. It tries to make policies from a solid evidence base. And does so with the presence of stakeholders from business, civil society and the Internet technical community sitting at the same table with government experts and representatives of other international organisations like the Council of Europe, European Union, etc.

Here in the WSIS, it is useful to highlight that broader context.

The Review of the OECD Guidelines

The OECD Guidelines on Privacy and Transborder Data Flows were the first international privacy instrument (beating the Council of Europe by a hair) and have been a seminal contribution to the privacy landscape over more than 30 years.

In 2010, on the occasion of the 30th anniversary of the Guidelines, we began reflecting *on the current state of privacy at the OECD*, through a series of events and papers, but all the while looking ahead to a formal review of the guidelines themselves, which began last year.

We are conducting the review in accordance with a short Terms of Reference document. The *Terms of Reference* provide the orientation for ongoing discussions in an informal expert group, which is being chaired by the Canadian Privacy Commissioner, Jennifer Stoddart.

The Terms of Reference highlight that, as compared with the situation 30 years ago (and maybe even 5 years ago), we are looking at a real *change of scale* in terms of

the role of personal data in our economies, societies, and of our course, our lives.

The environment, in which our traditional privacy principles have to function, has to take into account significant changes in:

- the *volume of personal data* being collected, used and stored;
- the *range of analytics* enabled by personal data, providing insights into individual's movements, interests, and activities;
- the *value of the societal and economic benefits* enabled by new technologies and responsible data use;
- the *global availability* of personal data, supported by communications networks that permit continuous, multipoint data flows;
- and not least, the *extent of threats* to privacy in such an environment.

The review is focused on three bundles of issues that OECD members have identified as requiring further work:

1. Roles and Responsibilities of key actors – how, for example, should we address the role of individuals which are now empowered with new tools to put privacy at risk.
2. Geographic restrictions on data flows – this goes back to heart of the OECD interest in this issue. How do we develop rules that work on a global scale? Cloud computing shine a bright light on this issue in particular.
3. Proactive implementation and enforcement – descending from the cloud, how do we ensure real effective protections on the ground. The rash of security breaches that regularly expose personal data highlight the need for greater efforts to apply our privacy principles in practice.

The informal expert group has met 5 times over the last 6 months, and is preparing recommendations to the WPISP, that has formal responsibility. No formal decisions have been taken at this stage as to whether the Guidelines will need to be revised.

The current approach is focused on adding new elements to the text that did not feature in the 1970s thinking about privacy. Issues include accountability, data security breach notification, privacy enforcement authorities, national privacy strategies, and improved metrics. Also looking to update our thinking on transborder data flows.

These changes would not necessary affect the basic principles for privacy protection contained in part two of the guidelines. The expert group is also preparing a new explanatory memorandum to propose to the WPISP, which would explain the proposed changes and the new context in which they have to function. These proposals are being finalised for consideration at the October meeting of the Working Party after which the more formal consensus building process begins.

Key URLs:
www.oecd.org/sti/privacyreview
www.oecd.org/sti/privacyanniversary
www.oecd.org/sti/security-privacy

Council of Europe

The modernisation of Convention 108

Objectives:

- To respond to challenges to privacy related to the use of new technologies
- To reinforce the right to data protection
- To raise the need to reconcile the right to privacy with other fundamental rights and freedoms
- To strengthen the implementation and follow-up mechanism of the Convention

General orientations:

- Maintain the Convention's general and simple principles
- Ensure consistency and compatibility with other relevant international legal frameworks, such as the OECD Guidelines and the European Union framework
- Maintain technologically neutral provisions
- Reaffirm the Convention's potential as a universal standard and its open character

Scope of the Convention:

- Preserve the comprehensive approach of the Convention, which applies to the public and private sectors alike
- The Convention should apply to all types of processing: both automatic and manual ones, structured to enable a search per data subject.
- Introduction of an exception concerning "purely personal or household" data processing

Duties of the parties:

- Take the necessary measures to give effect to the provisions prior to the ratification or accession of the Convention
- Undertake to allow the Conventional Committee to evaluate the observance of their engagements

Legitimacy of data processing and quality of data:

- The principle of proportionality
- The data minimisation principle
- Grounds for a processing to be legitimate

Special categories of data: sensitive data:

- Go beyond the existing closed definition of such data to enable to consider a functional aspect: the data may become sensitive according to the purpose of the processing considered
- It is proposed that data be qualified as sensitive, either by nature (genetic data, health data) or by the use of such data, as well as depending on the risk it entails for the data subject.

Data security:

- Security should apply to data as well as to its processing
- The obligation to report security breaches is introduced: this obligation will only be applicable to breaches, which may seriously interfere with the fundamental interests, rights and freedoms of the persons.
- This notification is to be done, without delay, to the data protection authority.

A new article on transparency and the list of information to be provided to the data subject is proposed.

Rights of the data subject:

- It is proposed that access to the origin of the data and to the underlying reasoning of the processing (Recommendation on Profiling) as well as the right to object to a processing be introduced.
- It was decided not to propose the explicit inclusion of a …*right to be forgotten*…as it was felt that the existing safeguards (length of time of data storage combined with right of rectification or erasure of data) coupled with an effective right of opposition could offer an effective protection to the person concerned without undermining the right to freedom of expression.

Additional obligations of the actors of the processing:

The controller is responsible for ensuring the implementation of the data protection provisions: asked to comply with those at all stages of the processing, carry out a risk analysis of the potential impact of the data processing on the rights and fundamental freedoms of the persons concerned.

Products and services intended for the data processing: they shall take into account the implications of data protection from the stage of their design and include easy-to-use functionalities allowing the compliance of the processing with data protection requirements.

Role of the Consultative Committee:

A strengthening of the Committee's functions and powers will be proposed in order to secure an effective implementation of the Convention.

Countries outside Europe:

Uruguay was invited to accede to Convention 108 by the Committee of Ministers last year. The Council of Europe is looking forward to this accession scheduled this year. Formal talks are occurring with other interested countries (in Africa, Latin America).

Further information is available via www.coe.int/dataprotection

APEC ECSG Data Privacy Sub-Group

The APEC Cross Border Privacy Rules (CBPR) System, endorsed by APEC Leaders in 2011, is a voluntary accountability-based system to facilitate the movement of data among APEC economies while still protecting privacy. It has four main components:

- an intake questionnaire for organisations wishing to be certified as CBPR compliant by a third-party certified Accountability Agent;
- recognition criteria for Accountability Agents seeking APEC approval;
- assessment criteria for use by APEC-approved Accountability Agents when reviewing an organisation's answers to the intake questionnaire; and
- a regulatory cooperative arrangement to ensure that each of the CBPR program requirements can be enforced by participating APEC economies.

The CBPR System documents are available to download via:
http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx

Q. What are some unique features of APEC's Cross Border Privacy Rules system and how did they come about?

The development of the APEC CBPR system was in no small measure shaped by the challenges that were faced. Chief among these were the cultural and regulatory differences in approaches to data privacy. Addressing these differences, while maintaining the consistency required to create an interoperable system, produced a unique mix of prescriptive, process-oriented details alongside a flexible approach to enforcement. For example, the CBPR system is very prescriptive in terms of the process for accrediting Accountability Agents and the way in which they demonstrate to member economies their ability to participate. At the same time, APEC has adopted a flexible approach to the way in which regulators in participating jurisdictions enforce the activities of Accountability Agents or the CBPR program requirements themselves.

Q. What challenges did economies face when developing this system?

One of the biggest challenges economies' faced, when developing a regional system that needs to function across as many as 21 jurisdictions, was moving from the principles-level to the degree of specificity required to ensure comparability. In practice, this meant taking the nine Information Privacy Principles found in the APEC Privacy Framework and turning them into specific program requirements and exemptions (50 in all). This process was by far the biggest challenge and took nearly two years to complete.

Q. How might the APEC CBPR System serve as a model outside the APEC region?

The APEC Privacy Framework is itself modelled on the 1980 OECD Privacy Guidelines. Insofar as these two principles-based documents are comparable, the CBPR system, which implements the former, would be particularly instructive for any country seeking to implement the OECD Guidelines.

Cristos Velasco (from civil society)

Q. What is your own personal assessment of the Madrid Resolution on International Standards on the Protection of Personal Data and Privacy after more than two years of its adoption?

In November 2011, Mr. Velasco had the pleasure of moderating a workshop on the assessment of the first two years of the International Conference of Data Protection and Privacy Commissioners' Madrid Resolution on International Standards on the Protection of Personal Data and Privacy and the Madrid Civil Society Declaration, as part of the activities of The Public Voice network of NGOs.

The purpose of that workshop was to analyse and discuss the practical implementation of the principles, recommendations and callings contained in both instruments, and to consider whether it would be feasible to establish additional measures after two years of their corresponding adoption.

Among the most relevant outcomes of that workshop were:

- That the principles contained in the Resolution are consistent with other principles codified in international instruments such as the OECD Privacy Guidelines, the APEC Privacy Framework and the Council of Europe Convention 108.

- That the principles and recommendations contained in both instruments, were followed and adopted in some Latin American countries (e.g. the obligation to notify users in case of data leakage and loss of personal information and the establishment of an independent data protection authority were adopted in the Mexican legislation on data protection of July 2010).

- There is currently NO universal standard on privacy and data protection even though some proposals have been previously established in statements of the data protection and privacy Commissioners conferences (Montreux Declaration of 2005) as well as in the Madrid Declaration and the Resolution.

- There is a strong need for the harmonisation of standards on transborder data flows and to strengthen the compliance and the enforcement regime of the data protection authorities.

- There was an interesting discussion about the *accountability principle* and consensus that a number of challenges still remain in the scope of interpretation of such principle by national data protection authorities as well as its practical adoption in most national data protection laws.

- The importance of establishing a harmonised regional framework on data protection within OAS with the possibility of creating a model law on data protection for the American region in the near future was also part of the main discussion.

- The need for creating user notification rules in case of data leaks and data breaches, not only from private companies but also from public and

government sector.

The panel concluded with the question of whether it would be feasible to establish an international convention on data protection taking into account the current social environment, the evolution and constant technological change and public policies on privacy and data protection. The great majority agreed that it would not be feasible at this point, and instead, the panellists considered that existing international instruments should be strengthened. One speaker mentioned that there is the need to promote the privacy and data protection principles of the Madrid Resolution and the Declaration in other international fora such as UNESCO, IMF, and APEC among others.

A brief report of The Public Voice Workshop on the Madrid Resolution and Civil Society Declaration is available in Spanish at: http://protecciondatos.mx/2011/11/espanel-sobre-la-declaracin-la-resolucin-de-privacidad-de-madrid-de-la-sociedad-civilenpanel-madrid-privacy-declaration-resolution-years/.

Rigo Wenning (from the Internet technical community)

The W3C has been working on privacy standards since 1997, starting with the Platform for Privacy Preferences (P3P), a standard for privacy policies in machine-readable form. The landscape has changed quite significantly since then. There is so much more information and personalisation, which led to advertisement via the Web ➔ monitoring ➔ targeting advertisements.

This led in turn to the development of a "Do Not Track" HTTP header that was seen as "an expression of will", i.e. it was not binding. Civil society said this was not good enough. The European Commission and the US Federal Trade Commission indicated that they wanted something binding. They turned to the W3C, which formed the Tracking Protection Working Group (http://www.w3.org/2011/tracking-protection/).

The first tangible results from the W3C Tracking Protection WG are due in June. Anyone can follow the work on the public mailing list, but the discussions are very technical.

The tracking specification is really a token that flows via the header. The rules are provided by the tracking compliance specification (i.e. what a web server is supposed to do if it receives the token).

One of the issues is that policy approaches to "do not track" vary. The European model of "opt-in" creates problems for technology.

"Do Not Track" could be a communication mechanism to convey what is intended and an interface to ask consumers about that consent thus again harmonising policy goals and technological capabilities.

The W3C Tracking Protection WG is trying to close the gap between regulator's expectations and what actually happens and is realistic in practice. At the moment, they are far apart.

Joe Alhadeff (from the business community)

Q. Some people refer to the revolutionary impact of the cloud? Is that hype or is it true?

Cloud is an evolution, not a revolution. What we see is the penetration of "cloud" into the consumer space and between consumers. There is not a regulatory vacuum – all laws apply. There are, however, some more complex issues such as jurisdiction. Data can be in multiple places at the same time, so there may be multiple legal jurisdictions involved.

Q. Individuals are interacting more and more with other individuals, directly on the Internet through platform services and across a myriad of devices. Does regulation adequately address these interactions?

Privacy itself is in a state of flux – more so than ever before since 1980. For example, the OECD Privacy Guidelines are under review, the Council of Europe Convention is in the process of being modernised, a new data protection framework has been proposed for the European Union, Mexico has adopted the APEC approach, Australia and New Zealand are revising their national laws and the US produced a white paper calling for a privacy bill of rights.

It is important to remember the dual objectives – privacy and international data flows – covered by a common set of principles.

Information is the currency of the digital economy.

What we see is an emerging focus on *effective* privacy regulation. We need effective, credible, practical, implementable laws. Well-intentioned legislation may not be narrow enough for real world application. For example, if by definition "personal information" includes IP addresses, there could be unintended consequences. Virus programs may need IP addresses to operate effectively. A known source IP address may also help identify possible malicious activity (e.g. if an account is accessed using an IP address normally allocated to a different region). If IP addresses cannot be used, the trade-off may be a need for higher levels of authentication to balance the increased risk.

It is difficult for regulators to keep up with human and technological developments. Consultative processes are very important, especially to ensure that unintended consequences do not materialise. A collective, collaborative and interactive dialogue is needed.

There has been some good work on voluntarily binding approaches, e.g. the European Binding Corporate Rules (BCRs), the APEC CBPR System and industry codes of conduct. BCRs in Europe need to be adapted to allow exchange of data between BCR validated companies.

DISCUSSION

Q. What is the role of users?

Mr. Velasco observed that one of the main concerns is how should users convey consent to all the different services they are using. In Mexico, signing up to a newsletter is "opt-in", according to new regulation. Users are aware, but do not know how to manage that consent. An Ontarian Privacy Commissioner has proposed the idea of "smart data" which would be managed by agents (i.e. they would manage the consent), but to whom would they be accountable?

Mr. Dumitriu stated that the Council of Europe is trying to cover both awareness and user control. The modernised Convention should provide user rights to: access to the origin of the data; the underlying reasoning for the processing; and to object to processing.

Mr. Donohue observed that the role of the individual is one of the key changes since the original OECD privacy framework was developed. He added that what we see today is a difference in scale and complexity of transactions, which needs to be reflected in an updated approach. Education and awareness raising are important, as is evidence-based analysis. Further, there is also a need to understand the behavioural economics and context.

Mr. Alhadeff said that "user-control" has become a buzzword and that we have to make it meaningful. Unfortunately, strict compliance means the user gets more information than they need which makes meaningful choice difficult. He added that we have to understand where the meaningful choice has to be made. Too much choice may not be meaningful. Mr. Alhadeff also noted that some of the work being undertaken around advertisement preference managers, which allows users to customize their experience, is a consent-based model provided there is enough transparency in the dashboards. It is not an "on-off" switch, but rather, a customisable structure.

Mr. Wenning noted that a recent study reported that it would take a user 76 days/year to read all the privacy policies of the services he or she uses. On social media, when users "friend", they need to realise that they are actually "friend-ing" "friends of friends" and that Facebook remembers all that they do.

Children and Privacy

A participant suggested that privacy policies should be written in a way that the young public could understand – bullet points and icons. She also referred to some research undertaken by Microsoft and published for Data Protection Day 2012 (see https://www.microsoft.com/privacy/dpd/default.aspx). Another participant reported an example where there was one privacy policy for the school administration and another for children.

There was also a discussion of netiquette, i.e. respect for individuals by individuals.

A participant observed that the more prevalent harmful effect among children is not actually online bullying, but rather, posting embarrassing pictures of others.

Seniors and Privacy

Mr. Alhadeff observed that senior citizens fall prey to fraud at higher levels than other groups of the population, but that as a group, they are very active on social networks. This may be in part because they are often physically challenged and social media offers a means to interact with family and friends. A Canadian study showed that senior citizens are very skilled at social networking, but less well skilled to use online social media. In contrast, children are very skilled at using the technology, but less well skilled at social networking. It could be very productive to have children and senior citizens teaching each other.

Some challenges

The discussion about user understanding, choice and control (adults and children) highlighted some of the challenges facing regulators, data controllers and others.

Mr. Donohue emphasised the importance of context and the need to incorporate this concept into privacy frameworks.

Mr. Lee Hibbard (Council of Europe) noted that "there is no silver bullet", and that businesses are not presently compelled to be at the table. He added that it is important not to underestimate the importance of dialogue – more dialogue is needed.

SOME BRIEF CONCLUDING REMARKS

Mr. Velasco reiterated the importance of involving all stakeholders in the due implementation of the data protection principles and standards at the domestic and international level. He also emphasised on the need to develop effective mechanisms for the enforcement of data protection laws.

Mr. Wenning observed that there will be a multiplication of fora, but added that he was not sure whether that was really a good idea. He also encouraged the Council of Europe to invite "techies" to the discussion and warned against using laws to solve technological problems – the system is fragile and there could be unintended consequences.

Mr. Dumitriu shared his involvement in the formation of the WSIS 10 years ago and commented that 10 years later we see complimentary dialogue among different interests (civil society, business, government, etc.). He added that for Europe, more focus is needed on "Pan-European" approaches.

Mr. Donohue noted that the discussion had covered rules, principles, frameworks, self-regulatory approaches, but had not covered privacy enforcement authorities in any detail. He noted the importance of international co-operation and drew attention to the promise of the Global Privacy Enforcement Network (GPEN).

Ms. Yamanaka joined other panellists in emphasising the importance of multistakeholder dialogue, referring to the IGF and WSIS Forum as examples of fora for such dialogue. She added that UNESCO is keen to ensure a global dialogue.

Mr. Alhadeff concluded with some key features – interoperable, context-aware, practical, implementable, and enforceable.

THANK YOU

The Internet Society would like to express our thanks to the WSIS organisers (ITU, UNESCO, UNCTAD and UNDP) panellists, moderator and participants for making this a very successful roundtable.

ABOUT THE ORGANISER

The Internet Society is the trusted independent source for Internet information and thought leadership from around the world. With its principled vision and substantial technological foundation, the Internet Society promotes open dialogue on Internet policy, technology and future development among users, companies, governments, and other organizations. Working with its members and Chapters around the world, the Internet Society enables the continued evolution and growth of the Internet for everyone. www.InternetSociety.org