26 May 2016

Report of the UNCTAD Ad Hoc Expert Meeting on Data Protection and Privacy: Implications for Trade and Development

Held at the Palais des Nations, Geneva, from 19 to 20 April 2016

Introduction

The Ad Hoc Expert Meeting on Data Protection and Privacy: Implications for Trade and Development, was held at the Palais des Nations in Geneva from 19 to 20 April 2016. Over 220 participants representing all stakeholder groups attended the meeting.

I. Chair's summary

The Ad Hoc expert meeting discussed recent and expected regulatory changes in the field of data protection and privacy, especially as they related to new challenges and opportunities for cross-border trade and development. Governments and international organizations as well as industry players and consumers presented their perspectives and outlined recent developments, current practices and relevant frameworks. The ultimate objective was to consider possible ways forward towards creating more coherent and internationally compatible frameworks for protecting data and privacy without unnecessarily hampering trade and innovation.

A. Opening statements

The Director General of the e-Government Bureau in the Ministry of the Interior of the Republic of Korea stressed the long standing cooperation on e-commerce, e-government and relevant legal reforms between the Government of the Republic of Korea and UNCTAD. He recalled that the world was changing into a borderless hyper-connected smart era beyond information society, as Internet of Things oriented services have expanded through the usage of Big Data and Cloud Services. As globalization was generalized and advancing, the enormous expansion of cross-border data circulation and transfers was raising new challenges. As the levels of approaches to data protection and enforcement of each nation were different, it was necessary to ensure a multi-stakeholder dialogue to discuss better interoperability of various data protection regimes. across borders. The expert meeting organized by UNCTAD was important in that respect, especially with regard to the often limited development of such legislation in developing countries.

The Deputy Secretary-General of UNCTAD highlighted the importance of multi-stakeholder platforms, such as the E-Commerce Week, for discussion on e-commerce and development. He highlighted that personal data had become the fuel driving current online activity as data traffic was changing the nature of globalization. Data protection was essential to create trust online and it was urgent to examine different ways to address the concerns that Internet users are expressing. Finally, there was a need to make progress with regard to the protection of data and privacy in the case of cross-border data movements. Having a clear understanding of the potential advantages of international data flows to trade and development as well as of the various concerns of the different stakeholders was essential to make progress on the international treatment of data protection and privacy. More work and cooperation were needed to ensure an enabling environment for e-commerce based on data protection that was inclusive and facilitated economic growth and sustainable development.

B. High Level Round Table

Panelists highlighted that digital transactions represented a large part of all trade today with information and communications technologies (ICTs). They were impacting all sectors and affecting everyone. Emerging trends and technologies, such as Internet of Things, smart cities, smart grids, and in the explosion of devices as well as data added urgency to this situation. The United Nations Special Rapporteur on the right to privacy highlighted the tight links between technology and commerce and how ICTs have changed everyone's life. Considering the increase in online

activities and e-commerce, the definition and respect of personal data was fundamental and there was a need to reinforce safeguards and creating new ones in order to protect privacy in this context.

Subsequently, it was important to recognize digital trade as an integral part of trade as a whole, rather than as a specific sector. Data transfers affected the business processes in sectors ranging from agriculture to logistics and among e-commerce players both large and small.

Data had become a key commodity for the digital economy in the same way that oil was a key commodity for the industrial era. Large numbers of products and services in today's global economy were created from data. However, some panelists expressed the need to be vigilant with regard to big data. As the volume of data went up, consumer trust and sense of control seemed to be going down.

Current consent models, through which consumers were presented with terms of use and had to give consent to acquiesce their data to use certain services on the Internet, were seen as not looking after the interests of consumers and were turning into forms of consumer "submission", according to some panelists. The problem was exacerbated by weak enforcement of consumer protection regimes.

Panelists highlighted that there was a need to consider how technology could help alleviate the problem and support in building trust. For example, some applications like "adblock" was one technological tool which could help consumers to handle data.

The formulation of standards was challenging as could be seen by the wrangling over the "Safe harbor" agreement. Poor legislation could act as a trade barrier that could deepen the lack of trust. Panelists warned that introducing misinformed legislation would cause harm for decades to come. Many panelists viewed legislation as something that was not transparent and should not be left in the hands of lawyers only, as it involved technology aspects.

Similarly, some panelists cautioned against separate regulatory regimes in different sectors to avoid the creation of fragmented data protection standards.

Mobilizing political will, such as in the case of the ECOWAS, had been an important part of regional initiatives to help promote trade aimed at reinforcing the security of data and data interoperability.

Privacy, freedom of expression, the right to liberty and to security, as well as the right to run a business, were mentioned as fundamental rights. Governments' needs and interests in accessing data for law enforcement reasons and national security needed also to be considered. Determining how to address law enforcement and national security needs put another layer of complexity on data protection and privacy issues. There was a need to "broaden the tent" so that different communities and stakeholders representing these various interests could communicate with each other in search of a solution.

C. Presentation of the new UNCTAD study on Data Protection and Privacy: Implications for Trade and Development

The Chief of the ICT Analysis Section of the Division on Technology and Logistics provided an overview of the UNCTAD's study entitled *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. This study reviewed the current landscape and analysed possible options for making data protection policies internationally more compatible. The study concentrated on seven areas when action is particularly needed. i) Addressing gaps in coverage, ii) Addressing new technologies, iii) Managing cross-border data transfers, iv) Balancing surveillance and data protection, v) Strengthening enforcement, vi) Determining jurisdiction and vii) Managing the compliance burden.[1]

[1] The study is available at unctad.org/data-protection-study .

D. Data Protection and International Trade: What's at Stake?

The panellists and experts discussed the rapidly changing digital landscape and the expanding role of data in international trade. A central theme was the increasing connectedness of the world, and the shift in prior globalization patterns to the digital era now taking shape. This new era was characterized by a prevalence of intangible and knowledge-intensive flows, more digital infrastructure, more participation from emerging economies and small and medium-sized enterprises (SMEs), free exchanges of information and content, more sources of innovation and instant access. This new type of globalization was leading to a new economic paradigm increasingly dependent on cross-border data flows.

While certain countries were increasingly connected, others still lagged far behind, especially in rural areas. Panellists also noted an increased volume of international flows of goods, services and finance. The major trend was the increasing volume and relevance of data flows, which, according to the McKinsey Global Institute, had added an estimated $2.8 billion of value to overall international flows of goods and services in 2014. Bandwidth in 2014 had increased by a factor of 45 times compared with the situation in 2005. There was evidence that data connectedness correlated with increased overall connectedness.

It was noted that many transactions, including related to e-commerce transactions, were now based on exchanges of data which were integrated into core business functions. Volumes of information were being gathered about operations in a wide variety of business sectors and practices, including production and outsourcing. The Internet of Things and impending spread of smart applications were identified as trends that will continue to increase the importance of data management. In view of these developments, panellists pondered the magnitude of disruption that would result from miscalculated regulation. Economic analysis – measuring the impact of economic uses of data and of data regulation – was stressed as critical. Challenges included the difficulty of measuring data flows, the economic relevance of data, and quantifying the impact of regulation.

Panellists emphasized the need to avoid overburdening businesses. There had been an explosion of data protection regulation since the 2000s as well as an increasing restrictiveness of regulation. Compatibility and clarity were highlighted as important regulatory qualities. The danger of having businesses caught between competing requirements in different jurisdictions was in disadvantaging SMEs, making it harder for them to take advantage of the global marketplace. Localization was considered as largely negative, resulting in economic inefficiency, increased vulnerability, and fragmented markets. Experts maintained that the ultimate effect was, however, highly contextual. The unique case of Estonia's "data embassy", located in a different country but subject to Estonian law, was referred to as a special localization measure that was made to address legitimate safety concerns.

Experts analyzed the potentially protectionist effect of data localization requirements and debated the relative value of fostering local industry versus the value of having existing and more efficient services present. It was widely thought that the net effect of such requirements would be negative in this regard. It was important to identify what regulations could act as trade and competition barriers. Developing countries were advised to consider their own cases as unique, especially in drafting data protection laws. In addition, countries were advised to consider the implications of competition. Using, but not blindly relying upon, existing instruments by default was also recommended.

Thailand presented its experience in enacting data privacy legislation, and identified the need to recognize different conceptions of privacy across different jurisdictions. On a similar note, experts discussed the difficulty of defining different categories of information, noting that conceptions of what is "personal" differs across cultures. Privacy was characterized as contextual in and of itself, further complicating matters.

Countries were encouraged to build capacity and continuous educational initiatives as a way to increase regulatory effectiveness in the face of an ever-changing technical field. Consensus was built around the fact that enacting baseline

data protection legislation was beneficial to all stakeholders, including businesses, governments, and civil society. The cost of "doing nothing" was potentially huge and should therefore not be regarded as an option.

Countries were encouraged to consider the correcting effect of market mechanisms. Protecting personal liberties was a common goal for stakeholders. Businesses, such as Apple and Microsoft, were mentioned as examples of companies engaging in activism. Multi-stakeholder involvement as such helped increase transparency and protect personal freedom.

E. Key Instruments and Current Practices

In this session, key players in international data protection presented current frameworks and data regimes. Several of the data protection instruments had been finalized very recently. The core principles of data protection, as well as the importance of interoperability and flexibility in the face of rapid technological change, were common to all frameworks.

The representative of The European Commission Directorate-General for Justice and Consumers, responsible for data protection policy in the European Union (EU), addressed the recent reform on data protection rules in the EU. The objective of this new set of rules was to give citizens control and consent over use of their personal data, and to simplify the regulatory environment for business. The data protection reform was a key enabler of the Digital Single Market in Europe.

The European reform had raised the interest of countries outside the European Union. To ensure that the regulation did not constrain business in the future, it followed a risk based approach, through which controllers and processors, depending on the level of risk of the data flow, had to adjust the safeguards and protective measures for personal data. Data protection by design meant that data protection accompanies the full cycle of development of services. The regulation recognized that international data flows were a necessity for business, and rules allowing transfers from the EU to other countries had been streamlined.

In discussing whether the adequacy requirements of the EU data protection regulation regarding privacy in data transfers discriminated against developing countries, the EC reminded that adequacy means "essentially equivalent"; i.e. third countries gave assurances that EU citizen data would have the same level of protection as in the EU, where privacy was a human right. That said, few countries were in the EC adequacy list, and concerns remained that compliance with data protection regulation would inhibit SMEs in developing countries from trading with the European markets.

Regarding the costs of implementing the new regulation in EU countries, there was no additional burden of having a well-developed data protection system; rather, the simplification of procedures between jurisdictions was expected to produce savings.

The representative of the United States Federal Trade Commission (FTC) provided an overview of the data protection regime of the United States which followed a sectorial and layered approach to data protection. Different laws at different levels governed types of personal information at the federal level, but state laws could also go beyond federal protection laws and have stricter privacy rules. The FTC had broad jurisdiction over consumer protection matters, including privacy. The US approach was to remain flexible enough not to have to update the law as technology evolves. The FTC did however stay on top of technology developments and made policy recommendations referring to such changes that have an impact on privacy and data protection. Finally, it provided business education and guidance to SMEs on data security. International cooperation work of the FTC included the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Enforcement Authority.

The APEC Privacy Framework had 9 core privacy principles (not legally binding) that represented minimum standards for cross-border data protection. In addition, the cross-border privacy rules facilitated international data transfers

without creating unnecessary barriers to data flows (like a privacy seal of certification obtained by businesses by complying with the APEC privacy framework principles). The principles built trust in the marketplace from businesses and consumers, and provided interoperability between national data protection regimes. The privacy framework also facilitated enforcement cooperation in Asia-Pacific. Interoperability with other regions of the world was enhanced, for example with the EU by developing a dual certification. In 2015, APEC Trade Ministers had acknowledged that the protection of personal information was an important tool for developing trade. In the ensuing discussion, there was a reminder that minimum standards for interoperability did not mean that individual countries need to lower their national standards for data protection.

The representative of the Council of Europe talked about the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was open to all countries in the world, not only in Europe. Open for signature since 1981, the principles were still applicable but the Convention's provisions had recently been revised. The scope of the convention was extended to non-automatic data processing, and reinforced the principle of proportionality. Obligations of data controllers and processors had been increased, as well as the right of data subjects to be informed. The revised convention strengthened national supervisory authorities responsible for ensuring compliance with personal data protection laws and transborder data flows, including those to third countries. In fact, data would only be transferred if the recipient State or international organisation was able to afford an adequate level of protection, and countries that had chosen to adhere to the Convention were obliged to legislate on data protection. The finalized draft of the revised Convention was to be discussed in June 2016 in Strasbourg, and the text was expected to be open for signature in early 2017. A universal framework for data protection was seen as necessary, and the Convention could give a solid basis to such a framework. The revised Convention was technology neutral, to be complemented by recommendations or guidelines to adapt to technology changes.

The representative of the Commonwealth Secretariat explained the diversity of Commonwealth member States. Some countries were following the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, some were bound by the EU Data Protection regulation, and others followed the African Union Convention on Cyber Security and Personal Data Protection, the ECOWAS Supplementary Act on personal data protection, Convention 108 or the APEC Privacy Framework. Some countries still did not have adequate laws and policies in place. In summary, there was no binding legal regime applicable to all Commonwealth jurisdictions, and data protection was regulated by domestic laws, mainly constitutional and statutory law provisions, as well as common law principles. However, the Commonwealth Secretariat had provided countries with a model legal framework that drew largely from the OECD Guidelines and its core principles. Going forward, the Commonwealth Secretariat aimed to take stock of the uptake of the model laws and to embark on a revision, taking into account new developments and weaknesses identified by the UNCTAD study. The Commonwealth Secretariat was concerned about the impact of data protection on global trade, transborder transfers, and the informal sector.

The representative of the African Union (AU) Commission presented the recent AU Convention on Cyber Security and Personal Data Protection. The result of 4 years of continental consultations and discussions, it aimed to strengthen basic rights related to data protection but also to facilitate data transfers. It applied to all sorts of personal data and national security information in electronic transactions. The basic principles for data protection were in line with the core principles of the other instruments that were presented during the session. The Convention adhered to international human rights law, with a particular emphasis on the African Charter on Human and Peoples' Rights, with several provisions that protect the processing of personal data. The representative explained that while the AU Convention would enter into force only after 15 signatures, implementation might come before entry into force and national ratifications. African countries had different levels of advancement regarding their data protection regimes, infrastructure, or institutions, but the Convention could be already an inspiration for adapting national laws. There was also a need to raise awareness about cybersecurity and data protection at the higher level of governments.

F. What Works and What Doesn't: Country experiences

Several countries presented their strategies with regard to Data Protection. Japan had enacted data protection legislation in 2005 and recently revised it to reflect changes in ICT developments, such as big data. Four points were stressed in connection with the amended legislation: i) the newly created Personal Information Protection Commission, which aims to facilitate the cooperation with the authorities and make it easier for consumers to file complaints, ii) a more up-to-date and complete definition of personal information, iii) the principle of making it necessary to obtain the prior consent of the customer, and iv) the identification of three types of cross-border transfers of personal data and the law applicable to each of them.

A representative of the Korean Internet Security Agency presented the basic structure and features of the data protection laws in the Republic of Korea. Privacy was recognized as a fundamental right in the Constitution, which included the right to control one's own personal information. The country currently had a general law - the Personal Information Protection Act (PIPA) - and several specific laws which mainly regulated the "data handling entities" in relation to personal information that pertains to living persons. Several OECD guideline principles were applicable in the Republic of Korea: collection limitation, data quality, purpose specification, use limitation, security safeguards, individual participation, openness and accountability. Public education and raising awareness were emphasized as very important during implementation.

In Sri Lanka, there was currently no comprehensive data protection law. Instead, issued related to data protection were covered across several different acts. The presentation identified possible considerations and approaches that could be taken to address this situation: i) adopt a comprehensive data protection law, ii) revise and add new sector-specific laws depending on ICT deployment and national interests, iii) opt for a self-regulatory approach and encourage self-regulating by the private sector, e.g. through codes of practice. Some of the factors influencing decision in this respect were the cost burden of new legislation and/or of setting up new government authorities, the fast changing nature of ICT, the growing business process outsourcing sector, and extensive public sector use of data, existing open government partnerships. At the same time the importance of international standards was highlighted. Sri Lanka had in 2015 become the first South East Asian nation to accede to the Budapest Convention.

In Brazil, the domestic approach to data privacy was still sectorial and fragmented. There was currently no consensus on the need for a comprehensive data protection law. Brazil had contributed to the Right to Privacy in the Digital Ages resolution by the UN General Assembly and the establishment of a UN rapporteur on this topic. The Government was a heavy user of private data given the large population residing in the country. Currently no data localization provisions were in place but the topic was likely to be discussed again in Parliament.

The Ghanaian perspective on data protection drew on a research report prepared by the private sector. It highlighted the lack of capacity and resources of the Government at the time of enacting and official launching the data protection legislation. Due to such constraints, a significant time lag had appeared between the drafting of the legislation and its actual implementation. Awareness-raising campaigns were also identified as essential in ensuring the effective implementation of such laws. Among lessons learned were the need to seek further international and bilateral support to ensure the transfer of knowledge to the competent authorities, development of expertise and support for policy guidance.

In the interactive discussion, the following questions were explored: what would be possible fora for knowledge transfer and expertise on data protection (and cost implications)?; to what extent had countries already enacted data localisation laws and factors driving demand for data localisation?; and what aspects could incentivize and revive government commitment on data protection in low-income countries. Among the factors mentioned in connection to data localization were the growing incidence of cybercrime, the competitive edge of the private sector, the need for governments to secure tax revenues and others. The session ended with a submission by Senegal on its data protection legal framework, including the law on personal data protection, the establishment of a Commission for Personal Data

Collection and the Community Law on credit which allowed financial operators to exchange information to deal with customers with excessive debt.

G. The way forward

This session began by noting the importance of capacity building and education in successfully implementing data protection legislation. Awareness and knowledge were identified as key elements leading to a compatible and sustainable future in global data protection. An understanding of context-specific challenges faced by different stakeholders, as well as knowledge of the global landscape, were critical to establishing a successful national regime. Countries were advised to bolster digital literacy through multi-stakeholder dialogue, held with the aim of empowering the individual.

Cooperation between Mali, Morocco and Burkina Faso was mentioned as an example of regional dialogue geared towards addressing national and regional concerns. The sharing of best practices between these countries had been an effective way to leverage experience. Mali had persevered through various challenges, including political disruption and changing political priorities, lack of training and knowledge and budget constraints.

Panellists stressed that creating frameworks which were at least interoperable and compatible with the global landscape was a more realistic goal than frameworks which were based on complete mutual recognition. Going forward, it was not only important that frameworks included commonly recognized principles, but also strong institutional support. Measures included in bilateral and multilateral trade agreements often lacked this institutional support. An important theme throughout the session was recognizing that data protection regulations have trade restrictive and competitive implications.

Effective institutional support included a competent regulatory agency, or "independent supervisory authority." Meaningful independence from other governmental affairs, supervisory behavior as a surrogate for data subjects' own enforcement of rights, and sufficient authority were necessary qualities. Acting as a surrogate was particularly important because data subjects did not always have the knowledge or tools to investigate whether their rights are being safeguarded.

Team-building between agencies was a way to bolster the strength of fledgling authorities. Established telecommunications or consumer protection regulators were identified as good partners for data protection regulators. Panellists stressed the building of a culture of cooperation in this regard. On the same note, there was a need for participation by wider audiences and industries in order to build a wider toolkit for managing data and for revising legislation. The issues were not only for lawyers and policy-makers to address, but also engineers, social scientists, etc.

Clear definitions, including the definition and categorization of different types of data, were important. Some panellists stressed that other areas would better be left less defined. For example, prescriptive laws with regards to technology were widely considered as detrimental to both businesses and consumers. Instead, simple, adaptable and interoperable regimes were preferable. A careful balance was needed in order to benefit all stakeholders and foster consumer confidence.

The European Union's General Data Protection Regulation was also discussed. Although the Regulation had received mixed reviews, parts of it, such as the "privacy by design" element, were generally regarded as positive. The Council of Europe Convention 108 was discussed as a potential basis for international consensus. Although panellists thought the instrument had potential, some were wary of the highly political process involved in ascension. Panellists advised countries not to wait for international consensus or standards before attempting to draft data protection laws. Starting down the path to creating an initial baseline law was important. In this process, countries were advised to consider the data protection regimes of countries that were doing trade with and seek compatibility with their principles. The

UNCTAD study on Data Protection Regulations and international Data Flows[2] had proposed several examples of countries such as Japan, New Zealand, Malaysia and Singapore which had recently revised their legislation to simplify it (no exemption; a central regulator), with the support of businesses, could also provide good example of current standards in this field.

On the issue of balancing personal privacy with surveillance, panellists noted that several guiding principles were common to most jurisdictions. These included: narrow tailoring, necessary and proportionate surveillance, and the provision of redress.

The meeting called for continuing the dialogue to address the concerns of all stakeholders in a balanced manner.

[2] Unctad.org/Data-Protection-Study

Annex

Attendance*

1. Representatives of the following experts attended the expert meeting:

Algeria
Australia
Azerbaijan
Angola
Bahamas
Belarus
Benin
Bhutan
Burkiana Faso
Burundi
Cambodia
Canada
China
Columbia
Costa Rica
Côte d'Ivoire
Cuba
Ecuador
Egypt
Finland
France
Gambia
Germany
Ghana
Greece
India
Japan
Jordan
Kenya
Korea, Republic of
Lebanon
Lithuania
Madagascar
Mali
Mauritania
Mexico
Montenegro
Morocco
Norway
Parkistan
Panama
Russian Federation
Saint Lucia

*This list contains registered participants.

Saudi Arabia
Senegal
Sierra Leone
South Africa
Sri Lanka
Sweden
Thailand
Turkey
United Arab Emirates
United States of America

2. The following intergovernmental organizations were represented at the session:

Commonwealth Secretariat
Council of Europe
East African Community
Economic Community of West African States
Eurasian Economic Commission
European Free Trade Association
European Union
Organization for Economic Cooperation and Development
South Centre
Organisation Internationale de la Francophonie
Organization of Petroleum Exporting Countries Fund for International Development

3. The following United Nations organs, bodies or programmes were represented at the session:

International Trade Centre
Internet Governance Forum
United Nations Commission on International Trade Law
United Nations Conference on Trade and Development

4. The following specialized agencies and related organizations were represented at the session:

IBRD
International Labour Organization
International Telecommunication Union
Universal Postal Union
World Bank
World Customs Organization
World Trade Organization
World Tourism Organization

5. The following non-governmental organizations were represented at the session:

Consumers International
International Centre for Trade and Sustainable Development
World Economic Forum