# WORKSHOP no. 86 REPORT

## ICC BASIS / Internet Society

**Internet Governance Forum (IGF) 2012, 6-9 November, Baku, Azerbaijan**

# SOLUTIONS FOR ENABLING CROSS-BORDER DATA FLOWS

A report from a workshop co-organised by the International Chamber of Commerce Business Action to Support the Information Society (Ayesha Hassan and Constance Weise) and the Internet Society (Christine Runnegar) at the Internet Governance Forum (IGF) on 7 November 2012 at Baku, Azerbaijan.

### INTRODUCTION

A thriving global Internet economy depends on international transactions and, therefore, cross-border flows of data. The free flow of information across borders is also a sign of a healthy and global information society. Accordingly, it is important to closely examine the multiple factors that may enable or impede this activity so that constructive strategies may be implemented to achieve this objective.

Enabling cross-border data flows, however, raises a number of important Internet governance policy considerations for a broad range of stakeholders, such as business, intermediaries, users, law enforcement agencies, governments, policymakers and the wider Internet technical community.

#### *The organizers*

The International Chamber of Commerce (ICC) created Business Action to Support the Information Society (BASIS) to raise awareness among the public, governments, civil society, intergovernmental organizations and technical community of what business requires to continue contributing to the development of the Information Society. It serves as the voice of business in the global dialogue on the Information Society, following two World Summits on the Information Society (WSIS) held in Geneva (2003) and Tunis (2005). For further information regarding BASIS, the partners, members and activities, visit: www.iccwbo.org/basis

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. For more information, visit www.internetsociety.org.

***The panellists***

- Meredith A Baker, Senior Vice President, NBCUniversal Government Relations
- Maria Häll, Ministry of Enterprise, Energy and Communications, Sweden
- Malavika Jayaram, Partner, Jayaram & Jayaram, Fellow, Centre for Internet and Society, Bangalore
- Christine Runnegar, Senior Policy Advisor, Internet Society

Unfortunately, two additional remote panellists, Danilo Doneda, General Coordinator, Consumer Protection and Defence, Ministry of Justice, Brazil and Ivan Sanchez Medina, Member of the Columbian National Telecommunications Commission, CRC (remote panellist) were unable to participate.

***The lead discussant***

- Kevin Bankston, Senior Counsel and Free Expression Director, Center for Democracy & Technology

***The chairs and moderators***

- Jeff Brueggeman, Vice President-Public Policy & Deputy Chief Privacy Officer, AT&T (moderator)
- Constance Weise, Assistant Policy Manager, ICC BASIS (remote moderator)
- Ayesha Hassan, Senior Policy Manager, Executive in charge of Information and Communication Technologies (ICT) Policy, ICC BASIS (chair)

***The participants***

The workshop was very well attended and included active participation.

***Background paper***

The background paper for the workshop is available here:
http://wsms1.intgovforum.org/sites/default/files/Background%20paper%2028%2006%2022.doc

### *The opening*

The moderator (Jeff Brueggeman) opened the workshop with an observation that the topic of this workshop, namely enabling cross-border data flows, has been a "hot issue" at recent IGFs. He added that there is increasing interest at IGF in cloud computing and its inter-relationship with policy. The moderator also noted that conversation began around "what is cloud computing" and what data transfers are involved. It then evolved into a discussion about potential barriers to deployment and policy concerns that may be raised by use of cloud computing across borders such as privacy and security. He concluded that the goal of this workshop is to take the discussion to the next step – to identify some solutions and positive trends enabling, promoting and facilitating cross-border data flows, which are important for the evolution of new types of services and the free flow of information, freedom of expression, as well as social and economic development.

### *Discussions with the panellists*

*What is the government perspective on enabling cross-border data flows?*

Maria Häll:

The key word is "opportunity". The government has an important role to play in enabling all sorts of development. It is very apparent, including at this IGF, that we are moving into a new space – new hardware, new software, new services, new ways of using services, etc. One of the most important objectives governments is to make sure they are also moving into this new world.

One course of action that governments can take is to act as a driver for innovation by applying good procurement practices and buying new services. Another enabling factor is balanced regulation.

*From a company perspective how are changes in technology and the growth of cross-border data creating (a) opportunities for your business and (b) potentially some new challenges to deal with?*

Meredith Baker:

We are at the crux. We see so much opportunity. Emerging technologies are offering the "unimaginable", transforming the economy, society and our daily lives. Traditional boundaries such as the distinction between online and offline, is it the system or the network, etc. are blurring. This presents both opportunities and challenges.

All of these new services rely on data flows, and those flows do not stop at the borders.

Some governments tend to be reticent and it is unclear whether that is fear of the unknown or just a lack of clarity or purpose.

Focusing on privacy and security, in my experience, what seems to work best for rapidly emerging new technological and business development is guidance rather than regulation. Principles based on frameworks seem to work well. The Canadian paper on accountability and governance is a good example of such a framework.

Therefore, we should focus on the “what” not the “how”. In other words, specify what outcomes you expect companies to provide or support and leave enough flexibility to allow companies to continue to innovate.

*What is happening in India with respect to data privacy and security?*

Malavika Jayaram:

I think in India we have had this kind of “schizophrenic” situation where we have gone from having no data protection law to having too much, or at least that is some people's perception.

Historically we did not have any data protection law, which has made India an interesting place to outsource to. India has also been a place where we have had a certain competitive advantage, coupled with a very highly developed software industry. These factors mean that is has been a great place to do business. However, even when we did not have data protection laws, we used EU model clauses to contractually achieve what our own legal system did not provide.

Recently, perhaps in the last 12 months, we have seen more activity in this space than we ever have, prompted by many e-governance schemes relating to employment guarantees and the Indian government’s desire to serve the Indian citizens in a more electronic fashion. There has been a lot of outcry from civil society and from the legal fraternity saying that the government cannot roll out these schemes without examining issues such as security and privacy, and, further, in the absence of a very robust data protection and privacy regime, the government should not roll out at all.

We have now come full circle, where the community has prompted the government to actually enact legislation to cater to all these concerns.

A draft privacy bill was proposed, but it “died a slow death”. Recently, the government set up a committee to consider whether India needs a privacy law and what that should look like. The committee published a comprehensive report about two weeks ago and tries to achieve some degree of harmonization rather than inventing something totally new. *[Report of the Group of Experts on Privacy, available here: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf]*

Last year when we implemented the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules enacted under the provisions of the Information Technology Act*, there was a lot of concern especially from critics in the U.S. that we had gone from one extreme to the other. That is, that we now have too much data protection and India’s laws are actually a lot stronger than what the EU directive requires. The Indian government reacted with a press note *available here: http://pib.nic.in/newsite/erelease.aspx?relid=74990],* which was meant to clarify the rules, but actually lead to greater confusion (including questions as to what is the legal status of a press note). It is what some people call privacy law by “un-reform”. So, now we have the situation where they said the rules will not apply to the software industry.

This will be an interesting space to watch.

*What are some of the enabling factors and challenges?*

*What are the trends you are seeing as APEC has been wrestling with these issues?*

Christine Runnegar:

One of the enabling factors is the open, distributed and inter-connected Internet.

One of the challenges with respect to privacy is that there is no universal definition of privacy, and privacy laws vary around the world. However, there is some convergence on principles and some agreement in various regions.

So, one of the challenges that the APEC region wanted to solve was how to take the agreement on privacy principles that are in the APEC Privacy Framework and make them operational for cross-border data flows across the region (21 economies). This led to the development of the APEC Cross Border Privacy Rules System (CBPRS) endorsed by APEC leaders in 2011. This year, the U.S. became the first participating economy.

The CBPRS is a voluntary accountability-based system to facilitate cross-border data flows among participating APEC economies while still protecting privacy. Participation is voluntary for economies, accountability agents and for businesses.

It has four main components:

- an intake questionnaire for organizations 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 programme requirements can be enforced by participating APEC economies.

It is a voluntary accountability-based system. One of the biggest challenges that APEC faced is how to take the principles and make them specific enough to operate across a number of jurisdictions that, while they have agreement on principles, have very different approaches to how privacy laws operate and should be enforced.

*What is the prospect that governments and countries would be being willing to accept that there needs to flexibility in the application of principles to enable cross-border data flows?*

Christine Runnegar:

An example is the APEC Cross-Border Privacy Rules System. It is relatively flexible in the way economies can participate. It does not specify how an economy has to enforce the arrangement; just that it has to be able to do that. However, it is also much more prescriptive, when it comes to what the accountability agents need to do to assess organizations and ensure that they are compliant with the requirements. It is a mixture of both prescriptive and process-driven and flexibility. So, I think the answer is going to lie with a combination of those elements.

Meredith Baker:

I agree. That is probably why multistakeholder discussions are so important. It is why we are here. There seems to be kind of a growing force that is receptive to the idea that accountability, adequate safeguards and flexibility are the primary concerns that need to be

addressed. There also seems to be recognition that the approaches that are working are providing protection with oversight and allowing for redress.

*What are some of the concerns you see with respect to cross-border data flows? Has there been any progress to address these issues?*

Kevin Bankston:

We have seen specific examples of certain countries or economies avoiding placing data or routing data in other particular countries because of inadequately protective privacy laws and, in particular, laws that allow access by government. The best example is the United States where we have heard complaints from around the world that people do not want to store their data in the cloud in the U.S. because of concerns about the authority the Patriot Act gives to law enforcement and intelligence investigators in the U.S. CDT and others have been seeking to address this by seeking reform of our government access-related laws in the U.S. through a coalition called the Digital Due Process Coalition. The issue has really started to "heat up" in our Congress and we saw a number of meaningful proposals put forward that we hope will be taken up in earnest next year.

Less hopeful is the situation when it comes to wire-tapping by our country's National Security Agency (NSA). Many may be aware of an illegal programme of mass wire-tapping that occurred under the Bush administration. There was a broad expansion of legal authority for the NSA under the Foreign Intelligence Surveillance Act Amendments Act of 2008, and that is likely to be renewed again this year. So there is an ongoing challenge where differing concepts of what is appropriate government surveillance or government access to data pose a threat to cross-border data flows and effective sharing of information in a way that would be economically beneficial to all of us.

Maria Häll:

I think it is a problem with transparency. In Sweden, we have discussed transparency as to who has control over the collected data, who will have access to the data, is the data protected (including, what security measures are in place), etc. Also, which set of law enforcement agencies get access, and if other agencies want and might get access, these issues are important to a avoid insecurity about the process.

*Is it fair to say that the only practical barrier to cross-border jurisdiction claims is the difficulty in targeting assets or individuals on foreign territory? And if not, what are other barriers that data protection authorities or law enforcement authorities for that matter face when trying to assert jurisdiction over data about their citizens or relevant to an investigation in their country when it is stored outside of their country?*

Christine Runnegar:

This is a difficult question that many people are trying to solve. The first problem is that there are different laws in different countries. Then, when it comes to enforcement there are many investigatory challenges where conduct occurs across jurisdictions, such as investigating what has occurred or is occurring and collecting evidence. This may be difficult because some of the evidence a regulatory authority may need to prove a case may be located in other jurisdictions. Acquiring that evidence from other jurisdictions may be complicated because there may be no legal basis to allow it or just simply because it is just physically

difficult to get the evidence. Further, obtaining a remedy or other outcome across jurisdictions is not always possible.

However, there are increasingly attempts by different countries to figure out how they can cooperate internationally, specifically at the level of enforcement, in a way that still protects the privacy of their citizens, preserves fundamental rights and principles, and the due process of law, etc. While it is a difficult challenge, there are increasing examples of different types of agreements to facilitate that cooperative enforcement internationally.

*Is India looking at international and cross-border data issues?*

Malavika Jayaram:

Historically, India was not an easy place to litigate (e.g. court delays), so other contractual solutions developed.

One of the encouraging elements in the new data protection framework that has been proposed by the committee is to embed it into the culture of the industry, and use self-regulation as a way to provide privacy protection in a way that maybe the law does not quite achieve. If industry is willing to adopt certain privacy principles through certifications etc. and these principles are harmonized those with what the rest of the world, it is easier to achieve privacy by design.

There seems to be recognition in India that law enforcement for data protection is “rocky territory”, but if it is tackled through industry and education, there is a much better chance of achieving the standards in other parts of the world.

*What role can or should treaty organizations play in establishing international legal norms for data protection? What are the benefits and risks of that approach?*

*To the extent that the United States lacks a comprehensive data protection regime akin to what there is in Europe or in India, how important would it be for the U.S. to enact some sort of legislation to enable cross-border data flows?*

Kevin Bankston:

There are privacy laws and privacy enforcement, which is handled through the US Federal Trade Commission and state regulators. But, it is a complicated landscape. Therefore, companies would like a more uniform and consistent set of privacy regulations, whether it is in the U.S. or globally. At some point, the complexity of managing different standards is going to be outweighed by the benefit of a uniform standard.

Christine Runnegar:

There has been a growing realization that privacy is such a diverse and context-specific topic that the conversation has drifted more towards compatibility and interoperability of approaches, rather than harmonization.

In the short-term we are unlikely to have a worldwide scale binding agreement. However, we might get very close to more compatible and more interoperable approaches. Some may be binding and some may be voluntary, i.e. the whole spectrum.

Two approaches currently underway: the modernization of Convention 108 and the Draft Convention on Cyber Legislation in Africa, which includes principles concerning data protection.

Sophie Kwasny (Council of Europe, speaking from the floor):

There are currently 44 countries (all European), which are party to Convention 108. However, Uruguay will be the first non-European country to adopt the Convention next year and several other non-European countries have also declared their in intention to do so.

The Convention takes a human rights approach. It provides a general level of protection – minimal principles of protection for the individual. The principles in the privacy bill proposed by the Obama Administration match this level of requirement.

One of the key issues the T-PD is addressing in the work that it is doing in the modernization of the Convention is trans-border data flows. The approach is that there should be free flow of data between the parties of the convention, and where there is an exchange outside the parties, there should be some flexible mechanisms to enable transfer of data.

The large degree of activity in this area (e.g. in APEC, Council of Europe, nationally and elsewhere) is a good indicator that we might reach global agreement on the common principles. Convention 108, which has its origins in a European regional organization (the Council of Europe), but which already 30 years ago involved non-European countries, is a useful tool that should be used by more countries around the world.

Meredith Baker:

It would be useful if there were some consistency. But, at the same time, it would be unhelpful to have something overboard that inhibits innovation.

Comment from the audience (in the discussion):

WCIT, which is very focused and targeted in a very short conference, especially for the ITU, in a very short period of time, is not the right place to have that discussion. The IGF is a much better place to come up with guiding principles as opposed to come up with treaty-based resolutions.

*What are the other key challenges or emerging threats that are most concerning or difficult for you and your stakeholders?*

Meredith Baker:

Two large concerns about why governments and others would erect barriers to cross-border data flows are that there is a lack of a technical understanding and a fear of the technology. All of the developments that we are discussing are a positive signal that countries understand this it is in their interest to solve these issues, and that there are ways to establish accountability without having control of the data remain within a country's borders in the traditional regulatory sense.

A third concern would be that a government may consider that their country may be disadvantaged economically if data is allowed to flow across-borders.

Regional agreements where there is recognition that there is a mutual benefit are a useful tool.

There are reasons to be optimistic that there are more signs of cooperation building rather than signs of new barriers being erected.

Maria Häll:

One of the challenges that could really hamper the development is the problems that where discussed on the earlier proposed SOPA legislation, that is, legislation that is drafted with a lack of understanding as to how the Internet really works.

Further, not really sorting out what the respective roles of stakeholders are in the value chain is also a problem. Multistakeholder dialogue is useful in developing clever, efficient solutions. Without it, it is a big hindrance.

***Discussion with the audience***

*What is the relevance to trade liberalization?*

Nick Ashton-Hart, Geneva Representative, Computer & Communications Industry Association (CCIA):

In the WTO context in Geneva, there is currently a 20 country pre-negotiation, which will become a real negotiation next year, on liberalizing trade in services. One of the areas that is most interesting to negotiators is how to promote liberalization of electronic commerce. There is a particular and real interest in liberalizing so that there is the free flow of data. This is because the negotiators have very quickly appreciated that arbitrary, or seemingly arbitrary, limitations on the flow of information are not free.

There are many other ministries in government who believe that filtering or blocking a service because “you don't like what is said on it” has no cost. By contrast, the trade people actually understand that ensuring predictable arrival of data, allowing rooting to follow the least expensive path and operate most efficiently has a trade value. However, there is limited knowledge as to how it works.

To government - It is important to talk to your trade ministry about this, ensure that they consider the other issues such as privacy, but ensure that they also understand that there are a lot of countries who are not interested in free speech. But, there are no countries that are not interested in money and in trade. So if you can ensure that people understand that an attractive commercial environment for Internet services needs data flows. You have to create a predictable legal regime and you have offer a place where people feel safe in setting up a service where a user might periodically say something that somebody does not like.

*Is that some of the motivation for the APEC work?*

Christine Runnegar:

There is increasingly recognition internationally that facilitating cross-border data flows is key to development of trade and, therefore, economic growth and innovation within the society. This appears in different places around the world. For example, last year, the OECD held a

High-Level Meeting on the Internet Economy: Generating Growth and Innovation, clearly recognizing and calling out the value of the Open Internet to the development of trade among the OECD countries, but also beyond. It is also evident in the approach taken by APEC with the APEC Cross-Border Privacy Rules System. Additionally, in Africa, there is a desire to develop a cyber convention to provide a well-understood continent-wide approach that could then facilitate trade within the continent and beyond.

*What are the next milestones for APEC? Could the APEC Cross-Border Privacy Rules System serve as an alternative or a successful example to the EU of how interoperability can work?*

Christine Runnegar:

One of the interesting things to consider is whether we can map the APEC Cross-Border Privacy Rules System to other approaches that appear elsewhere around the world, and one of those is the Binding Corporate Rules in Europe. In other words, whether what other regions are doing that might be compatible.

There is some work to do because obviously it would be useful to have a cross-border system that is as extensive as possible if we want to enable the level of global transactions that we want to do.

In terms of milestones, two important steps were the launch of the system and the acceptance of the first participating economy (the U.S.). Other important milestones are: the participation by more APEC economies; the approval of accountability agents; and then to have participating businesses. Hopefully, businesses will also see this as an opportunity to demonstrate to their customers and their regulators that they take privacy seriously and that they want to be actively involved in the APEC economy, and hopefully beyond, in a privacy-respecting way.

Jeff Brueggeman:

An interesting development is the emergence of governments looking to rely on private sector accountability mechanisms. We are starting to hear governments realize that this can be an efficient, but also flexible way to have some baseline protections without the traditional regulatory model applying. APEC seems to be as part of the solution.

*What are other impediments to cross-border data flows (e.g. export controls, intellectual property, security, etc.)?*

Maria Häll:

Those aspects are equally important discussing cross-border data flows.

There is a rather intense debate in Sweden and elsewhere right now regarding the role of the intermediaries. It is important to be clear on the different roles and responsibilities of the different players. Without this clarity, cross-border data flows could be hampered

Christine Runnegar:

Regarding intellectual property, one of the challenges for many users is trying to understand why the Internet is global yet intellectual copyright tends to be geographical, with restrictions by territory.

Jeff Brueggeman:

Privacy is just one example. Telecommunications is another. Globalization of every type of service is creating these challenges.

Malavika Jayaram:

One problem can be national security. For example, the Indian government was very insistent on having Research In Motion (RIM) provide the encryption keys to the Blackberry system. RIM has been fighting this, but now all of the telecommunication companies will have to now connect to the interception server located in India. So, that can be one threat to transborder information flows.

History can lead to some strange cultural overlays. For example, in India, because the country has a long history of corruption, transparency often trumps privacy and confidentiality. Transparency has become a popular buzzword and a successful objective for civil society, whereas privacy is still relatively new.

*Should data flows be treated differently?*

Jonathan Zuck, The Association for Competitive Technology:

At some level, the sovereignty of nations is going to always play a role in the flow of anything into that nation, and the idea that data flows are afforded special protection is maybe something that a lot of governments are going to question.

Maria Häll:

There are new security issues to address. To do so, there needs to be a dialogue with government and all the other stakeholders. The dialogue needs to be open and transparent.

Meredith Baker:

Of course, there are places that will need to be regulated. The law does not end because the activity is on the Internet. But, the point is to focus on “the what” and not “the how” and to be specific. With all stakeholders we need to identify those that need further discussion and possible government intervention, and if so, how to achieve that.

Malavika Jayaram:

One of the flaws we have in India is that we have a patchwork of clauses that relate to data protection. Also, because some were enacted as amendments to the Information Technology Act, they only cover digital data and things that are online or in computerized databases. This creates the weird situation where an offline record is not subject to the same clauses and the same protections. Exactly the same piece of information, if it is in a handwritten ledger is not going to have the same degree of protection as something that is computerized.

Christine Runnegar:

We should also remember that there are many laws that have existed for a long time in the so-called offline world that apply in the online world as well. Fraud is an example. We also have to be careful not to be tempted to regulate the technology instead of behaviour, because that is where problems are likely to arise.

Balton Ackers:

One of the recommendations of my workshop yesterday on cross-border cooperation, was to start using the laws that you have and stop worrying about the Internet.

*Telecommunication companies have been told by government that they are dinosaurs, but are the governments the real dinosaurs here?*

Maria Häll:

We need to use existing laws. The Internet is actually part of our world. We should not create any specific Internet legislation.

Governments should not be guinea pigs. They should go for solid solutions. This does not mean they cannot do new things, we should promote innovation and that can be doable with clever procurement without jeopardizing services for the citizens.

Jeff Brueggeman:

Regarding the claim that telecommunication companies are dinosaurs – To some extent business has to adapt to the technology every bit as much as the government. Networks are becoming more valuable than ever to telecommunication companies because they are the foundation for all the services. But, the Internet is different in a lot of ways in terms of the practical realities and challenges that it creates. Telecommunication companies can either adapt to - and think - in a new way, or they are going to struggle. We will probably continue to see many types of companies trying to get regulation to solve the disruption that the Internet is creating, and ultimately it is very difficult to do that with the technical realities.

*How do you balance privacy with safety and crime?*

Malavika Jayaram:

One of the obvious things is to make remedies proportional.

In India, some people were concerned that there would be rampant misuse of data, scope and function creep when the draft legislation for the ID scheme was proposed. The strongest penalty under the law was about $185,000, even for hacking into the Central Registry and obtaining the personal data of 1.4 billion individuals (including biometrics). So, sometimes proportionality is not set in the right place.

There is greater interest in many countries to delegate state functions to the private sector. For example, surveillance is often outsourced to ISPs. Sometimes, the government does not want to go straight to the person, instead they get the data directly from an ISP. We have

also seen the sort of chilling effect that has on free speech and expression. It is one of the heavy-handed ways government tackles the problem.

*What is the level of safety for cross-border data flows?*

Christine Runnegar:

It depends on what kind of transaction; how your data is secured from the point that you start entering it into your device to the other endpoint, etc. Different services offer different levels of assurance and security for data.

Jeff Brueggeman:

We are going to see the emergence of more tools to help users protect their identity and their data online from unanticipated re-use. I do not think that is necessarily a cross-border data issue. It is just a general data concern. Do users think about whether it is cross-border or not? Do they look for a trusted party that they recognize?

*What to do about the special case of privacy and children?*

Jeff Brueggeman:

That is an example of other more specialized, sector-specific privacy concerns (e.g. banking, healthcare, etc.).

Christine Runnegar:

Privacy is very contextual, as we all know, and it makes sense that, when businesses develop a solution, to not only look at the general privacy rules that might apply to the service, but also any additional rules that may overlay that, that give special and additional protection to children.

*Note: There was also a discussion regarding Google's practices. This is not reflected in the report, but can be read in the transcript of the workshop.*

### *Closing remarks*

- Maria Häll: I feel very positive about development. This kind of dialogue we have here at the IGF is very valuable for me as the government representative, and I hope also for other stakeholders. I would also like to bring this kind of dialogue home. I will continue to debate this, together with my colleagues both inside and outside the government. Multistakeholder discussions should also take place in our day-to-day work, not only here. Thank you.

- Meredith Baker: I agree with Maria. This is a very valuable discussion. This is a great forum to get it. The multistakeholder approach of the IGF has really proven to be valuable and this is the perfect topic for it. There is clearly a long way to go, but we do want to continue to have innovation. On the one hand, we need to protect our data and have these cross-border flows, but we also need to make sure that industry can continue to innovate so that we have this data that can flow across borders.

- Malavika Jayaram: In developing countries, we are moving from a “stick” to a “carrot” kind of approach. Previously, you protected data because of the fear of sanctions, whereas now, there is a growing sense that it actually makes business sense and it can actually add to your competitive advantage rather than take away from it. There is also a growing sophistication with the way the debate is progressing, and more often acknowledgment that it actually promotes business rather than adds to the cost, which was the fear before. That is looking very positive.

- Christine Runnegar: Thank you, everyone, for making this a really interesting discussion. We only had an hour and a half and there are many, many other issues that we could have discussed that are solutions for enabling cross-border data flows. So I hope you will go away and think about what some of those things are and spread the word. To end and echo the comments of Meredith, the IGF is a really excellent place to have this sort of discussion from different perspectives of different stakeholders from all across the world, and thank you very much.

**THANK YOU**

The International Chamber of Commerce Business Action to Support the Information Society and the Internet Society (ISOC) would like to express our sincere thanks to the IGF Secretariat, our expert panellists, moderator, lead discussant, remote moderator and participants (in-room and remote) for making this a very successful workshop.

:-:-:-:-:-:-:-:-:-:-:-:-:-:-: