Relatório de participação

Evento: IGF 2018
Datas: 12 a 14 de Novembro de 2018
Local: Paris / França

Conselheiro: Thiago Tavares Nunes de Oliveira
Representante do Terceiro Setor no CGI.br

Nota introdutória: o presente relatório pretende registrar a minha participação no evento em epígrafe, com destaque para a sessão #393 CLOUD Act & e-Evidence: implications for the Global South, moderada por mim. Procura-se evitar redundâncias e sobreposições com outros relatórios já elaborados pela assessoria do CGI.br e pelos demais conselheiros que participaram do mesmo evento e disponibilizaram seus respectivos relatórios.

Os grades *clusters* temáticos discutidos no IGF foram sumarizados pelo secretariado e estão disponíveis em: http://www.intgovforum.org/multilingual/content/igf-2018-key-messages

O sumário do Chair está igualmente disponível online:
https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6212/1417

RELATÓRIO DA SESSÃO

#393 CLOUD Act & e-Evidence: implications for the Global South

http://www.intgovforum.org/multilingual/content/igf-2018-ws-393-cloud-act-e-evidence-implications-for-the-global-south

IGF 2018 WS #393 CLOUD Act & e-Evidence: implications for the Global South

Format:
Round Table - 90 Min

Theme:
Cybersecurity, Trust and Privacy

Subtheme:
LEGAL & REGULATORY ISSUES

Organizer 1: Hartmut Glaser, Brazilian Internet Steering Committee (CGI.br)
Organizer 2: Luiza Brandão, Instituto de Referência em Internet e Sociedade (IRIS)
Organizer 3: Paloma Carmo, Instituto de Referência em Internet e Sociedade (IRIS)
Organizer 4: Thiago Tavares, Safernet Brazil
Organizer 5: Nathalia Patrício, NIC.br

Speaker 1: Fernanda Domingos, Government, Latin American and Caribbean Group (GRULAC)
Speaker 2: Malavika Jayaram, Civil Society, Asia-Pacific Group
Speaker 3: Paul Fehlinger, Civil Society, Eastern European Group
Speaker 4: Luiza Brandão, Civil Society, Latin American and Caribbean Group (GRULAC)

Relevance:

The development and spread of the Internet worldwide have reinforced traditional discussions about jurisdiction, as cross-border data flows aspects increase in scale and complexity. The adoption of data protection laws in more than 120 countries over the world has also raised a challenge in terms of legal harmonization and judicial cooperation to mitigate conflict of laws that have proliferated in recent years and to enforce judicial decisions transnationally as revealed by the Internet & Jurisdiction Observatory database. Besides those general aspects, the issue is extremely relevant from a global south point of view, given the concentration of Internet platforms in the developed countries and the fact that law enforcement standards and data protection frameworks are generally built around the experience of the developed north. As more countries from the developing south become integrated to the Internet ecosystem traditional global political and economic imbalances tend to be aggravated by the diffusion of formal and informal norms and practices related to the access to data for criminal persecution by domestic and foreign authorities. This session aims to entertain the debate among different stakeholders groups and the IGF community as a

whole about the following policy questions: a) What are the implications of recent institutional solutions adopted in countries in the global north to reconcile the protection of privacy and access to data to address crime and how will they affect the Internet ecosystem in general? What are the implications of those developments for countries in the global south? b) Bearing in mind the position of developing countries in the global Internet economy, how can the protection of fundamental rights of users be reconciled with lawful access to data in the context of criminal persecution by domestic and foreign authorities? What are the challenges and opportunities for the creation of legal interoperability between developed and developing countries in a mutually-agreeable and negotiated way (considering both the synergies and the incompatibilities of intergovernmentalism and multistakeholderism)? How to build a global scenario of balanced and coexisting jurisdictions?

Session Content:

Jurisdictional tensions were one of the key issues identified with the future of Internet governance by the NETmundial Multi-Stakeholder Statement. The jurisdictional problem (as adequately captured by the work of the Internet & Jurisdiction Policy Network) has mainly affected three issue-areas of the overarching IG policy agenda: (1) the reconciliation of transnational data flows and the protection of privacy be with lawful access requirements to address crime; (2) the global availability of content in light of the diversity of local legal orders and norms applicable to online activities; and (3) the preservation of the functionality and stability of the global Internet's addressing system (mainly the DNS) in light of different local laws applicable to local operators. While the three of them are interrelated and represent pressing issues in contemporary Internet policy debates, there has been a considerable amount of institutional development around the first item on the list as a way of updating legal frameworks that apply to the access to data (including cross-border access) in the context of criminal persecution. The issue is not new, however some very recent developments (e.g.: the expedited adoption of the CLOUD Act in the United States against the backdrop of the US versus Microsoft case before the United States Supreme Court and the beginning of parliamentary discussions about the e-Evidence Framework within the context of the European Union) have raised the stakes in discussions regarding the currently valid MLAT agreements and the political consequences of legal provisions that expand the reach of one country's jurisdiction and law enforcement prerogatives (either in terms of surveillance and access to data to inform criminal investigations and procedures or in terms of privacy and personal data protection, such as in the case of the European GDPR). As the majority of those initiatives stem from developed nations, this workshop aims at fostering discussion about the impacts in the Global South for countries to exercise their sovereignty and jurisdictional prerrogatives, for peoples to access justice and have their personal data protected, and for businesses to operate within solid and predictable legal environments.

Interventions:

The format chosen to this session enables both interventions from selected experts representing the full range of the multistakholder Internet community as well as for the general IGF audience. The onsite moderators will start the workshop by explaining the flow of the session (5min). The keynote speaker will make a short presentation on the topic of the session (10min). The following segments are structured around two segments, which will be dedicated to the discussion of the policy questions presented above (70min). In each segment (35min), the moderators will give the floor in a random fashion to four selected participants for a 5-minutes intervention each (20min). The remaining time in each segment (15min) will open the microphone for 2-minutes intervention from the audience / other participants. The second segment will repeat the format and length of the first one, but will deal with the second policy question presented above. That format is believed to enable both a controlled as well as a free style of multistakeholder dialogue and aim at providing an overarching conversation by a very plural group of participants on all of the aspects inherent to the international cross border access to data. The last five minutes of the session will be used by the moderators to summarize discussions.

Diversity:

The list of confirmed and prospective speakers comprises people from all stakeholder groups and individuals who have convergent and divergent economic, political and social perspectives on the policy questions proposed. The panel will comprise a majority of women among the speakers and follows a 50/50 gender balance in the moderation. Moderators and speakers come from countries in the Global South, some of them being newcomers to the IGF space.

Online Participation:

Online participation and interaction will rely on the WebEx platform. Those joining the session using WebEx (either invited members of the round-table or the general audience) will be granted the floor in the Q&A segment of the workshop. People in charge of the moderation will strive to entertain onsite and remote participation indiscriminately. Social media (twitter and facebook) will also be employed by the online moderator who will be in charge of browsing social media using some hashtags (to be defined).

Discussion Facilitation:

The discussion will be facilitated by the onsite moderators who will guide the debate in each of the proposed "rounds" for the workshop as well as during the Q&A and comments session. The online moderator will make sure the remote participants are represented in the debate.

Onsite Moderator:
Luiza Brandão (Technical Community, Brazil), Thiago Tavares (Civil Society, Brazil)

Online Moderator:
Paloma Carmo (Technical Community, Brazil)

Rapporteur:
Nathalia Sautchuk (Technical Community, Brazil)

Report:

- Session Type (Workshop, Open Forum, etc.): Round-table

- Title: WS #393 CLOUD Act & e-Evidence: implications for the Global South

- Date & Time: 13/11/2018, 11:50 – 13:20

- Organizer(s): CGI.br & IRIS BH

- Chair/Moderator: Thiago Tavares (CGI.br)

- Rapporteur/Notetaker: Diego R. Canabarro (NIC.br / CGI.br)

- List of speakers and their institutional affiliations (Indicate male/female/ transgender male/ transgender female/gender variant/prefer not to answer):

- Ms Lani Cossette, Microsoft, Business, female;
- Ms Fernanda Domingos, Federal Prosecution Service in Brazil, Government, female;
- Ms Monica Rosina, Facebook, Business, female;
- Ms Luiza Brandão, IRIS BH, Scientific Community & Academia, female;
- Mr Bertrand de la Chapelle, Internet & Jurisdiction, Civil Society, male.

- Theme (as listed here): Cybersecurity, Trust and Privacy

- Subtheme (as listed here): Legal & Regulatory Issues

- Please state no more than three (3) key messages of the discussion.

1. New unilateral, bilateral and multilateral solutions to balance the protection of privacy and access to data to address crime have reconcile three main objectives: fighting abuses and crime, while respecting human rights and fostering the digital economy.
2. Participants noted that the majority of cases of international cooperation today have some sort of connection with the jurisdiction of the United States. Institutional solutions developed in the Global North - disregarding the contextual aspects inherent to the Global South - have the potential to marginalize countries in the latter. A proper equilibrium between the needs and characteristics of every country should guide discussions about the development of institutional solutions to balance the protection of privacy and access to data to address crime.
3. There was a recognition that the MLATs system is ill-suited for the dynamics of the Internet. However, participants also underscored the importance of procedural and substantial rights inherent to the MLATs system, which is something that should not be abandoned in future modalities of cooperation. Scalability and interoperability are the main tenets for moving forward in discussions related to the matter.

- Please elaborate on the discussion held, specifically on areas of agreement and divergence.

Three institutional approaches were presented by the keynote: CLOUD Act, e-Evidence Framework, Additional Protocol to the Budapest Convention. The differences among them were explained. Some of the challenges inherent to each initiative were raised: challenges inherent to scalability of unilateral (e-evidence), bilateral solutions (CLOUD Act), as well as the multilateral approach (Budapest Convention). The first can be emulated (raising the risk of conflict of laws); the second can create casts of "recognized and unrecognized" states; and the third involves very different sets of interests that might complicate the achievement of consensus. A fundamental question that guided discussions was: “why (and what sort of cooperation is needed) in an international system?" There was consensus among the participants that cooperation as it stands today is more of an obstacle (talking about MLATs) instead of a sound instrument for enabling cooperation. However, participants also underscored the importance of procedural and substantial rights inherent to the MLATs system, which is something that should not be abandoned in future modalities of cooperation. One participant contended that due process and respect of human rights are fundamental linchpins to discussions regarding the evolution of international cooperation. Another participant explained that the global north has asserted its jurisdiction over data regardless of where it is located. Countries in the Global South could follow the same path and increase the complexity of the current landscape. Panelists underlined the importance of thinking of legal interoperability when discussing all this initiatives. There was a clear recognition that it is imperative to move away from the idea that location of data is relevant to allow for access or not to it in an interconnected World. All participants seemed to agree with the notion put forward by one of the panelists that independent judicial oversight is a sine qua non requisite for Law Enforcement Agencies to use data and information. Discussion with the audience covered the following topics: the role of independent judicial oversight for access to data; the fragmentation of national and international legal orders; and the perils inherent to data localization laws.

- Please describe any policy recommendations or suggestions regarding the way forward/potential next

steps.

One participant criticized the unilateralism of some of the initiatives under discussion and called for a more cooperative approach to the topic. Another one explained that uncoordinated initiatives can increase conflict of laws. One of the big challenges to be tackled by all stakeholders according to the participants is “how to provide human rights protection across borders”. Multi-stakeholder cooperation, especially for the Global South, was recognized as a means to assure that intergovernmental solution will not marginalize relevant actors that could help craft solutions that might avoid conflict of Laws. Additionally, agreeing on fundamental principles to guide cooperation and the development of institutional solutions was perceived as a fundamental step in moving forward towards scalable and interoperable solutions. The role of the private sector in working collaboratively with governments as well as in pushing back abusive behaviour by countries was highlighted. Additionally, some participants highlighted the importance of expanding the array of people involved in discussions such as the ones enabled by the session: from Law Enforcement Agencies and private companies to International Organizations, journalists, data and privacy protection community, academia, etc.

- What ideas surfaced in the discussion with respect to how the IGF ecosystem might make progress on this issue?

This topic was not covered by discussions that took place during the session.

- Please estimate the total number of participants: 63.

- Please estimate the total number of women and gender-variant individuals present: 32

- To what extent did the session discuss gender issues, and if to any extent, what was the discussion?

Gender issues were not within the scope of the discussions. However, all panelists took note and commended the session organizers for putting together an almost-all female panel for the discussion of Internet & Jurisdiction at the 2018 IGF.

- Session outputs and other relevant links (URLs): Not applicable.

Session Time:
Tuesday, 13 November, 2018 - 11:50 to 13:20
Room:
Salle VI

Istanbul

- 2013 IGF: Bali
- 2012 IGF: Baku
- 2011 IGF: Nairobi
- 2010 IGF: Vilnius
- 2009 IGF: Sharm El Sheikh
- 2008 IGF: Hyderabad
- 2007 IGF: Rio de Janeiro
- 2006 IGF: Athens

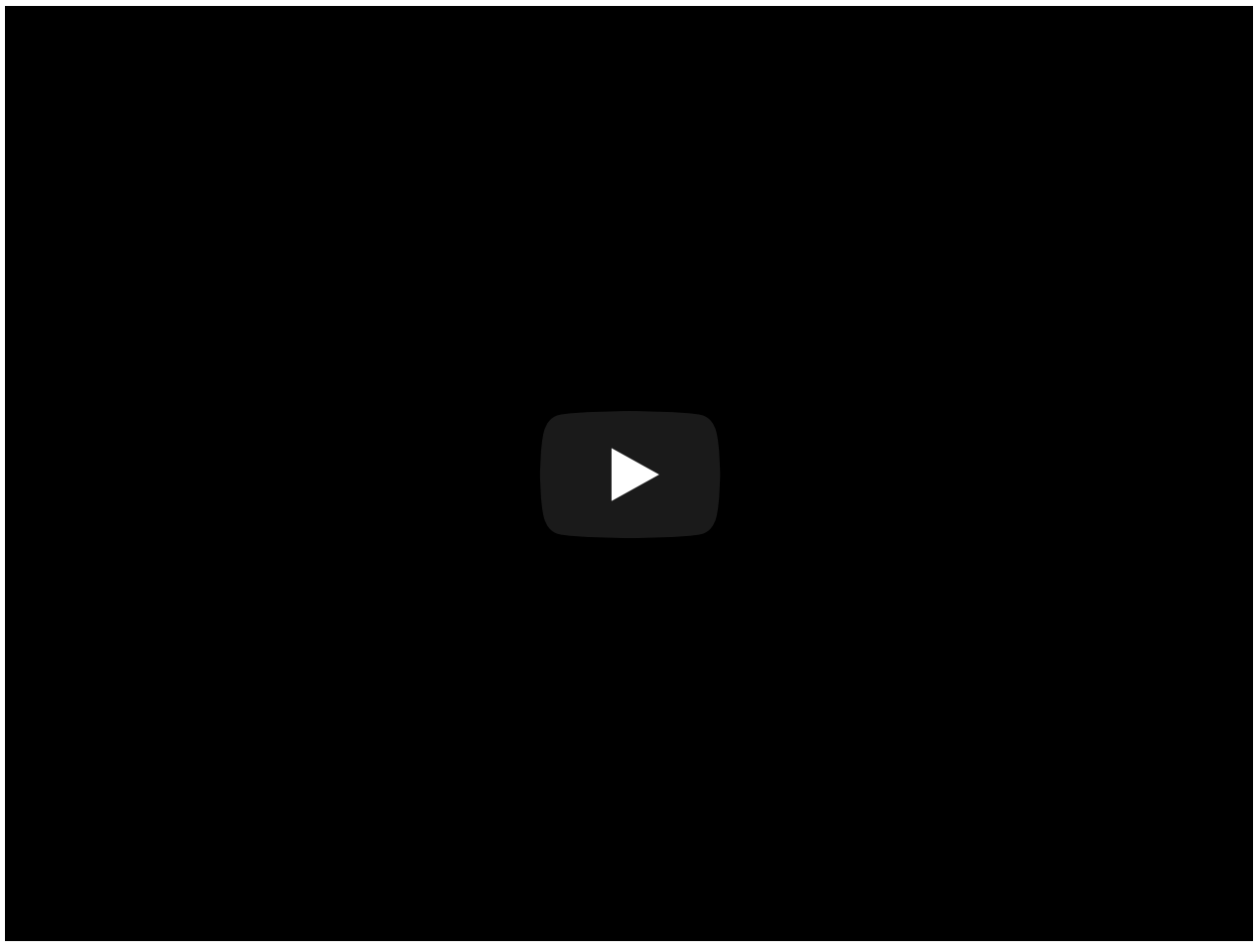
CH-1211 Geneva 10
Switzerland

igf [at] un [dot] org
+41 (0) 229 173 678

UNITED NATIONS

Contact | Copyright | Privacy Notice | Terms of Use

IGF 2018 - Day 2 - Salle VI - WS #393 CLOUD Act & e-Evidence: implications for the Global South



· Get the Report of the Session HERE

The following are the outputs of the real-time captioning taken during the Thirteenth Annual Meeting of the Internet Governance Forum (IGF) in Paris, France, from 12 to 14 November 2018. Although it is largely accurate, in some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the event, but should not be treated as an authoritative record.

***

>> THIAGO TAVARES: Good morning, ladies and gentlemen. Welcome to this session, CLOUD Act & e-Evidence: Implications for the Global South. This is the Workshop #393. And my name is Thiago Tavares. I am a board member of the Brazilian Internet Steering Committee. And today I have the honor to moderate this session with distinguished speakers that were invited, and in behalf of CGI.br, I would like to thank you very much for accepting our invitation.

Our schedule today is going to be structured in three segments. First we are going to have the pleasure to hear Mr. Bertrand de la Chappelle as a keynote speaker, and he will give us details and context on CLOUD Act and e-Evidence frameworks and provide some food for thought for the discussions we are going to have in the second segment, which is structured around two policy questions regarding those new national and regional institutional solutions to balance the protection of privacy and access of users' data to address crime online and the implications for the Global South.

So let me introduce you to the six distinguished speakers invited to this session. On my left hand I have Fernanda Domingos. She is a federal prosecutor at Sao Paulo office in Brazil, and she coordinates the cyber crime working team at the prosecutor services in Sao Paolo as well, and she is also a member and second coordinator of the National Brazilian Cyber Crime Working Team.

On my right hand, I have Monica Rosina. She is a law professor at Fundacao Getulio Varas in Sao Paulo, and currently she works as a public policy manager at Facebook offices in Brazil.

And on my left, I have Lani Cosette. She is a director of Microsoft EU Government Affairs based in Brussels, and where she focuses on data and privacy issues, and she also manages the company EU Academic Partnerships program.

And on my right hand, I have Luiza Brandao. She is founder of the Institute for Research on Internet and Society, IRIS, and she is also a master's student on privacy and international law at Federal University of Minas Gerais.

And I have my friend, Bertrand de la Chapelle, who is the Executive Director and Cofounder of the Internet & Jurisdiction Policy Network. Bertrand has been the team lead promoter and priority implementer of the multistakeholder governance process for more than 15 years. And he is building upon his diversity experience as a career diplomat. He was a member of the French Foreign Ministry for many times or many years. And civil society actor and entrepreneur. He was previously a Director on the ICANN Board, was a French Ambassador, and Special Envoy for the Information Society between 2006 and 2010. And an active participant in the World Summit on the Information Society from 2002 to 2005, where he promoted dialogue among civil society, private sector, and governments. Bertrand is a frequent speaker in major Internet governance process, Internet

Governance Forum, and others. Bertrand, it's a great pleasure to have you on this table, and you have the floor to give us your keynote speech.

>> BERTRAND DE LA CHAPPELLE: Thank you very much, Thiago.

Two things. First of all, it's a great pleasure to be here, also to see in the room a certain number of familiar faces, also from people who participate directly in the Internet & Jurisdiction Policy Network.

There's another thing I particularly appreciate, that for once it's not a man panel. So it's a great thing. And I want to start with the question that people usually don't ask when they discuss those issues is why are we talking about this? Because we are discussing various approaches to solve a problem, but if there's not a common understanding about why we are talking about this, the discussions cannot go very far. So very quickly, the situation, as you know, is that we have an international system that is based on the separation of sovereignties. It worked pretty well for a significant time. What used to be interactions between people across borders is becoming not absolutely the norm, but it is certainly far from an exception. And the second thing is that whenever something bad is happening -- and it can be a physical crime in a country or an online crime -- most of the evidence that is needed to actually do the investigation is increasingly digital, and it is increasingly digital and held by, in most cases, companies that are not in the same country as the country that is investigating

the crime. In addition, in most cases, it is held by companies at the moment are mainly headquartered in the U.S. It's not all cases, but it's the major cases.

So the bottom line is if you want to conduct an investigation, the international system currently is more the obstacle than the tool you want to use because the tool that you are supposed to use as an investigator in one country to access this information is to use the so-called mutual assistance treaties, they were designed for a period where those interactions across borders were very rare. So the Mutual Legal Assistance Treaty, they do work, but they are very slow, and this can take, for instance, depending on the countries, between ten months, up to two years, to get access to this information that is essential for the investigation. So yes, there are efforts to reform this thing, but it is also bumping into another problem, which is that in many respects, if you have an investigation that is taking place on a crime in Germany, for instance, or in France or any other country, or Brazil, the victim is there, the crime was done there, the suspect is also from there, and the only connection to the U.S., for instance, is the fact that an American-based platform was used. Why should the authorities in the U.S. have full understanding and vetting of whether this information is going to be provided or not? This is the reason why the three regimes we will discuss today -- the CLOUD Act, the e-Evidence proposal by the European Union, and the project of an additional protocol to the Addis Convention from the Council of Europe -- are intended to improve this and to provide modalities

for direct requests by the investigating authorities in one country to private actors in another country. And we are confronted with a challenge, which is it is all well and nice to try to be more efficient, but this shouldn't come at the cost of the protection of human rights, and generally speaking, the mechanisms of due process. So as we often say in the context of the Internet & Jurisdiction Policy Network, we are all confronted in most issues -- it can be for takedown of content or access of e-Evidence, with the challenge of three dimensions. We need to fight abuses that we are increasingly aware of of all sorts, and in this case, crime. We need at the same time to do it while respecting human rights, in terms of procedures in particular. And third, doing so without putting excessive burdens on the digital economy, which is one of the main drivers of the economy as a whole.

So reconciling these three objectives -- and I insist on the fact that this is not about balancing the three objectives. I hate the expression where you have to sacrifice one thing to obtain the other. If done well, it is possible to promote at the same time fighting of abuses, protection of human rights, and the protection and development of the digital economy.

So now there are three initiatives, as I mentioned. They have actually emerged pretty rapidly in the course of this year and last year. One is the CLOUD Act in the U.S. I don't remember by heart the wonderful acronym that they found, but it was a nice label. The second one is the e-Evidence proposal developed by the European

Commission, and the third one is the additional protocol to the Addis Convention.

What we are addressing today, after the comment on what those three proposals are, what are the specificities, is to see how countries in the South relate to those proposals, and particularly on the notion that I want to introduce and that I will develop further, which is the notion of scalability.

So what are those three approaches? Some of you may remember that there was last year -- and even before -- a very important case in the U.S. that was the Microsoft Ireland case. In a nutshell, investigation done in the U.S. by the FBI. The FBI was asking Microsoft to have access through a normal warrant, to have access to data regarding a suspect, and Microsoft was answering that this data was stored in servers in Ireland. And there was a long debate that actually went all the way up to the Supreme Court and was to be decided by the Supreme Court on whether, in other words, there was some dimension of extraterritorial reach of U.S. warrants when it was served to an American company, even if the data was stored somewhere else. And you understand that it's a big issue because it touches on very fundamental element of jurisdiction, which is territoriality. So in which conditions is there a dimension of extraterritorial reach or not was the core of the topic.

We didn't have the opportunity to see the Supreme Court decide on this case because beforehand, the so-called CLOUD Act

was adopted, and as you may know -- or not -- the CLOUD Act has two parts. The first part solved the Microsoft case, saying yes, the warrants that are served on an American company can have an extraterritorial dimension because the location of the data is irrelevant.

But there is a second part, which is the one that we are more directly concerned with here, and I would say without offending our American colleagues that the United States government cared much more about the first part of the CLOUD Act, which gave the power to the law enforcement in the U.S. to have extraterritorial reach than the second part -- which I detail now -- which is about whether another country can directly access or request from an American company access to this information. And you must know that in the U.S. there's a blocking statute, which is the Electronic Communications Privacy Act, the Stored Communication Act, that dates back to 1986 and that basically says a company in the U.S. can voluntarily provide information to a foreign subscriber, but you cannot do it if it is, for instance, about the content of an email. And the CLOUD Act in its second part is intended to solve this conundrum and to say in a nutshell if there is a bilateral agreement between the United States and a particular country that is deemed by the State Department and the Department of Justice jointly as being -- as providing a sufficient level of protections, then the investigators of that country will be allowed to make a direct request to a company in the U.S., including for content data, according to appropriate procedures that will be detailed in this so-called

executive bilateral agreement.

I don't get into the details. What is interesting is that the first bilateral agreement that was intended is still pending. It is between the United States and the UK. And it is important to see that the CLOUD Act was invented, and the second part was purposefully invented to allow this bilateral agreement, and so far it hasn't been implemented yet or concluded yet.

That's for the CLOUD Act, and if you think about it -- and I will come back to it in terms of scalability -- it is a series of bilateral agreements. It's a sort of hub and spoke mechanism, where the United States, which has the main operators, is saying I will unilaterally decide whether a particular country has sufficient protections in its own legal system, and we will make a bilateral agreement.

The second approach is different. It's the approach by the European Commission that has proposed a couple of months ago, a few months ago, something called the e-Evidence regulation that takes a different approach that I would qualify in some ways as multilateral, but it's not pejorative. One of the main differences is the CLOUD Act only lifts the blocking statute of the Electronic Communications Privacy Act, and allows the companies to voluntarily provide this information.

The e-Evidence proposal in Europe is considering so-called binding production orders. It would say that according to a very specific and detailed, very elaborate, actually, set of procedures, a European Union actor -- sorry -- investigator can ask

an American company -- and probably any other company that is "providing services in the Union" for the preservation or the production of data concerning a particular suspect. What is interesting is that there is a companion document that is not a regulation but a directive that is establishing the principle that any company from around the world that is providing services to European Union citizens should have and designate one legal representative in the European Union that will be entitled in a certain way to be served with those production orders. So it's a two-part regulation, a regulation that establishes the very detailed procedures for doing this, and a second directive that will be implemented in the different countries when passed that forces the companies to have a representative.

The difference between the two acts is also that the CLOUD Act has passed in the Congress, a bit strangely because it was actually slipped into the bottom part of the big budget document, so there was not much real debate. Whereas the European Union proposal is still a proposal that still has to be completely validated by the Council. And then go to parliament next year which will raise certain problems because as you know, there will be elections for the European Parliament next year, and nobody knows what will happen in that environment. But the proposal is on the table, and without getting into details, it is intensely discussed in the Council of the European Union, and there are a few challenges that are preventing this from moving forward very, very smoothly at the moment.

The final element that is a little bit less evolved at the moment is the discussion in the Council of Europe of an additional protocol to the Budapest Convention that will deal with those issues, and of course, given in the Council of Europe -- this is a multilateral approach. Remember the first one is multi/bilateral. The second one is unilateral but covering the rest of the world with a mode couple of extraterritoriality. And the third one is a multilateral approach which has a certain number of challenges. One is there are more countries, so it's more difficult probably to have an agreement. And second, most of the countries of the European Union -- not all of the country of the European Union -- are a member of the Council of Europe. So there will be a sort of scheduling of this because you cannot imagine really that they will agree in one space before they agree in the other one. So this is the landscape, three different initiatives.

Now, to finish this keynote, the topic of how does this impact other countries is a fundamental element because there's impact and scalability. Because the problem that I was mentioning at the first stage is clearly a problem that all countries in the world have to address. They all have investigations and all have citizens that are using foreign social media and so on. And of course, without making a judgment, the different legal systems in the different countries are very, very variable. The types of protections, the types of crimes that can be investigated, the procedures that are set at the national level, and in particular whether there is an independent validation of the warrant at the national

level or not varies tremendously from country to country. And I don't have to elaborate on the fact that whether you have an independent validation or not is a major distinction in terms of protection of human rights.

So the key challenge in terms of scalability is that, one, something like the European e-Evidence proposal has an impact on any operator around the world that actually has users in the European Union. Something that not all actors are necessarily aware of at the moment. And there is one category in particular that I know pretty well because I have been, as Thiago said, on the Board of ICANN and followed the work of ICANN for a long time -- this also applies to registries and registrars. There is a direct connection to a problem that we don't address here but that you may be aware of, which is the impact of the GDPR on the WHOIS system and whether or not you can know the name of the person who is registered the domain name. This is just to highlight those issues are not isolated. You cannot address this without taking into account the rules for protection of privacy, the whole criminal procedure rules in every single country, and even spaces that were not directly in the minds of the people as much in the beginning, i.e., the domain name system.

So part one of relation to the South is that operators in the South will have to designate one corresponding entity in the European Union if there are users in the European Union. But the second part that is more interesting is there is a connection today -- and I will finish with that --

there is a connection today between two debates, this one about cross-border access to user data, and another one, which is the so-called data localization laws. You know that there are some thoughts and some countries were thinking about adopting or have adopted strong data localization laws, in particular -- which means obligation of, I think, the data of their citizens, at least, located in the country so that they can exercise their jurisdiction -- because they are frustrated in many cases by the slow mechanism of the mutual legal assistance treaty. I don't want to delve into that localization as an approach except to say it is something that is technically difficult to scale and that will raise a number of questions regarding the situation of small countries, developing countries, if they have to adopt this sort of thing. So this means that it is extremely important to find a solution that is scalable to this issue of cross-border access to data. What I mean by scalable is it can go beyond the European Union or the few countries that the U.S. will make a bilateral agreement with, so that the incentive to have data localization is reduced.

And given the diversity of the legal systems in the different countries, there are tracks that are being envisaged that would say for instance -- and it's just a suggestion that has been raised and is being discussed in the contact group that we have on Internet and jurisdiction -- the notion that if you have a country that follows its national procedures for anything that is entirely national, that's okay. But whenever there is a transborder request that involves another platform and so on, there

might be additional procedures, guarantees that have to be determined. Think of it as a little bit an effort to have an interoperable global cooperation system for investigations that works a little bit like the Internet. Think about a legal system at the national level, and you have a sort of router that plugs into this legal system so that whenever it is sent to another country, it respects a certain level of criteria, procedures, protocol, et cetera.

So that's the challenge that we are confronted with. And the question of scalability, as a final point, is that it is different with the three systems. Very simply, a multibilateral system has some elements of scalability in particular because it puts the whole decision-making in the hands of one country, and it puts all the others in the position of having basically to pray that they will be recognized as sufficiently relevant.

The e-Evidence proposal in the EU has a different model for scalability, and I could very well imagine that beyond the European Union, it's not about having other es joining the system, but it's potentially having other countries mirroring or adopting a similar system. I could imagine Brazil, India, or other countries or even subregions adopting a mechanism that says these are the conditions and these are the standards we apply for the cross-border request.

The Budapest protocol has a different scalability. Just like the Budapest Convention, it has the ability to grow. But it may be difficult to get agreement at first, but it has the ability to grow. But

as you know, there are certain arguments about the Budapest Convention by certain countries who are necessary negotiator, signators to the Convention on the first hand. We say we actually apply the principles of the Budapest Convention, but we don't necessarily sign on the Budapest Convention. That's the case for many countries. In Africa, we had a session at the African union, where this was clearly indicated, there a range of countries mirroring the Budapest Convention.

So that's the landscape. I want to finish by saying the big challenge is that whenever we develop something -- and I want to repeat that the first objective is to solve a real problem with the objective of providing sufficient human rights protection for criminal investigations across borders. I think it's very important to keep in mind those two. It's not a matter of bypassing or lowering the standards. It's establishing a modicum of interoperability between the different regimes. So we need to develop this, and at the same time, we need to develop any regime keeping in mind that it needs to continue to develop and be adopted or mirrored by other actors in the future. And we have an Internet jurisdiction. One particular contact group at the moment that is working on this topic -- you can find it on the site, and some of the people in this room are actually participating in this exercise, and there will be proposals for concrete solutions for interoperability that will be proposed by April this year -- next year, sorry -- so that it can feed into the third global conference of the Internet & Jurisdiction Policy Network in June 2019 in Berlin in

partnership with the Government of Germany.

That's it. I am sorry I have been longer than I was allowed to, but the topic maybe called for it.

>> THIAGO TAVARES: Thank you very much, Bertrand, for this high-level and very comprehensive landscape. I would like to invite to take the floor Ms. Lani Cossette from Microsoft. We are going now to start the second segment of the session, and I would like to let you know that the speaking queue is already open on the system, so the audience remotely and also that are present here, you can use the system to speak and include on the queue for the third segment after the speech of the speakers.

Please, Lani, you have the floor.

>> LANI COSSETTE: Thank you, and thank you for including me and Microsoft in the panel to discuss this issue.

As mentioned, I am based in Brussels, so my focus and attention has been in the most level of detail with the legislation that's currently moving in the European Union, but I thought it would be helpful just to give a picture of the timeline. I know a lot of people in this room and on this panel have been working on this issue for years. We all seem to find each other, this complex issue. I will say we received, and Bertrand also referenced the Microsoft case that dealt with a warrant that we received for data stored in Ireland. Just to give you a sense of the timeline, we received that warrant, almost five years ago. It was December 2013. So it takes some time for the courts to adapt laws, and in parallel,

legislatures across the world have also been innovating laws. I think that's exactly what's happening. There's always been this outstanding question, maybe even a little controversial, how do we move away from this idea that the location of data should be a part of assessing the overall jurisdiction? I think it is a pretty significant development, the resolution of our case as well as the introduction of legislation in the United States and in Europe within the last nine months or so. I would say we are starting to see the rough boundaries of what an international framework could look like. So I think that that is interesting, at least we know what we are working with as we are moving forward. I will also say on this issue of the location of data and territoriality, I will say the issue is not completely solved. There is this inherent problem with the exercise of police powers.

That's not going away, so this needs to be part of the solution. The only way we see this moving forward is the introduction of international agreements to be able to manage the questions of sovereignty and also to manage issues around conflict of law, which was really the center PD piece and driver behind the litigation that Microsoft brought about five years ago.

So I think that's an important place to start, and I will also say with regard to international agreements, we are anticipating the UK has announced publicly that we should see the text of the agreement perhaps by the end of the year or maybe early in 2019, and you know, I think that this will also be an important step forward in defining what the overall picture and

landscape looks like so that we can continue to have conversations around scalability and as Bertrand suggests, mirrors systems around the world to make all of this fit together. But I think it's also important to remember that no two agreements will be the same. These agreements are negotiated between two sovereign countries, and there's a history and a culture and different set of laws that need to be understood, and the context needs to be considered when these agreements move forward. So I know there's been a lot of anticipation to see what's in the agreement. But the very idea of how these agreements work, which is based on application of the domestic law of both countries, is very important to keep in mind. That's why no two agreements will be the same.

I think also just a couple of broad comments that we need to take in mind when we move forward. We are talking about moving from mutual legal assistance to expedited access to data, and the tech companies are very much in the middle of this. I think taking a practical and realistic approach, that there needs to be a change and a role for the service providers, and I think based on the conversations we've been having in Brussels about what this looks like, this is a really, really important conversation to have, and it's a conversation that should not just involve the law enforcement beneath the data and the service providers that will be required to comply with requests when we receive them. This is truly a question for all of society. I think the conversations we've had to date, a lot of the litigation that has taken place has shown that the interests

go well beyond the two obvious interests of the providers and law enforcement, and that involves, I mean, you name it. You think of a large international organization that's protected by a complex set of privileges and immunities that could have implications for life and death. You think of journalists and concerns around free speech. You think, you know, conversations between clients and their lawyers and the protection of confidential information. Of course, data privacy I could have said first because we spent a lot of time talking about that. And of course, it's significant. So the concerns are quite vast and spread across all of society, which I think if this turns out the way we would like to see it turn out, the agreements will be able to acknowledge and represent some of these concerns when they become an action.

And I guess I want to keep this real short, so I will just finish with one last thought. You know, there has been this question about, you know, what level of detail and what role a service provider should play in pushing back or challenging an order when we receive it, and you know, this is something that Microsoft has been talking about for quite some time. We have always had this process of assessing legal process before complying with an order, and it was that very process that led to a determination obviously at the highest level of our company that we needed to challenge this order that we received in December of 2017. And this very question will take place in multiple jurisdictions. So far the conversation has taken place in the U.S.

because by and large our data centers have been in the U.S. and we have been mostly operating under U.S. law. But as all this expands, we need to have a serious conversation about exactly where the line is, and the conversation that's taking place in Brussels right now has to do with on what bases a provider could challenge an order. Could there be a challenge based on fundamental rights ground? You know, there's a question about if you add more notice into the procedure, does that decrease the role of the service provider, and should the role of the service provider be diminished in some way because the other safeguards protect it? And it is our very committed and strong view that providers absolutely have to play their own unique role. We don't want to replace the role of a judge or the judiciary, but we do feel strongly about the need to have a means by which providers can assess the valid process and make determinations about whether compliance would meet the requirements of the rule of law or the governing law that applies in that case.

So I look forward to your questions. I'll wrap up here.

>> THIAGO TRAVARES: Thank you, Lani. I would just like to remember the fashion that we proposed for this segment. What are the implications of institutional solutions adopted in countries in the Global North to help the protection of privacy and access to data to address crime, and how will they affect the Internet in general? What are the implications of those developments for countries in the Global South? With that in mind, I would like to invite Fernando, you

have the floor. (Off microphone).

>> FERNANDO DOMINGOS: Thank you, Thiago. Thank you for joining me here in the conversation also. I am law enforcement in Brazil. During the panel, I will give you the perspective of law enforcement for the Global South with all these initiatives.

Firstly, well, both CLOUD Act and e-Evidence initiatives grant their law enforcement agents the right to reach digital evidence stored cross-border considering some conditions. Also, the additional protocol to Budapest intends to regulate this possibility. At the same time, they have strong privacy protections to their citizens' or residents' data. So what I may say, when the Global North stands its jurisdiction over data, no matter where it is stored, the natural implication is that the Global South does the same and that it issues data protection laws to guarantee at least a minimum of privacy protection to the data other countries will reach in their territory or data pertaining to their citizens.

So considering the Global South follows the same path as the Global North, affirming its jurisdiction over data no matter where it is stored, I would like to make some ponderings considering the CLOUD Act. As Bertrand has explained, this is a unilateral initiative that solves U.S. problems to access their data stored abroad once it is controlled by an American company. Nevertheless, the option to qualify foreign countries to enter into bilateral agreements in order to get data from American providers

may not be a good option for countries which already have a legislation that grants jurisdiction over this data. When the qualifying country enters into an agreement like that, it is recognizing U.S. jurisdiction over data controlled by American companies. But these companies are providing services in the foreign countries and collecting data from its citizens and residents. Why should this data be under jurisdiction of the American government?

I would like to highlight some points about, for instance, hate speech or terrorism, propaganda, or incitement. The CLOUD Act will not allow American providers to disclose content in this case since the CLOUD Act is meant only to split up the MLAs and cannot change U.S. institutions in which the First Amendment grants freedom of speech. The only exception to freedom of speech in the United States was stated under the Brandenburg v. Ohio case saying that speech can only be prohibited if it is directed at inciting or producing imminent lawless action and it is likely to incite or produce such action. So the harm has to be imminent.

I think quite a number of countries grant freedom of speech -- like Brazil -- but with restrictions such as hate speech and terrorism incitement. Entering into a CLOUD Act agreement means recognizing U.S. jurisdiction over all data controlled by American providers, even if this data was collected in the country, as I already said, and renouncing to get data content in these cases of hate speech and incitement to terrorism. What it means to us, impunity to hate speech crimes and incitement to

terrorism, besides giving up the possibility of sanctioning the providers under the country's law when they refuse to disclose the data requested.

And don't come to tell me that we don't need content because it is already there in the hate speech. It's not true. We do need communication, private communications in these cases. Most of the times a group's planning something, so we do need the private communications, and so we need the collaboration of the service providers.

So I believe that countries which already have a legislation granting jurisdiction over data collected in its territory or countries with no regulation on the matter yet must be aware about leaving important crimes according to its citizens' ideas without criminal prosecution because another country will not disclose your data they believe does not concern to an illicit.

So that's it. I would like just to highlight these points on the CLOUD Act, and I think during the panel, I will come back to the e-Evidence approach. Okay? Thank you.

>> THIAGO TRAVARES: Thank you. Thank you very much, Fernanda.

And then I would like to invite Monica Rosina to the floor.

>> MONICA ROSINA: Thank you so much for inviting Facebook to be part of this conversation. I would also like to highlight how proud I am to see Luiza, who was one of the first youth fellows, to participate in IGF and to see how she is

leading a lot of these discussions in Brazil.

So we understand our responsibility as a social network to collaborate with governments when they are in pursuit of keeping their community safe. We agree that governments do need to keep their community safe. And we understand that safety and security are essential components of a more open and connected world. You cannot have one without the other.

We have committed to making Facebook and secure and good for society, and working constructively on public safety in the digital age with law enforcement is a big part of this. We have a shared interest with law enforcement in driving safe communities. Of course, in this context, we do need to also think about digital security, especially when it comes to less democratic countries. One of our greatest responsibilities is to protect the data that our users entrust us to. But we have been working with law enforcement to better enable them to protect the public without impacting user privacy. We have teams on the ground in every single region of the world that work with law enforcement in terms of understanding how we can provide access to data. We have a portal at Facebook that's specially designed for law enforcement to directly request access to data. But it comes -- there are cases in which as a company we are forced to choose which law to comply with. Because Facebook Inc. is the controller of the data and American law blocks us from providing content in most cases, whenever we have a sovereign nation saying that they have

jurisdiction, then in many cases -- and that's the case in Brazil -- we are faced with this conflict of law.

The Mutual Legal Assistance Treaty is an instrument that was designed to solve that, but it was designed way back then, when we weren't living this reality we are living right now. We understand and recognize that it's a slow process. It works, as Bertrand said, but it's slow, and it frustrates law enforcement. We do work with law enforcement providing access to content whenever the law of the controller, in the case the U.S., allows us to. So for example, in emergency requests, whenever we believe the matter involves imminent risk of serious injury, physical injury or death, the U.S. law allows us to provide access without necessarily breaking it. So we have worked with law enforcement in Brazil on that front. But whenever that isn't the case, then we understand that the international treaties are the due process for us to provide access to that content.

The CLOUD Act changed U.S. law to enable foreign governments to enter bilateral agreements with the U.S. This would tremendously speed up the process and remove legal barriers. And we, as a company, I just want to make sure that everyone knows that we worked very hard with the American government to make sure that the CLOUD Act worked.

So we understand that it will make the process easier and speed up, but we also understand that there has to be concerns over data protection taken into consideration, due process of law, and I

think it's important not to forget that we live in a world where local laws vary a lot, and so I believe that the international treaties, be them bilateral or multilateral, then that does provide a safe way for companies such as Facebook to provide data in a way that complies with human rights standards and also with best practices.

>> THIAGO TRAVARES: Thank you very much, Monica.

And then I have the pleasure to give the floor to Luiza Brandao, and I am very proud to have you here, Luiza, as a former youth program participant. Please, you have the floor.

>> LUIZA BRANDAO: Thank you, Thiago. Thank you, Monica, especially for the kind words.

So I think the order of debate will make a lot of sense because of the convergence of the ideas I have prepared here and the keynote that preceded our debate round.

So recently we have witnessed the adoption of the CLOUD Act in the United States and the beginning of discussions about the e-Evidence Framework within the context of the European Union. They represent the discussions regarding the current approach for international corporation through MLAT agreements and the political consequence of legal provisions that expand the reach of one country's jurisdictions and law enforcement prerogatives over the order. Concerns are raised about surveillance and access to data, especially regarding privacy and personal data protection. The case of

European GDPR or different data protection views over the world, including bills from the Global South, like the Argentinean or the Brazilian data protection regulations, are examples of these measures to safeguard users' rights.

Considering the global ecosystem of the Internet, an uncoordinated increase of agreements and regulations by different countries could mean deeper conflicts of law and a risk of fragmentation on different standards. Furthermore, it's undeniable that there is a power struggle between developed and developing countries that could be reflected in these active bilateral agreements and decrease the relevance of the multinational scenario, which has been viewed over the last years or even less decades. The bilateral approach, such as the one CLOUD Act suggests, include this agreement directly between states and could also marginalize other stakeholders, especially from the Global South, where decision-making is not as easily influenced by civil society or academia, for example.

The concerning about the development of new institutional solutions should include not just the Global South's point of view, but also the preservation of Internet's global nature, avoiding fragmentation, and a multistakeholder approach to build Internet governance.

So these are my notes for the first policy questions, and I think we have a lot to discuss now. Thank you.

>> THIAGO TRAVARES: Thank you very much, Luiza. And before we move for the second suggested proposed policy question, I would

like to ask Bertrand if he wants to make any comments.

>> BERTRAND DE LA CHAPELLE: Well, thanks for the privilege. In order not know delay this too much, two quick points. One, we are thinking a lot in a context where the big players are mainly American companies. But when we talk about scalability, I always tell my American interlocutors that if you have somebody living in American that is of Chinese organization that is using WEBO or any of the big applications from there, or there is somebody that is using a platform that is based in India or even that is coming from any other country -- it can be Brazil or Germany or whatever -- if we continue in the direction of the set of bilateral agreements, we need to have a sort of patchwork of multiple bilateral agreements between all those countries, and scalability will have to work also in the reverse. The situation should work also for future requests that the Americans may make to Chinese platform or that sort of thing. And the challenge of scalability for mutual legal assistance treaty is that it's purely mathematical combinatorial exponential growth. If you have to develop bilateral agreements between 190 countries -- I made the calculation once -- mind you, not by hand -- it's in the tens of thousands of agreements.

So what we need -- and that's the second point -- is something that's more generic and scalability approach that is more like the Internet. This is why I was making the analogy. When you have a network, nobody cares how your own network is structured. All you need to know is that the interface

to the Internet respects the TCP/IP protocol. And here is the same. There is no way the laws of all the countries are going to be harmonized. No way. Probably they shouldn't be. In many cases, it is a huge issue of identity. In France, for instance, denial of the Holocaust is criminal. It doesn't force anybody to adopt the same, but it is clearly part of the history. This is not about harmonization. This is about interoperability. And in that regard, part of the things that we are trying to develop in Internet, is not to develop a fourth proposal or regime. It's to discuss, for instance, how can you have a format for requests that use a series of tags so that whatever you develop in your own country to produce the request and however the portals are being developed by the countries, everybody knows that this is the field that says where it comes from, this is the field that says where it is going to, this is the field that says where the legal basis is or what it is, this is the elements regarding the crime. Think of it like HTML tags.

And the second element is that every time there will be a bilateral agreement in the context of the CLOUD Act, when there will be the discussion in the European Parliament next year, when there will be discussions in the Council of Europe on the Budapest Convention or any other country that was to develop something, part of the things needed is a set of criteria that we all agree should be checked in each of the proposals at two dimensions; one, the existence of this provision; and two, the level at which the cursor is being put. Example, I mentioned there is no agreement

at the moment on the fact that there should be an independent evaluation of any request that is transborder by an independent authority. There is no global agreement. But there is an agreement, I think, that is emerging that this is a criteria that has to be taken into account. Some will have, some will not. But everybody knows that there is a line, and you tick the box or you don't. That's the kind of work that is needed so that this is an interoperability regime rather than harmonization or just one global treaty and so on. These are the two things I wanted to share.

>> THIAGO TRAVARES: Excellent. Thank you very much, Bertrand.

The second proposed policy question is bearing in mind the position of developing countries in the global Internet company, how can the protection of fundamental rights of users be considered with lawful access to data in the context of criminal prosecution by domestic and foreign authorities? What are the challenges and opportunities for the creation of legal interoperability between developed and developing countries in a mutually agreeable and negotiated way, considering both the synergies and the incompatibilities of intergovernmentalism and multistakeholderism? How to build a global scenario of balanced and coexisting jurisdictions? With those questions in mind, I would like to suggest -- seeing no other interventions on the first round -- so you have the floor.

>> LANI COSSETTE: Thank you. I think this is a good segue to talk about some of these global trends and universal principles

that we might keep in mind going forward. I think I mentioned initially no two agreements will be the same because they do reflect what Bertrand mentions with regard to the unique sovereign experience of each country. So what we have done at Microsoft, we thought through the process of responding to these orders over prior years. We've thought through what we consider something that is a universal right, something that could be part of any domestic law in order to achieve an order that would comply with the standard of due process and human rights.

I have six of them. I will run through them quickly, maybe spend a little more time on a couple of them.

The very first and I think most important principle that we begin with is notice. No person's or company's rights can be vindicated if they don't realize their data is being turned over without them knowing. And I mean, it's really surprising to see the different and divergent approaches to notice in all countries. And it's something -- we've also had some litigation on this issue as well. I think this is one area where it's very easy for someone who is investigating a crime to check the box and say no, no notice. You can't tell the target of the crime ever sometimes where some of the orders that we were receiving. So I think that for all of us working on these issues, it's important to remember that the process begins with notice, and you know, there is a reasonable and a practical approach such that keeping these orders secret is the exception, not the rule.

We also have been observing with interest what we see as a trend toward independent judicial authorization. This seems to be a useful safeguard that could be applied.

Next would be we would want to see that there's specific and complete legal process. This is exactly what I alluded to previously when a provider receives these orders, you know, we are not going to be looking up case law and determining -- you know, and thinking about countries' constitutional law. But we can pretty quickly tell you if an order is abusive, if it's too broad in scope. These kinds of reaction also generally fit -- (tone sounding) -- is that me? -- will generally fit into an international agreement. Definitely I think, you know, we've learned that there needs to be provisions for ways to handle conflict of law. In the U.S. we have a process under common law for a hearing. For countries where this process doesn't exist, there could be statutory basis to create such a process.

And then the last two that I will mention, one has to do with specifically our customer base, and that is making sure that the order goes to the person or entity that is closest to the data. So rather than come to Microsoft for a company's data, it is better to go directly to the company. I think this is already being considered and baked into different policies among law enforcement, definitely in the U.S., and it's actually proposed and codified in the legislation we are looking at in Brussels.

Then the last principle would be there

needs to be attention and focus on transparency. There needs to be some understanding and publication of the number of requests, where they are coming from, and this I think will help inform the process more generally. Thank you.

>> THIAGO TRAVARES: Thank you very much, Lani. Then I would like to invite --

>> I will make some comments. Thank you, Thiago. I believe the countries have to enter into agreements or they have to grant a common level of data protection in order to allow the flow of information, mainly for law enforcement purposes. And yes, main and mandatory guarantee is an independent and judicial oversight, or at least an independent oversight, on the information to be used by law enforcement.

And in all this, I believe countries will need to take into account where the services are being provided and that data belongs to those persons in that territory.

I would like to tell about Brazilian legislation now. In Brazil, there is the possibility of cross-border access to data stored abroad by law enforcement, since 2014, when the Brazilian civil rights framework was issued. So it recognizes having legitimate interest over data that has been collected in Brazil's territory while a service is being provided there. If the service was collected there by a provider but the service wasn't being offered, we say we don't have jurisdiction over this. What happens a lot in Internet too. But data collected when the service is being provided there, we say that -- we affirm jurisdiction over this data. So in

this matter, Brazilian legislation accompanies the evidence proposal because that's exactly what e-Evidence says. If the service is being provided in the territory, they can request the data from the ISPs. And I believe the e-Evidence proposal has what Bertrand has said, in issue that you have -- the companies must have a representation there in order to assure the ordinance will be obeyed.

About data protection, in Brazil it has been recently enacted a data protection law. It's not a reaction to the CLOUD Act. On the contrary, it comes along with the European legislation, the GDPR, with the intention of having a data protection framework that allows the development of digital economy and allows the flow of information. So this law hasn't entered into force yet, and it's not completed because we don't have yet a data protection authority. But it's going to be created, and we also -- we don't have for now a data protection for law enforcement purposes, a specific law like the Europeans have Directive 680. However, concerning international data transference, this data protection law explicitly allows it for purposes of investigations in order to facilitate the international cooperation. So I think that's what all the countries have to do, facilitate this cooperation, the flow of information, given the human rights protections, be sure that this data will be -- will have all the guarantees, but the cooperation with the information has to be reached.

And what I think, considering all the panel, the question of Thiago, I believe

where countries start to affirm their legitimate interests over data and are beginning to be aware of the importance of data in the economy nowadays, this is the best moment -- well, I was going to say to harmonize legislation, but -- (Laughter) -- after Bertrand's statement, I think okay, we have at least to agree on the criterias about jurisdiction and about data treatment before the conflict of laws being insoluble.

Okay. Go on. Thank you.

>> THIAGO TRAVARES: Thank you very much. And we also must agree on principles.

And then I would like to invite Monica Rosina.

>> MONICA ROSINA: I totally agree that interoperability is at the center of this discussion. It is. You know, we are happy to see agreements and proposals being developed. No matter the approach, unilateral, bilateral, they seem to be a way forward for us to be able to work with law enforcement without having to go against the data controllers legislation. But one of the big challenges here is whenever we are developing something like this, how do we provide sufficient human rights protections across borders? I think that's one huge key element. Human rights safeguards should be at the center of this. And government access to data across borders and across the world must be consistent with sustained global norms of privacy, free expression, security, and the rule of law. That's where interoperability comes into play.

So I am extremely curious to see, Bertrand, how your Internet and jurisdiction is -- that's hard work.

(Laughter)

Yeah. I am very curious to get more info on that as well.

On a closing note, I would like to say we abide by and enforce the standards we set for our community. We comply with applicable laws in the places where we operate. And we insist the governments abide, as well, by their laws and with international recognized norms, which means that whenever governments exceed their authorities in requesting data, we will push back. So that's still an issue. Number just on a closing note, I would like to say that on the data localization topic that Bertrand touched upon, it is a technically -- we are seeing this conversation move forward in so many jurisdictions, unfortunately. It is technically difficult to scale. Bertrand mentioned especially for small and developing countries. But let's just remind that makes it really hard for also small companies to innovate. So not only on the governance side, but also on how will small entrepreneurs compete if they are forced to also have their data localized, and that's another issue that must be also taken into account.

>> THIAGO TRAVARES: Thank you very much, Monica.

Luiza.

(Cell phone sounding)

>> LUIZA BRANDAO: Thank you.

There is no question as reporting issues regarding crime investigations, the collection of evidence, and cooperation by foreign authorities. However, these actions must not come to the detriment of hard-earned and century-long fundamental rights, due process, and the rule of law. The relevant of users' privacy, security, and legality ought to be considered throughout the law-making and enforcement process. If we take into account that some of these states do not allow for public oversight, especially due to the need of confidentiality on criminal investigation, it's hard for us as civil society to ignore the fact that different players have been underrepresented in this process of bilateral negotiation. Both the CLOUD Act and recent European initiatives seems not -- seem to not fully consider the diversity of points of view in Internet governance that could come from the Global South and users' perspective on very basic concept. But extremely intricate, like privacy.

Therefore, the challenge relating to users' rights and the transnational enforcement to collect e-Evidence from the civil society point of view should also be followed by discussions involving multistakeholders in scenarios like the IGF provides and not just be centralized on the states or their authority's approach to Internet.

I agree there are challenges and opportunities here, as we all can see, and as an optimist, I believe civil society can play an important role in shaping these negotiations, like the IGF or law-making process such as the one adopted in Brazil's

Internet Bill of Rights. But we have to be organized, practical, and strategic, acting both at domestic and global levels in networks like the Internet and jurisdiction national community or in national coalitions in favor of users' rights. In addition to that, increasing cooperation between branches of government and their foreign counterparts, even for capacity building, may raise chance of success and correct enforcement of these laws and agreements, having in mind especially the transnational rule of law.

There is a long path to awareness on digital issues, and this is where the underlying challenges are. There is no easy or one-way solution to address the balance of jurisdictions. It is fundamental to consider local regional systems and their diversity. We must have in mind that complete submissions to one jurisdiction to another is no longer applicable. The international community must develop an approach of cooperation, including on what regards to the digital environment.

Finally, I believe there is an ever-growing necessity of reshaping the way we understand the concept of sovereignty. Under the digital age in the 20th century, jurisdictions must be shared, taking into account the global Internet governance standards, the fundamental rights of users, and documents we already made. Thank you.

>> THIAGO TRAVARES: Thank you very much, Luiza.

Now we have an opportunity to take questions and comments from the floor. I have -- there's one microphone there.

>> AUDIENCE: Okay. Does that work? I think so. It should.

It's just a small comment about what Monica said about the control of legislation and the way it is to safeguard human rights and have high standards for human rights. That is not necessarily true, and the discussions we are having about on the Internet and jurisdiction project about traditional independent oversight is showing that this is not true. For example, if you take the Brazilian legislation, every type of access to data, including subscriber information, demands an independent judicial decision. And in other countries, including the U.S., who has the controls, Facebook legislation does not require judicial order for subscriber information. So this is not very precise.

And if you I this the problem that we are having today at the Internet jurisdiction project with judicial oversight is that many countries that have strong safeguards on human rights do not require independent judicial oversight to have access to some types of data. So even though we all agree that independent judicial oversight is a great thing, many countries with strong safeguards to human rights do not require them. So this is a problem that we also have to address. I am from the federal prosecution service in Brazil.

>> THIAGO TRAVARES: Thank you very much. I have another question here and another one there, so we will take those two questions and then give back the floor to the speakers.

You have four questions. Okay. So you first, and then after you.

>> AUDIENCE: Thank you very much. I do represent the Ministry of Foreign Affairs of the Russian Federation. Frankly speaking, I do not have much questions. I've got many answers for these questions.

(Laughter)

Well, frankly, I didn't expect to see such quite professional dialogue there, including with the participation of just now of such giants like Microsoft, Facebook, and something like that. If you permit me, please, I would like to divide the whole of your discussion into parts. I will start from the latest one. Now, what is happening? What is possible that we in principle are discussing such different things like different jurisdictions, no rights at all, human rights, and all that. That is due to the absence of the international legal system well developed right now. Probably the Microsoft representative just mentioned about it.

What do we see right now in the world? It's a strong fragmentation, original legislations, and national legislations. Altogether in the world, there are seven, if my memory doesn't fail me, or eight -- probably seven -- original instruments, including the Budapest Convention, including the Shanghai Cooperation Organization Treaty, including African Union, Latin America, Arab States, and something like that. So the Russian Federation believes that it is imperative to develop a universal instrument for combating cyber crime in order to avoid such strong discrepancies,

like for example, the CLOUD Act initiatives. And right now, by the way, the latest idea in this regard, the Russian Federation did present this year during the 73rd Session of the General Assembly two drafts on the First Committee on the International Information Security that was accepted last Friday, and the second draft, the title of that, well, Countering the Use of ICTs for Criminal Purposes. The resolution will be presented tomorrow, and probably voting should be tomorrow. Right now there are 32 countries are the cosponsors of our draft, including all the Shanghai Corporation Organization countries, so it does reflect the importance of this issue. And with our draft, we would like to start the strong and wide political dialogue on the variety of issues in the UN system.

The problem number two, CLOUD Act. That is quite a curious document, frankly speaking. Russian Federation was the first one to start to ring the bells since January, as soon as we did read this draft. Well, I do completely agree that to some extent the United States would like to solve their initial interest at the expense of any other countries, unfortunately. That is true. Just for your understanding, I talked to Bertrand about it, on 14 February, The New York Times published an article in support of the bill by Thomas Bossert, Assistant to the U.S. President for Homeland Security and Counterterrorism, and Paddy Mcguinness, the Deputy National Security Advisor for Intelligence Security, with the title of "Don't Let Criminals Hide Their Data Overseas."

What is the main plot of this article?

The main message of the article is that the American leadership in cyber security cannot be ensured when U.S. law enforcement bodies investigating crimes lack access to users' data stored outside the country. At the same time, the idea of dividing the international society in two blocks is clear. The first one includes so-called democratic countries, which respect human rights and good faith and allow to enjoy the maximum freedom of access to users' data and to counter criminal and terrorist threats. In other, there are authoritarian states that should be denied such options. But there is a big concern among American companies that the introducing of this law will just go to the -- well, flowing out of the different customs along the road.

So just shortly, just last word. Now, the political influence of this CLOUD Act, unfortunately, saying precisely about the Budapest Convention and the second protocol, how it is possible to convince the whole community to hold this document as the universally accepted when the second protocol, it is closely connected with the American jurisdiction and the founders of this convention right now directly and loud and clear saying we don't need any other legislation of other countries, but only the American legislation should be very close to the second protocol.

Thank you.

>> THIAGO TRAVARES: Thank you. We are strict on time, so I would like to kindly ask you to keep your interventions around maximum one minute to give back the opportunity to speakers to react.

Please, your name and affiliation.

>> Firstly, thank you for the very engaging and articulate discussion. I represent Freedom Law Center, an organization based out of New Delhi, India.

Quickly, India is rapidly heading towards data localization regime, where already certain sector regulators, like the Central Bank, have mandated a strict mandate for data localization.

My question is to -- we have corporations and civil society here. In a situation where India does bring in data localization, what is the role of corporations, and also what should civil society organizations do to make sure that that doesn't infringe privacy and data protection principles?

Thank you.

>> THIAGO TRAVARES: Thank you very much.

There is another question from remotely.

>> RAPPORTEUR: There is another question. I am just rapporteur, I had a question, but I yield to the chair in order to keep the discussion going.

>> Sure. Just I am sorry, I forgot your name. Melissa? Just maybe as a response to your comment, I would just like to remind you that compliant with Brazilian law, also raised by Fernando, Facebook does provide basic subscriber information directly to law enforcement through our portal. It is when it comes to content that we are faced as a

company with the conflict of laws. However, of course, if we can overcome the challenge of having human rights safeguarded in international treaties or approaches, we would be happy to work even closer as long as we make sure that those standards are internationally met. Because we are a global company, that's something we must keep in mind. We are not only dealing with Brazilian government. We are also dealing with several other countries in the world who hold certain standards of human rights and data privacy extremely different. So I think that's our challenge. That's the challenge on our part. How do we -- and the word is not interoperate -- but how do we harmonize that on our part?

>> So thank you for your question about the civil society action. As I mentioned before, a way could be more coalitions between these actors from the civil society in a way to not be in this space but also contribute with proposals, so joining the debates and looking for those comments as we have talked here. So we could manage to engage more in this debate.

>> I'd like to make a comment on the Budapest Convention because I don't think it goes -- it is an American biding to the legislation American. I think Budapest Convention does exactly what is needed to agree on criterias. And although maybe it's more a slow process because it's a multilateral agreement, but I do think it's a good way, it's a good path for countries. Because a big agreement with all countries, I think it's complicated because it touches the problem of harmonizing legislation with what will never happen. So at least

agreeing in the criterias would be a good way to provide cooperation among everybody, every country. So I don't know. We have to see.

>> Picking up from several of the questions, you know, around defining the principles and independent judicial authorization and the role of civil society, I would say I think that this is -- this is an important moment in time when, you know, civil society groups have never been more important to -- I mean, the entire existence is thinking about what is a procedural right and how can it apply. So you know, I know that it's an interesting moment, too, when companies, you know, we need each other at this moment to be able to learn from each other and build a legal process that is future proof but that fits with our traditional ideas and understanding of due process. So we are already doing that, and I think there's absolutely definitely a role for civil society in the Global North and the Global South to figure out how to accomplish that.

The other point I wanted to mention around the independent judicial authorization question, I think this is an interesting one. You know, among the six principles that I listed, it is one that requires countries all over the world, you know, to change their laws. But I think realistically, you know, for a country to enter into a bilateral agreement for expedited access to data, moving away from mutual legal assistance, requires some significant thought and negotiation, including potentially reconsidering domestic law.

The last point has to do with thinking about data and how our understanding of the data itself has to adapt to older laws. If you think about some of the recent course cases in the U.S., we saw the Carpenter case, which dealt with the level of sensitivity around location data. I think it had to do with location data from cell towers. There are also some cases in the European Court of Justice dealing with IP addresses and the IP address being able to determine the location of a person. These are new questions, courts and legislatures should be asking, are asking, and now is the time to think about what is the safeguard, what is the procedural right that should match the level of sensitivity of that data? And those are open questions right now. You know, it's kind of a moving target when legislatures are trying to write new laws that deal with what may be independent prior judicial authorization should be required for content only. Maybe it should be required for other types of sensitive data that could reveal something about a person based on their location. So I think these are open questions, and you know, even if there's quite a diversity, you know, what we at Microsoft are trying to do is identify what are some universal principles that could be applied everywhere, and in light of global trends and thinking about how do we make this process future proof and applicable to the actual data that we all have and are being asked to produce.

>> BERTRAND DE LA CHAPELLE: So I will be quick. I have only 25 final points to make.

(Laughter)

No. More seriously, one, I am very happy to hear a modicum of convergence on the notion of interoperability. That's clearly a word that is moving ahead. Likewise, on the debate regarding independent judicial authorization, it's a very interesting situation where we see the evolution because there clearly is an agreement on the notion that something independent should be there, and the debate now is moving about the difference between oversight or individual validation on case-by-case basis. And I would add that there is a discussion that is very interesting at the moment that says maybe the national law does not oblige this to have it. But in many cases -- that's the case in India, for instance -- the national law apparently allows a judicial authorization if the government wants to do it. And there's no problem in using this component to say if it is a transnational request, we apply this existing provision in the law to do this. So this is one of the pieces that we have explored.

Likewise, location of data, there has been a tremendous evolution. We followed this topic for many years. Now the notion that we need some sort of a regime for the cloud that doesn't care, except in some conditions, about the location of the data, is a real evolution. That was not the case three years ago, as we saw with the case of Microsoft.

And finally, the notion of sovereignty, I was saying to someone before this session, we now are in a situation where the exercise of sovereignty is going to be slightly different because extraterritoriality should

not be a taboo as long as it is used with measure -- and there are conditions -- and likewise, there might be conditions on the exercise of sovereignty in the countries, on the territory itself, if in the context of analysis, it has a transborder impact on another country.

So this is a fluid moment, but with we have to avoid some of the very rigid interpretation of the connection between sovereignty and territorial because it is still valid in most cases, but increasingly we want to play more with it. If you want to know more about the policy network, in room 4, just now after this, we have a whole session about the process which we are running, which is the reason why I am quietly moving to be on time on my own panel. But you are kindly invited to join.

>> THIAGO TRAVARES: Thank you very much. We are very strict on time. We passed it five minutes. But I would like to highlight the importance of the principles and highlight that at the national level, the Internet Steering Committee has approved --

>> BERTRAND DE LA CHAPELLE: And you can arrive late.

>> THIAGO TRAVARES: -- thank you, Bertrand -- has approved by consensus in 2009 a set of ten principles for governance and use of Internet in Brazil. Those principles inspired the discussions and shaped the view linked to Internet civil rights law. Four of them are directly related to our session today, and I would like to highlight them as an additional food for our group.

The first one, freedom, privacy, and human rights. The use of the Internet must be driven by the principle of freedom of expression, individual privacy, and the respect for human rights, recognizing them as essential to the preservation of a fair and democratic society.

Principle number 7, known liability of the network. All action taken against illicit activity on the network must be aimed on those directly responsible for such activities and not at the means of access and transport. Always upholding the fundamental principles of freedom, privacy, and respect for human rights.

Principle number 8, functional and stability. The stability and overall functionality of a network must be activated through the adoption of technical measures that are consistent with international standards and encourage the adoption of best practice.

And principle number 10, legal and regulatory environments. The legal and regulatory environments must preserve the dynamics of the Internet as a space for collaboration.

Having said that, I would like to recall one very important quote from Bertrand's keynote speech, which is that we should have an interoperable global cooperation system for investigations that works a little bit like the Internet. Think about a legal system at the national level, and you have a sort of router that plugs into this legal system so that whenever it sends to another country it expects a certain level of criteria, procedures, protocols, et cetera.

As concluding remarks, I would say that such system should be also scalable, fast, neutral, secure, and lawful.

Let's build that trusted system together. Thank you very much.

Contact Information

United Nations
Secretariat of the Internet Governance Forum (IGF)

Villa Le Bocage
Palais des Nations,
CH-1211 Geneva 10
Switzerland

igf [at] un [dot] org
+41 (0) 229 173 678