

ROUGHLY EDITED COPY

EURODIG 2010
MADRID, SPAIN
29 APRIL 2010
14:30

WORKSHOP 1
CROSS-BORDER CYBERCRIME JURISDICTION
UNDER CLOUD COMPUTING

Services provided by:

Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.captionfirst.com

This text is being provided in a rough draft format.
Communication Access Realtime Translation (CART) is provided in
order to facilitate communication accessibility and may not be a
totally verbatim record of the proceedings.

>> CRISTOS VELASCO: Well, let's wait five more minutes
before all the people come here from lunch.

Let's get started. First of all, good afternoon,
ladies and gentlemen, guest participants, friends and
colleagues. I see a lot of well-known faces from
previous IGFs, and previous EuroDIGs, and that makes me
glad that you all made it to this session.

First of all, the Council on Computing has evolved in
the last years. There is a better understanding of the
benefits for companies, government entities and general
people. However, security is still a major concern under
this current trend and cloud computing continues to raise
a number of technical and regulatory concerns.

Cybercrime is on the rise and cyber criminals continue
to exploit security and their activities will also be
moving to the cloud. Internet is transnational by
nature, but enforcement of criminal law is still confined
to national boundaries. And most criminal laws favor the

principles of territoriality and nationality under public international law.

Cloud computing and cybercrime raises other concerns. For instance, in the field of data retention. This year there was an important decision from the German Federal Constitutional Tribunal, Bundesverfassungsgericht, that declare unconstitutional the data retention legislation, which requires telephone companies and Internet service providers of that country the storage and preservation of data for a period of six months. This Resolution is a clear sign of the importance of protecting personal information as a fundamental right at the European national level. However, the decision of the Bundesverfassungsgericht might represent a major obstacle to law enforcement authorities since they largely depend on the storage and retention of data for conducting criminal investigations in realtime and the possible identification of crime and terrorism-related activities.

During the Octopus 2010 Conference on Cooperation against cybercrime held last month in Strasbourg, there was consensus on the application of full implementation of existing Council of Europe instruments like the convention on cybercrime, the Convention on the protection of children against sexual exploitation and abuse, and Convention 108 for the protection of individuals with regard to automatic processing of personal data. There was consensus as to the improvement of international cooperation as a prevention against cybercrime. There was a strong emphasis on the need to develop additional international standards for law enforcement access to data stored abroad and to information stored in the clouds. Establish transparent and effective procedures, rules and best practices for cooperation between cloud providers and law enforcement agencies. And establish adequate guidance to service and cloud providers with regard to the privacy of information and procedural safeguards when carrying out criminal investigations in the cloud.

Another major concern of cybercrime related investigations are the possible conflicts in the application of national laws, regulations, Conventions, and the different European framework decisions that in practice may likely create problems and confusion to judges and magistrates that sit on cybercrime cases that affect their national or internationals or entities located inside or outside of their territory.

This workshop has a three-fold objective. First, to

discuss technical and European legal frameworks, policy and industry initiatives, and best practices surrounding aspects of jurisdiction in the area of cybercrime, with a special emphasis in the cloud computing.

Second, to raise awareness on importance of the intersection between cybercrime, Internet jurisdiction, and cloud computing as an emerging Internet governance aspect at the European level.

Third, to identify and put forward possible solutions for future policies in this area.

For this session, we have gathered an excellent panel of experts coming from different sectors that will seek to illustrate the current problems and the challenges in cloud computing and cybercrime jurisdictions.

First I'd like to introduce my co-moderator, Ioana Bogdana Albani. She is the chief prosecutor and head of the cybercrime unit at the prosecutor's office attached to the high court of Cassation and justice of Romania. And she has been very active in providing training to the law officials of Romania.

Our rapporteur is Estelle De Marco. She is a member of the European cybercrime training and education group, and participates in the creation of the French cybercrime center of excellence for training and research and education.

Next on my left is Cornelia Kutterer. She is a senior policy manager for Microsoft EMEA and she is responsible for technology, child online safety, security and consumer policies. And she is working with a number of trade associations and is chairing the Digital Europe as well as the TechAmerica privacy and security working group. She worked as a senior legal advisor and head of the legal department at the European Consumer Organization.

Then we have Francisco Monserrat. He is a member of IRIS-CERT since 1999, a spanish academic and research network that provides communication services to the scientific community and national universities, which is currently managed by the public corporate entity Red.Es. He was a former member of the board of directors of the Forum of Incident Response and Security teams and is an active member at other national incident and security response teams.

Then we have Michael Rotert, he is the vice president of EuroISPA, the organization that represents the Europe Internet service provider industry and one of the world's largest organizations of ISPs. He established the first

connection from Germany to the Internet after setting up one of the first ISPs in Germany while working at the University of Karlsruhe in the early 80s. He was part of the German delegation to the Group 8 cybercrime summit. He became the president of the German ISP association, ECO, in 2000 and was elected EuroISPA president from 2003 to 2008.

Then we have Alexander Seger, who has been with the Council of Europe since 1999. Currently the head of the economic crime division and responsible for the Council of Europe's cooperation programs against cybercrime, corruption, money laundering, and trafficking in human beings. From '89 to '98, he was with what is now the UN office on drug and crime, in Vienna, Austria, Laos and Pakistan and a consultant for the German Technical Cooperation GTZ in drug control matters.

And then at the end we have Professor Henrik Kaspersen, who is the Director of The Computer Law Institute of the Vrije Universiteit of Amsterdam since 1991, in charge of conducting scientific research to several topics and aspects of computer law. He was involved in the preparation of the Dutch Computer Crime Act in 1993. Between 1995 and 2003 he served as the chair of three expert committees of the Council of Europe that worked on cybercrime investigation, the Convention of cybercrime, and the first additional protocol to the Convention concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. He has been active within the Council of Europe in promoting the implementation and accession to the Convention on cybercrime worldwide.

I'd like to introduce Roxanna, who will give us the remote participation.

I'd like to talk about the logistics of this panel, which is simple. We have come up with a list of 8 questions, which each panelist is to answer in a brief manner, from 3 to 4 minutes, and then we will pass those questions on to you and then we will start the dialog.

So welcome.

>> IOANA BOGDANA ALBANI: Good afternoon. There is a list of questions that will be handled by Cristos. But there is another Question starting with the two practical cases. I've been a prosecutor for two or three years and I've been dealing with cybercrime for 9 years. So I'm somehow equated with the problem and I've seen all the time that cybercrime is concerning people, but also the law enforcement.

I don't know if in the room there are some other agents, prosecutors, Judges, maybe, or simply police officers, but for sure I can tell you when I became a prosecutor, I took an oath to protect and to serve the citizens, to protect the law, to enforce the law, if necessary, and to bring offenders to justice. So, the prosecutor is from the bright side of the road, so is the good Guy.

I raise you the Question of what should I do? And the case is like this. I have an informant. He is working for me. He is collecting information for my case. I have jurisdiction to investigate the case. So one day he overheard a conversation he was not supposed to hear, and he managed to find some credentials from an e-mail account or Web mail, a web-based e-mail account, a Google account, let's say. And he is passing this information to me.

The question is, what should I do with this information? Am I able to search that space, that means the space that my offender is holding in the Google space, or not? The second case is like this: I'm an online investigator and I started the case in my country, in Romania. I'm chasing a child pornography offender. He is moving his forum to another country, to another server, and I'm pursuing him. Am I doing good or wrong? What should I do if I will find a large quantity of information situated in a storage? I can be very sure which jurisdiction it is. Those are the two questions. What should I do? And I hope that during this conversation today I'll get some answers.

>> CRISTOS VELASCO: First of all, before we start, it would be important to really know how does the cross-border investigation work in practice? What do Internet service providers do in order to get access to that information in order to trace criminals, and also law enforcement. So if you could sort of like pretty much explain so that we could illustrate to this audience and then start like on the following questions.

>> IOANA BOGDANA ALBANI: Okay. Based on the legislation that we have now, based on the Romanian law, it was drafted after the Budapest Convention, allowed us to conduct searches and investigate cross-border, meaning with the help of the mutual legal assistance and of course with other instruments we have in this respect. As a prosecutor, when I'm starting an investigation, I'm trying to find the most relevant evidence that I can find. At first, the Internet, it's something which is

not so clear for everybody. And starting to gather evidence over the Internet, it's putting you in a position very awkward. You don't know where is that evidence. So, at some point you don't know if you are crossing a border or not.

And this will be the first thing to understand and to settle in that investigation, to have your jurisdiction very well set. You also have to observe some principles.

We have substantive law. But for the proposal law, it's for sure a principle of materiality. There are some cases where you can't cross the border and do investigation in another country until the other country is giving him the permission to do so, maybe in a joint investigation or some other sort of cooperation. So, there are some tools, but in my opinion they are not up to date. And for the Internet maybe it's good to have, in the future, an agreement to share the Internet as the offenders are doing, to share the jurisdiction, a sort of sharing of the jurisdiction between the states. And if we are talking about the clouds, for sure it will be needed another agreement.

My opinion.

>> CRISTOS VELASCO: That's a very important legal point and that leads me to the next question. Perhaps professor Henrik Kastensen could answer this. What about Article 22? What about the provisions provided in Article 22 with regards to the jurisdiction? It provides jurisdiction on territoriality, nationality, and the principle of universality. Could you please, professor Henrik Kastensen, illustrate a bit more about the Article 22 and do you believe this provision would be good enough to sort of like assert jurisdiction for cybercrime criminal cases across Europe?

>> HENRIK KASPERSEN: I'm on?

>> CRISTOS VELASCO: Yes.

>> HENRIK KASPERSEN: Thank you for your question, Article 22 that you're referring to is related to substantive law. There is a difference between the extra territorial scope of domestic law in the substantive field and possibly extra territorial actions on the basis of procedural law.

I don't know any principles recognized, if I may elaborate the second topic first, under international public law, jurisdiction principles that would allow extra territorial investigative actions. So, in my opinion, we need, in order to make that possible, we need international agreements, like we have. For instance, in

Europe we have joint police teams. We have regulation of pursuit. We have sometimes occasionally cooperation models between law enforcement of different countries. But that is all on the basis that law enforcement is reigning its own territory.

When we look to more modern needs, like those established by my colleague, that sometimes we have to follow the data and sometimes we don't know exactly, when we have an investigative action, where we are. I would say that that situation definitely requires new international agreements. Because without international agreements, we could come to the situation that we are indeed interfering with the sovereignty of another state.

If you wish me to elaborate on that further, I might do that. But maybe I could stick with it for a while at this point, at this moment in time.

>> CRISTOS VELASCO: Thank you very much. Now I would like to hear a little bit more about the technical aspects. What are Internet service providers doing with regard to cooperation with law enforcement? Perhaps Professor Rotert could illustrate on this.

>> MICHAEL ROTERT: Well, at least I can try to. If you look at before it was called, (Temporary loss of audio) and now it's called cloud computing. There is one difference. With cloud computing, it's more extensive, the storage of data in places, the user just -- (temporary loss of audio)

I mean, this has been a problem for law enforcement ever since. But with the visibility and marketshare of cloud computing, it's just coming back into the fold with even higher complexities.

Most of the questions I could find in here are from the view out of law enforcement. So, this might vary a little bit, because it should be a dialog between all of the stakeholders and they should all treat it equal, because we have a lot of, from the service provider view, a lot of questions as well. Too often ISPs are just expected to Judge whether the conduct or content of users are illegal, but they are definitely not the appropriate people to do so.

ISPs feed as well legal certainty for information, duties, and handling requests, which they don't have in a couple jurisdictions especially when they deal with data crossing borders. And at the moment, there is a huge discussion going on with ISPs, as intermediary, and they are really in a difficult position and have to face post duties with risk to illegal content. They are obliged in

one way for the data protection and privacy rights, and on the other hand they are requested to support law enforcement, which sometimes gives them jurisdiction conflicts.

But let me come back to the data retention directive you mentioned at the beginning. And the German court. When the data -- the data retention tool came out it was for only terrorism data only, which was to exchange data between the countries, and to review the direction after a while. Of course, any access was restricted to terrorism only. These goals have been missed I would say and we're -- and now we have a totally different implementation in the various countries, and this is what the constitutional court said in Germany. It declared the German implementation as not valid, and it explicitly said that data retention as such is a valid instrument, but they should look -- the -- the government should go again looking at new laws which benefit to the constitution.

And I have to admit that in all discussions, and I was an expert at the constitutional court, and all discussions, I couldn't hear real cases which couldn't have been resolved with existing data or with data you could get in -- who would be made available through fast freeze mechanisms.

That means most of the data were not -- did not come out at least in -- this is true for Germany -- did not come out of the retained data from the data retention.

And there is a lot of things which are still coming up in the future which have to be looked at. And not only the old questions dealing with the problems from cross-border data and tracking data and the criminals. Imagine that IP version 6 leads to IP addresses for everybody. They may immediately become personal data in a couple of countries. And then the whole discussion starts again, how do we handle this if in some country personal data are treated differently due to data protection laws in these countries? And everything is starting over.

But even if you have, I would say, maybe Patrick knows, Patrick Fraström who is sitting in the audience, knows better data. But I would say that if we have IP version 6 in some years, there will be still five or six or seven years both systems run in parallel. So you will have both problems. The one dealing with the new systems and the one still not resolved dealing with the old system.

And this shows in principle that it's even more -- that's why I said at the beginning, the multi-stakeholder

approach is even more necessary with equal partners on both sides.

There are a lot of initiatives dealing with the subject. We have the guidelines for cooperation between law enforcement and service providers against cybercrime from the Council of Europe, and according to the recommendations from the European Commission, there are human rights guidelines for Internet Service Providers from the Council of Europe, which are currently worked upon to see on how they could be implemented in the Internet Service Provider industry.

We have of course the Cybercrime Convention. We are currently dealing with notice and takedown procedures instead of blocking illegal content, especially child pornography. Notice and takedown in combination with fast freeze to preserve the evidence, and using hot lines for reporting illegal content or conduct. And according to the cloud, because everything was set under the cloud computing mechanism, my association has an initiative started together with friends in France, the so-called Euro cloud. It's some kind of best practice. And those might be the ones, if you want to deal with cloud mechanisms only, to talk to. It's a European initiative with associations in the various countries, but it has just started since one or two months. Thank you.

>> CRISTOS VELASCO: Thank you very much. Professor Michael Rotert, is there any questions from the audience that you would like to address to the speakers, or just if you have something to say before I pass it to Professor Henrik Kastensen? Professor Henrik Kastensen, please.

>> HENRIK KASPERSEN: Just in support of your -- the language about the German position of the constitutional court. Indeed, the court didn't say that the whole directive was in violation of the German constitution. It just said that it's not. But the way it was implemented in German law, it was a problem.

I happened to be able to read the decision of the Romanian constitutional court. Maybe you can elaborate on it because you are from Romania. But in that decision, it was said that the directive as such was violating Romanian constitution, and then you have a serious problem if that is true.

There is also a portion decision of the constitution of the court of Bulgaria, which I haven't read for problems of language, but I could imagine that they have a similar idea about incompatibility with their constitution as in

Romania. But I'd be happy to refer that to you.

But I just wanted to say that in the Netherlands, where I'm from, the parliament adopted the implementing laws as a directive, but instructed the minister to go back to Brussels to renegotiate the data retention directive, because parliament found it absolutely a disproportionate measure. Just for your information, what you'd like to do with it, or not. But maybe you can help us with Romania.

>> IOANA BOGDANA ALBANI: Yes. Our law was declared unconstitutional last year in October. Well, not the directive itself was declared unconstitutional to our constitution, but the principle of retaining the data was declared unconstitutional, because it's infringing the freedom of movement, the privacy of the correspondence, the privacy, but first the freedom of movement. Because a person might be reluctant to move to a place, from a place to another, having the phone, let's say, open. Because the cells from the places you are going to, they will be retained in the ISP system -- yes, the service provider system.

So this was the most important thing that our court said. Infringing the freedom of movement and the right of the privacy and the correspondence as well.

For the correspondence, I don't agree, because what was supposed to be retained were only data related to the communication, not the communication itself, or the constitution is protecting the content itself of a correspondence, not the outside, let's say, the network data from what time to what time, or from one place to another.

But another thing I would just like to say, this directive came from the first pillar, not from the third pillar, which means it's not -- it's not coming from the Homeland Internal Affairs Commission. It was supposed to help the law enforcement, not to make somebody as a suspect. This was not the intention.

And the information, most of the information retained under the directive were also retained under other law, domestic law. And they were protected as well by the directive for the data protection and other domestic law.

There were commercial information that should be retained. Maybe in some countries the retention was extended to some other information. But I feel that it was a good intention at first that became at some point maybe misunderstood.

>> CRISTOS VELASCO: Thanks. I'm very interested to

know what Spain is doing with regards to that. Like the 24 by 7 contact point of Red.Es. What is it doing to address this issue of jurisdiction under cloud computing?

Perhaps, Francisco, if you could tell us a bit.

>> FRANCISCO MONSERRAT: In Spain there are some -- there is some kind of different thing. It's not on agreement 11, but from the police and ISP, we have joined together. Next week we have a meeting here at Telefonica of all of the national ISPs, plus law enforcement, to talk about how to coordinate, how to get the data, most of the time what is happening. Because at the national level, we are talking about the 24/7 telephone line. If we talk about the amount of cybercrime, (inaudible) we will get 200 or 300 complaints of people every day. So this kind of 24 by 7 is not (inaudible). We are dealing with all of the problems that were commented on before, the personal data. In Spain, most of the laws say that IP is personal data. So it's difficult to exchange information between the feds and the ISP or the feds and the end-user, saying okay, your machine has been compromised or your bank account has been stolen. Sometimes there is control of this information.

You cannot submit to anyplace. So it's very difficult. But in Spain, for the government, for the end-user, trying to talk about the theft of the government, and the last few months it was allowed to enforce a lot of security improvements in the administration.

>> CRISTOS VELASCO: Thank you. I'm also interested to know about what the industry is doing with regards to cooperation with Internet Service Providers. Perhaps Cornelia has something to say.

>> CORNELIA KUTTERER: Thank you. Let me turn it around first and then come back with your question here.

First of all, the discussion here is extremely timely. We have had already first discussion at the Octopus Conference with a very clear call on how to enhance this discussion around law enforcement data access, privacy in that respect, and data retention.

And I see this discussion, this panel in particular, as a continuation. Timely why? Because within the context of the European Union, we have a new commission. We have a starting digital agenda, which deals with network and information security, mainly resilience questions, in order to enhance business. And we do have a Stockholm program which will develop a security internal strategy for the European Union, including law enforcement mechanisms. But also, privacy in law enforcement data

access requests.

This commission will also look anew at the data retention directive. There will be an implementation report, which is supposed to be published on the 15th of September, and Commissioner Manstom in her hearing back in Genoa that the directive will see the admission. This is sort of a triangle which needs to be looked at in a coherent way.

From a business perspective, let me point to, first and foremost, cloud computing enables the digital internal market to grow. It is the scalability and economies of cloud computing which will help the economy in the European digital internal market to regain and recover. And it is thus really important not to forget about that.

This means that we need within that internal market, and there is obviously the global aspects, which come on top of that, but it is like an infrastructure in itself to have a clear legal regulated environment for business to be enabled to enhance in these requirements.

Let me give just an example of the data retention directive and a service which has already been mentioned, a web-based e-mail account. In principle, I would say that most people in the drafting of the directive did not necessarily see Web mail based services being part of the directive. However, in the implementation of the directive, that has been becoming more questionable than in the directive itself.

Also, other new services, which also it's a very recent directive, have, in the meantime, been developed. It's something where there is a huge amount of legal uncertainty for businesses and they really need to go basically to each telecom communication regulator and discuss whether a certain service or not will be falling under the discussion. And that is not mainly about the question of whether because it is an electronic communication service, hence under the law you need to certify, but it is what kind of data you need to keep and where. And the -- that's where it's one of the unclear things is the jurisdiction around data retention. And at the end of the day, also, the retention period, because these questions are obviously very interlinked, and it poses considerable uncertainty for business in terms of legal compliance with other rules, such as data protection rules, if you're stuck in between two countries which have different retention periods.

It is -- I would like to come back also, just for the -
- for the picture of having different things working

together. One, we have the Cybercrime Convention. And this week the European forum ministers have in their council minister meeting announced that they will create a cybercrime agency, which is I think a step forward. They will do an impact assessment whether this is something feasible. Alejandro is waving. Sorry to be unprecise here.

But, it would be -- it would certainly be a step in the right direction, maybe a very slow step. We will see -- and that's part of this is really the underlying resilience of security, a new regulation for ANISA, and those two agencies in the future, if ever this agency will come into play, will need to work very closely together.

Now, to come back to your question on how we deal with that, for Microsoft it is very important that there is, as far as we can, a customer transparency. And in many occasions we would, if we can, abiding to the rule of law in a given country, if we can we would refer to the data controller if we are not. In many of the cloud services that is not necessarily the case. If you think about things such as infrastructure, application as a service and more in terms of software as a service, that might not be the case.

>> CRISTOS VELASCO: (Spanish translation, not English)

Talking about the Cybercrime Convention, I would like to ask Alexander Seger with regards to Article 32 about transborder searches. This Article really allows transborder searches when the data actually -- well, open source available, open on the Internet, or waiting for consent. So what are most you're countries doing implementing this specific provision; and if you could, provide some practical case scenarios.

>> ALEXANDER SEGER: Thank you. In trying during the past two years to focus the questions, to define the questions more clearly that we need to address, I get the impression from the discussions they are broadening again. There are all sorts of issues. Let's try to identify the key questions of IT that we need to address, at least from the perspective where we need to deal with cybercrime and access to data. Because that's it. Data retention, content related issues, responsibilities of Internet Service Providers, they are all separate issues, but I'm not sure that that is specific to this debate here. Under a normal law enforcement situation, law enforcement needs to trace the origin, they need to identify offenders, bring them to justice. If you have

an oath on that, that you would do that, your honor, and for law enforcement it's access to traffic data, content data, or other stored computer data and subscriber information, et cetera.

And in the normal situation, traditionally, computers, here on his laptop, and if I now as a law enforcement officer I want access to that, I go to a Judge or whatever and I get a warrant and I can search this particular computer.

There are safeguards in most countries, so that I cannot just go do that without asking for anybody's permission, and so on. And if there is an Internet incident, then I have to ask for an interlocutory letter or engage in police cooperation in order to freeze data in another country, et cetera, et cetera.

The problem with cloud computing is where is the computer system that we are searching? Where is the data and how can we get access to that? I would like to point out four scenarios in that. For two of them we have solutions identified, and for two of them we have to find solutions. We have to identify solutions and maybe even develop a new instrument or some standards.

The first solution is the cloud data is on a server in my own country. Stored in a cloud server in Romania for a law enforcement officer. You would apply the provisions of your law with the safeguards and whatever. The sort of provisions as specified in chapter 202 of the Budapest Convention under the proposal law issues, under your procedural code, right? That's easy.

If the cloud data is hosted abroad, you can do then -- you can access data with the assistance of the foreign law enforcement official. If you want to have the data frozen, you as the Contact point from Romania, you contact the French, US, French, whatever, contact point and have the data frozen. And you send an interlocutory and sooner or later you get the data.

There are also the 24/7 contact points to permit the immediate freezing of data in another country to give you the time to go through the normal procedures.

So for this tool we have -- and this is what you would have defined in chapter 3 of the Budapest conventions. The solutions are there. They could be applied more effectively, but the solutions for these two scenarios are there.

But then we have two scenarios where we have problems. And one is related to Article 32B of the Budapest Convention. One scenario is law enforcement wants to

directly access data that is in another country, or possibly in another country. And there you can use Article 32B, with consent.

Lawful consent -- voluntary and lawful consent. So you are now a Romanian here in Spain. I'm a police officer. I ask you to cooperate with me. You give me lawfully -- I'm not torturing you, I'm not deceiving you -- you give me lawfully access to a computer in Romania and I can access the computer there and download them and use them in a criminal proceeding. That is in Article 32.

In the late 1990s, which was discussed -- this was agreed first in principle by the G8, it was approved in the Russian Federation and now the Russian Federation has the biggest problem with this particular provision. So that's only one small opening in the Budapest Convention under that under 32B.

But there are other things in the Convention that are interesting. There is an Article, 19.2, which is about extending the search. So our prosecutor here gets the authority to search this particular computer, but this computer is connected to another system. She may then have the authority to extend the search to the collective system. The question is if the collected system is a Google server somewhere else, and so all sorts of questions will come up there. If it's within your country, it's clear. If you cross borders, it gets less clear. And in particular if you don't know whether the Google service actually is in your country or where it is -- and Google may change from day-to-day. Today it may be in one country, the next day it may be stored on a server in another jurisdiction -- and then the question is if data collected in this way through direct access to a computer system in another country, they can use it in a criminal proceeding, or if it's just for information. There are many questions related to that. If you realize that indeed the data is in another country, do you have to inform the law enforcement authorities of the other country? Do you have to send an interlocutory, et cetera? These are questions to be addressed when you talk about direct access by law enforcement to data stored in another jurisdiction.

Then there is a fourth scenario, where we have -- well, the service providers in Europe have encountered certain difficulties with access to data with the cooperation of ISPs or cloud service providers. A scenario, you may have a situation wherein one country, a Judge or prosecutor wants data to be intercepted between two

nationals of that country, but using web-based mail service, Hotmail or e-mail or whatever, can the Judge force the ISP or the cloud provider, the service provider, in that country to interpret the data if de facto this involves data stored on foreign servers? It's a big question. In one or two countries, they force them, actually. So that sort of scenario.

Or can you compel a service provider in your own country to give data that has a legal representation in your own country to give data stored in another country, and all of this without involving the authorities of the country where the data is, or is it where this legal person is based?

So these two scenarios, direct access by law enforcement to data abroad or access to data with the help of service providers. These are not properly regulated and this creates lots of uncertainties for service providers.

And the other question is do we need international agreements on that? I would like to phrase in addition to these four scenarios, two of which we have solutions, the issue of proposal safeguards. If I'm in my own country, and law enforcement wants to access my data in my own country, I have certain legal guarantees there. I'm protected by the constitution, by the traditional systems, by the judicial systems, and whatnot. But what if my data is stored abroad on a server? Do I have the same level of protection to my data abroad as if I have my data on the Hotmail or Goggle mail account? Do I have the same level of protection? And there are in some countries the understanding that the data on your computer is well protected. If it's traveling from one computer to the next, it's less protected. But if it's with a third computer, meaning a cloud server, there is no expectation of privacy. You don't have the safeguards where a Judge or prosecutor would have to prove that law enforcement gets access to that. So the question really is also here, the issue of proposal safeguards in a cloud-computing environment.

>> CRISTOS VELASCO: Thank you very much for illustrating those case scenarios. It's important to approach it here by regulation but also by providing training, law enforcement officials, ICP, because it's the only way to go. Those case scenarios are very important. But if we don't train all of those stakeholder, then it would be like impossible.

There are a couple questions from the audience. So, I

would like to give the floor to Katitsa, please.

>> AUDIENCE: Hello? Okay. Thank you. My name is Mrs. Rodriguez. I'm with the Electronic Frontier Foundation. We work to protect the rights on the Internet.

I would like to make a comment and a question and following the panel discussion.

When a consumer accesses a cloud computing service, for example, Google Docs or some of the service providers, these companies record information such as our account activity, the number of log-ins, actions taken, the clicks we make, the URLs, and other log-in information. For instance, the URL, the browser, the IP address, the date and time of access, the cookie ID. Collecting all of this information has raised privacy concerns. But even farther, when this data is linked to other cloud computing activity, it tends to reveal much more information for a consumer. For example, IP addresses and log-in times could be used to determine when and where a user was and who has used that same computer if she or he logged into a cloud computing service away from home.

This has been recently published, this Article, by ACLU recently, on paper on cloud computing.

So my question is: Does the distinction between in transit and stored really work in that world?

Furthermore, cloud computing usage has grown. It's true that they have been in existence for several years, but recently there is like everybody is using it. So this means that there are more data stored outside our control. More transactions with that data means more records of what we do, when, how, and how often. This also means more ordinary users in the cloud means more personal information.

And this new service also is storing very sensitive information, like health records. I would like to know which is the legal framework in Europe or case law regarding the access to e-mail messages stored in a Web mail account or text message stored with a service provider.

If these are protected, the information stored at home or on a device in our possession, does law enforcement need a warrant to access the data stored in the cloud? Furthermore, what happens when the provider accesses the server in some manner, such as to check for grammatical mistakes, or other general target based on the content, provided these are the consumer positions, is this

secondary use of the information? This profiling, will have the same level of protection and information stored in my computer? Thank you.

>> CRISTOS VELASCO: So who would like to take any of the questions that she just mentioned? It can be only one.

>> IOANA BOGDANA ALBANI: I'll answer only one. I have a lot of concerns, every day, when I'm using my credit card, because this information, it's kept for a long time in my record. I also have concerns when I'm filmed by a camera situated at the ATM or another, I don't know, department store for surveillance purposes. I have a lot of concerns in my everyday life and so I have over the Internet, where my information may be kept for some reason or maybe is not protected.

In Romania, personal data is well protected. And you can access information contained -- content of an e-mail account only under a court order. In our system it's called access. In other systems you may call it a search warrant. It doesn't matter where it's situated. It's important to have the search warrant or the authorization for access.

So, from the beginning, you have to have an investigation. You have to demonstrate that you have very important -- that you have a ground to ask for this search warrant. The person is protected and you can use only information which is related to the case. You cannot use any other information that you're gathering from there. In fact, it's forbidden to use personal information for other purposes than the investigation. And this will be -- I can assure you, in Romania, these things are very specific and respected by the law enforcement. Because it will be an infringement of the fundamental rights and we are liable in front of the court if we are not conducting The search properly. That will be my answer.

>> MICHAEL ROTERT: There are more than only Google as search engines. I mean, you can switch to other search engines if you would like and if you don't trust Google. But anyway, there is, in terms of cloud computing, as I said before, there are initiatives with Euro cloud, working on this subject and trying to get some of those companies to have certain guarantees or SLAs or quality labels, however you call it, to give more transparency to the end-user and make the business out of these things. This is one of the topics I have seen from the Euro cloud initiative.

Web mail concerns, for my knowledge, Web mail normally is encrypted. And even for interception, you need the special support from the ISP to get it in a normal readable format from the Web mail as such.

>> CRISTOS VELASCO: Professor Henrik Kastensen?

>> HENRIK KASPERSEN: I'd like briefly to add (Lost English audio)

Under Google or you can choose another service. First we have to realize what we are doing in the first place. The second place is we could use instruments like encryption that provides --

(Lost English audio) --

The third thing is I notice that when we talked about the cybercrime as a global instrument, that other countries, they also had interest for the data protection Convention, because they saw there was a direct relation between the criminal things and the criminal procedural things and data protection.

One thing Europe should do is make more pressure on our friends in the United States to look to our models, which have proven to be more valuable for the individual citizens than the system they apply.

But, most of all, I think within criminal procedural law, the criminal proceedings, we have adequate safeguards that prevent law enforcement to abuse the data. We have to adhere to the court in those cases if abuse has been reported about it. Then it is done.

So, it's true, we have more personal data on the Internet, but that's of course understandable. We have more societal activity on the Internet, so the interest of law enforcement for those data we can understand, because we have to deal with abuse, with criminal acts on the Internet, more than they have let's say a couple years ago, so it's a logical development. But we should not forget to look every time when we create new powers, to look at safeguards and guarantees. And to this extent we are only happy with some constitutional core decisions that we have seen.

For instance, in Germany, I'm referring to the decision of 2008 where we talked about online searches. Quite clearly what you have in your computer system, that is private. That belongs to the -- you have the privacy rights under the German Article 10, if I'm right. That is clear. That is the European decision. Maybe in the United States you have several decisions, but that is a good start. So we must be very much aware that we follow in our case law the developments of the Internet

quite precisely. And I -- well, I'm hopeful and trustful that that happens.

>> CRISTOS VELASCO: Okay. Well, before we pass, we are going to the next question, keep it brief.

>> I'd also like to underline the importance of the ruling of the court from 2008 that confirms the confidentiality and availability of the computer data as a fundamental right. And that was specifically on the individual computer. But through the data retention ruling from a few weeks ago, they actually broadened it to data held by third parties, which is an interesting aspect here, actually. And it's very interesting, also, why they say it. They say that, and I have here the ruling with me, but it's in German, and it talks about -- that even if the data retained is not on content, the type of data, the traffic data and other data that is retained permits to make conclusions on personal preferences, political preferences, social connections, et cetera, et cetera. And therefore intrudes into the very intimate private affairs of people. And therefore -- and even the perception that you are observed, that someone is observing and is watching what you are doing, even that perception will prevent people from fully making use of their fundamental rights.

I think this is an important statement and important here, the 2008 ruling was on the specific computer data, the CIA. But with this, they also broaden it to data held by service providers and thus to third parties, which to come back to Katitsa's question, even data held by cloud providers would have the same level of protection than your personal computer, if you take this sort of interpretation by the constitutional court.

I also believe that we need, to repeat again, we need globally accepted and globally trusted data protection standards. It was here in Madrid last year, no, that there was -- there was a meeting -- we have to come back. But I think it will also be economic pressure on cloud providers to -- and other countries to enact data protection legislation. Because a cloud provider that cannot guarantee data protection will soon be out of business, particularly here in Europe.

>> CORNELIA KUTTERER: I would like to add to that, because she made a very important point. She pointed to two concerns, really, of civil rights organizations, which is the commercial abuse on the one hand and the -- and the Democratic questions, which arise in the context of law enforcement, which are two separate things. And I

think it's important -- that is, indeed, an extension of the right, because it -- that has been at least true in criminal law, as far as I recall from a long time ago. There was, indeed, a difference, if you have that data somewhere else. And to put it into more practical situations, you have, for example, lawyers, confidential data in his premise but he outsources that and it could actually have an impact on how law enforcement could get data.

Or your health data kept somewhere else. So these are detailed questions which probably need to be addressed at one point to get that right.

Now, what is really interesting in the recently published Stockholm program, the initiatives under the Stockholm program is that the commission foresees to put the framework decision for privacy and law enforcement cases, which is a different set of rules, under the same framework as the data protection directive, meaning that the -- the thresholds for privacy in both areas will be the same.

Now, just one last word on Microsoft in that respect. We don't have all solutions to all of the challenges which cloud computing poses. There are a number of areas, threats, security threats, which will actually mitigate when moving to the cloud. And there are others which will have to be at risk management. It will become certainly something which is more important. But already now Microsoft adheres to the data protection directive and there is a sort of -- some of these questions which we're asking are actually answered by the data protection directive.

>> CRISTOS VELASCO: From the floor, if you could introduce yourself.

>> P. Falstrom, Cisco. I need to go back in the discussion about 35 or 40 minutes when you started to talk about the data retention directive. I also disclose that I'm part of the working group, the expert group for the commission that is reviewing the implementation of the directive. And I must say that, unfortunately, at the same time the data retention directive is a good thing to use as an example in this discussion, unfortunately, there are so many problems with the directive, like you pointed out from Microsoft, and because of that so many differences in the implementation of the directive, so I would urge people to be a bit careful when using that as an example. Because it ends up being a lot of discussion on the directive itself, and

how effective that text is.

For example, when you mentioned Web mail, because of course one of the big discussions is whether the Web mail which actually consists of two different communication parts, you have the Web surfing, which is the access to the Web site with the Web browser, which is a normal Web surfing activity. And then you have the back end, which is sort of the e-mail messaging activity. And the question is whether one of them or both is actually covered under the directive.

And that's actually one of the things that I personally have written I don't know how many pages on. So I'm happy to talk with anyone in here that would like to hear more about that and my personal opinion.

The other thing I would like to mention that I think we have been missing is that one of the big problems is with data retention and also responsibilities is actually who is responsible for what. And I think that is something that we should talk more about.

We would take an example of something having to do with blocking. There is a big difference whether law enforcement agencies or private entities have the responsibility of making a decision of whether something is to be blocked or not. And I think what people should be a little bit nervous about is that it might be a sliding -- that we might -- we might be on a sliding path towards having responsibility in private industry, nonlaw enforcement agencies, to be responsible for identifying what is illegal and not. And the question there is of course someone that is doing the blocking is often private industry, but the question is whether the same entity that is doing the blocking is also -- is also the one that has to make the actual decision of what is to be blocked.

This I think, in turn, has to do with the fact that only 30 years ago we only had one Telco in each country, but very often it was easy for the law enforcement agencies to talk with the Telco, get the data they wanted. It was easy with the regulator, if it was separate from the questioner, it was often the same organization, to make sure that it's done in the proper way. Now we have competition. We have multiple players. We have competing players. And law enforcement agencies because of that had to work in different ways. So training, and we need to talk more about who has the responsibility for what. Thank you.

>> CRISTOS VELASCO: Thank you very much. This is also

very important too, the fact that every participant should have a responsibility. And sometimes the responsibilities are not really clear, so we should really draw the line. And this is -- thanks for making this important linkage.

Well, the other question, I mean, we're almost about to finish. We have around 8, 10 minutes, so what are your thoughts, opinions, regarding the creation of a European system designed to attack computer abuse as well as to identify, collect and preserve electronic evidence and identity of criminals? Do you see this as a viable solution to counter cybercrimes and other forms of transnational crimes, such as child pornography and terrorism?

Who would like to start?

>> IOANA BOGDANA ALBANI: Okay. I'll start by saying that a sort of mechanism, a platform for detecting, not detecting, for reporting illegal conduct or maybe illegal content, it's under construction within the Europol. They are conducting this project, European project, and in my opinion if it will be done it will help a lot of law enforcement at least to share the information and to report on unlawful behavior over the Internet.

I really don't know if we can have really a European prosecutor, really a European prosecutor, fully empowered to investigate all over the European Union, let's say, countries. It's something to think about in the future and that's why I doubt that we might have a European system designated to detect. Because to detect criminal behavior, to discover criminal behavior, it's up to police officers and sometimes for the prosecutors.

So, you need a unified European system. It's something we should think about.

When thinking about how to retrieve electronic evidence, there are some steps that have been taken to have some standards and there are some trainings conducted as well by Europol to train the police officers, to conduct computer searches, how to retrieve this information from a computer and how to present this information, evidence, digital evidence, in front of the court. And I think in my opinion this was a big step in unifying the procedures.

Because we all have, at least the parties at the Budapest Convention, we have the proposal criminal law, we have the computer search. But it was very important to set some standards, which for the time being are not set yet, but through training and best practices to reach

these standards.

>> CRISTOS VELASCO: Yes. Another question from the floor.

>> AUDIENCE: Thank you. Andreas, I would like to come back to the idea that data in the cloud has -- enjoys the same level of protection as data stored at my computer at home.

If I understand -- if I understood the concept of cloud computing correctly, it basically says that the cloud provider has every freedom to store the data wherever he likes to and to do load balancing between the data centers that he operates.

And if this is the case, then the data that is stored on these -- in this cloud only in this situation enjoys the same level of protection if the data accidentally is under the same jurisdiction as I am.

Otherwise, the jury decision of a foreign country applies, and the effort, the level of protection could be completely different. And I'm never in the position to know which jurisdiction applies to my data because I have no information about where my data is actually stored. I only know my cloud provider and he has a contract with me, but I never know where my data is stored and how it's protected under which legal system.

>> CRISTOS VELASCO: This is a very, very important question from the user perspective. I mean, the user is very -- doesn't really, really know where the data resides, which jurisdiction applies. Perhaps -- I mean, there are some attorneys here that might be familiar with this. But for a general user, that's right. Thank you for making that point.

Yes, please.

>> AUDIENCE: I would just like to give a short comment about there are some providers perhaps from Amazon that in their storage system they have the ability for the user to choose and select very explicitly under what jurisdiction their data should be stored. If it's only to be stored in Ireland under the EU restriction or in the US or the ability to move between them.

I just wanted to point out that there is an ability, even for cloud computers like storage vendors, to have that kind of -- to give that ability for the users to do the selection. So maybe that is also something that should be implemented more.

>> CRISTOS VELASCO: We have another question from the floor.

>> AUDIENCE: Yes. Thank you. I'm Mazuki. I would

like to come back to the last two scenarios presented where law enforcement authorities may encounter problems, even with the Cybercrime Convention.

Article 32B needs consent from the foreigner law enforcement authority to give the data and Alexander Seger said that there are a lot of problems with Russia, probably with other countries.

Now, if the law enforcement authority wants to access data from a private company, from a service provider, ISP or cloud service provider, then what would be the safeguards if they themselves are making sure that in the other country, in the foreign country, the results are the same infraction. There is a bit of harmonization with the Cybercrime Convention, with all of the instruments, but not all infractions are the same in all countries. So, we probably need some safeguards also with this respect.

>> CRISTOS VELASCO: Thank you. We're running out of time. But before -- well, Professor Henrik Kastensen, and after that I would like the panel to keep perhaps in two, three or four sentences, what are the key messages that you're sending to the policymakers, in 3 or 4 phrases, so that we can conclude the panel.

Henrik Kastensen, please.

>> HENRIK KASPERSEN: You're pointing at exactly the key issue in mutual legal assistance. That means that countries can cooperate, but on their own terms. So they have their own legal system. If you want to have data as law enforcement from another country, that request is executed on the basis of the law of that particular country. That means that the safeguards and guarantees under that legal system should remain in place.

And one of the conditions to have mutual legal assistance is that you have the same, similar criminal act that is criminal under both jurisdictions. You will not find cooperation if there is not -- if the sort of conduct is not criminalized in the other country. So we have things in place, international law practice knows how to deal with it.

>> CRISTOS VELASCO: Yes. Another question from the floor before we conclude.

>> AUDIENCE: Yes. My name is Anna. I work for the United Services in Berlin. I'm interested to know if there are already examples where cloud computing is restricted to one country. So, if there a practice already where you just say we want to do cloud computing just within one jurisdiction? That means in one country?

Or if that happens to be their countries who have the same jurisdiction, which is not really likely.

>> CRISTOS VELASCO: Who would like -- Cornelia, please.

>> CORNELIA KUTTERER: This is already happening. And I understand that when the Obama administration negotiated about Google Apps, they insisted that also it was based in the United States.

If I may add, I think I made somebody unhappy. For the geolocation, the data location issues are of extreme importance in some cases. We at Microsoft are looking into the different options that our different services can offer and how we can eventually relocate certain offerings in that respect. But I can't go further, because these are reflections which are rolled out at the moment, which are considerations, which a company like Microsoft does indeed take into account in order to address concerns of data sovereignty. And if you like, I can also have a one-to-one discussion with you on that.

>> CRISTOS VELASCO: Well, I believe there are -- there is one more question.

>> AUDIENCE: My name is Noreena. I'm representing Armenia here. I'm with the education center. And I'm sorry, I missed some part of the workshop, but the question is: When in our country we detect illegal content, in the majority of cases we cannot do nothing with it, because it has originated not from our country.

I'm interested in the framework of cooperation between law enforcement agencies, which were made possible to fight illegal content on the Web in respect to child pornography, et cetera. Thank you.

>> CRISTOS VELASCO: Ioana Bogdana Albani, please?

>> IOANA BOGDANA ALBANI: First of all, there is under the Budapest Convention a network created, 24/7, and it was supposed to be created to help law enforcement to send what is called the preservation letter, the preservation letter for the content, data content, which can be illegal content or network data, IP address, identification, or other information.

For the illegal content, we receive in Romania preservation letters from our countries, and if the provider is in our country, we will freeze the information.

We also have also under the provision of the Budapest Convention to expedite this information to the other party who asked us to preserve that information, in order to make a decision.

Well, it's good that you can send preservation letters, but you can retrieve that information only under a mutual legal assistance request.

So, at some time for the IP identification, it's very old information by the time you will send me the Amlet in order to retrieve that information. But for the content, the preservation letter, it's very good and I can say it can be done very quickly. And if we are talking about child pornography, it will be our law enforcement duty to take down, let's say, that site, which is located in our territory and to take measure and preserve the information.

>> CRISTOS VELASCO: Thank you very much. This has been a very interesting discussion.

So let's just conclude. Let's just wrap up. Please, keep it simple, in three or four phrases, like the key messages that you would like to send from this panel. Cornelia, please?

>> CORNELIA KUTTERER: I think from the business perspective, the most important message would be that we need a coherent data governance that gives the business the necessary security and also the security of their users to develop cloud computing further.

>> HENRIK KASTERSEN: The problems in cloud computing are not exactly new. We had that before. And if that is -- if it really is a problem for law enforcement, because we're talking about the amount of law enforcement, maybe it's a bit early to say that, but we can imagine some things. And of course the Internet has no borders. It's quite clear that we must come to a certain international agreement which allows common activity on the Internet. But also, when we negotiate that facility, we have to negotiate the conditions and safeguards because we cannot do without it.

How precisely it can be done best, I cannot say. When talking about the Cybercrime Convention, we talked about cross-border. And the results were Article 32A and B as stands in the Convention. So my warning is it's extremely complicated, through government regulation. But we have to try again.

The last point, dealing with a European institution, while I have some concerns because cybercrime is, well, so very wide, there are many acts that we could put on the cybercrime. But I'm very happy with the activity of EuroPol, who are collecting MOs, technical things, rather than talking about crime in general, and making statistics about that. So I don't see a common European

agency dealing with cybercrime and investigation. Because that's too broad. And I do think it's necessary to have it.

>> FRANCISCO MONSERRAT: Well, about the last question, it can be economic, thinking that in the last five or ten years we have seen five or six products similar. We have the same problem, how to save information, because in Laos and Europe are different. It's impossible to deport, but in order to detect the activity, it's impossible to marshal to deport the IPs.

So only to focus on that most of the time, we are constrained to a border and to have laws that protect the end user, but that is not fast to resolve the problem.

>> MICHAEL ROTERT: ISPs in general want to have legal certainty and definitely the special sort of access ISPs, as in the media, do not want to deal with content. This is especially for two things I can mention here, because this was discussed.

Terrorism is totally undefined, and Arabs wouldn't see terrorism if another Arab does suicide in Israel with a bomb. So that wouldn't be terrorism for the Arabs, but for the rest of the world.

So this is difficult as well as it is difficult if police goes to an ISP directly to request data, or whatever, it might be the secret service of another country doing espionage. So legal certainty is what the ISP wants to have, and not more.

>> CRISTOS VELASCO: Alexander Seger?

>> ALEXANDER SEGER: Well, I think legal certainty is important also for the protection of rights. But also in order to give clear guidance to law enforcement. What we need is, again, global data protection standards that are applied, they could apply theoretically to Convention 108, if they wanted to.

We need to have safeguards and conditions confirmed also in a cloud environment. It's not there, to come back to one of the questions, it's not there. What I mentioned in Germany, there is a pointing that within Germany, yes, if you gave data to a cloud provider within Germany, it would enjoy normally the same level of protection, but abroad it's not there. It's a big problem. We need guidelines, standards, product protocol from the Budapest Convention to regulate access by law enforcement to data.

We need more of Article 32B, not less. For just our friends in eastern Europe, we need more of that.

And I think to come back to an earlier comment that

Cristos made, we work in a global context. We work with any country. We have been requested to help the south Pacific islands, to help them with cybercrime legislation. I've been asked to provide training in Pakistan and India, in the Asia countries, in Africa and everywhere. We need to provide training to put legislation in place, so that we have legal certainty. We need to provide training to law enforcement on how to apply legislation, how to investigate, keeping in mind also conditions and safeguards. We need to support countries around the world and putting data protection legislation in place.

The opportunities are there. We have masses of requests to help countries around the world.

But we also need financing. Let's come back to that point. There were in Salvador, or at the United Nations crime conference, very difficult questions on cybercrime, controversial, but there was agreement by everybody that we need a global capacity building effort to help countries put the necessary measures in place against cybercrime and through cybercrime and also the protection of fundamental rights.

>> IOANA BOGDANA ALBANI: Definitely I'm -- I can say that the time for discussion of the transborder access has come and an agreement maybe should be reached, I don't know, in a very short time.

I'm also -- I've also sensed that there are a lot of concerns regarding the protection of personal data, or maybe to be protected in advance on law enforcement abuse. I can assure you that our data, it's our data, as I'm a prosecutor, my data, it's also in the cloud when I'm using, let's say, the web-based mail. And I have the same concerns.

So, it's something that we are sharing, I mean me myself as law enforcement and you as end-users of a service. So, it's a problem of understanding and cooperation, and law enforcement always has the need to cooperate with some other people, with a natural person or a legal person, ISPs, and for sure this will be the future of any partnership between the law enforcement and, really, the people who are supposed to protect them.

>> CRISTOS VELASCO: Well, thank you very much for your participation. It was a very, very outstanding panel. Excellent participation. I would also like to thank the floor for their participation. And I would like to remind that this is a very, very important topic that should be provided to -- should be in the agenda of the

IGF for the next meeting and perhaps for following meetings at the international level. Thank you all very much.

(Applause)

(End of session)

This text is being provided in a rough draft format. Communication Access Realtime Translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.
