ICANN70 | Virtual Community Forum – DNS Women's Panel Discussion: Data Protection Laws
Monday, March 22, 2021 – 16:30 to 17:30 EST

TANZANICA KING: Hello, and welcome to the DNS Women's Panel Discussion on Data Protection Laws. Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior.

If you would like to ask your question or make your comment verbally, please raise your hand from the Reaction icon which you can find from the Zoom toolbar. When called upon, you will be permission to unmute your microphone.

Please state your name for the record and speak clearly and at a reasonable pace. Then mute your microphone when you're done speaking. Otherwise, please submit your question or comments in the chatroom.

This session also includes automated real-time transcription. By clicking on the Closed Caption button in the Zoom toolbar, you can view the real-time transcription. The transcript is not official or authoritative.

Interpretation for this session will be included in English, French, and Spanish. To listen to the interpretation, please click on the Interpretation icon in the Zoom toolbar and select the language you will listen to or speak in during this session. This is very important and has been a challenge this morning and this afternoon, so please make sure that you select the language that you want to speak in or listen to.

With that, I will hand the floor over to Vanda. Vanda, go ahead.

VANDA SCARTEZINI: Thank you. Thank you, everybody to join us this time. DNS Woman is finally getting together again after a long time because last year was impossible to do something. We are all getting a surprising times for those. And we discussed this time to start to have panels, at the least, to keep together all the members that we have around the world and to start again to work with them. And this is the first test for us.

So, thank you very much, and let's start. Laura, the floor is yours to ask the first participant. Thank you.

LAURA MARGOLIS: Okay. Hello, everybody. Good morning, good afternoon, and good evening, wherever you are. And welcome to ICANN70 and to our DNS Women's panel on DNS protection which I am sure you will enjoy.

The [resumés] of our panelists will be posted on the chat so we can optimize the time we have. If you have any questions, the people from the staff told us how we should proceed. And if you want to talk, also you can raise your hand and I will be happy to give you the floor.

I want to tell you that we will be switching between English and Spanish, so be aware of that, in order to use the interpretation tool on your screen.

Our first panelist, Mrs. Holly Raiche, will be opening our floor. So, welcome, Holly. The floor is yours.

HOLLY RAICHE: Thank you, Laura. And I will be talking essentially about Australian reform because we're in the middle of actually reforming—no, I'd say improving—our privacy law which I will talk about. Next slide, please.

Okay. The impetus for change was a report by a digital platform. It was done by our competition regulator, the Australian Competition & Consumer Commission. This report was originally initiated by the government to look into the enormous loss of revenue from our media, particularly press, to the digital platforms. And its primary purpose was all about how to support free journalism.

The report is several hundred pages long, covers many subjects because once the ACCC started looking at the issues, they realized the issues raised by the digital platforms were far beyond just the press. And if you look at just the list of headings of the chapters, you'll see it was a much broader report than simply digital platforms and competition.

If you go down the list of topics, you'll see there is one about really just—and I'll point this out here—digital platforms and consumers. And that's where the ACCC had a look at the platforms and privacy. And most of the recommendations, and what I'll be talking about, looks at the issue of privacy in terms of the issues raised by digital platforms. Next slide, please.

There were a range of issues that the ACCC highlighted with privacy and platforms, starting just with the awareness of the privacy issues. And

the collection not only of your personal data, but where you are and what you're doing. How that data is shared. Something I'll be talking a bit more about—consent. Is consent really given and really understood. And the conclusion, not surprisingly, is, well, no.

Information, terms of consent. One of the issues that was highlighted was, well, if people were going to give consent, it's difficult because there's so much information provided. Giving consent is so complex and ambiguous.

Another really important issue was, what do we mean by personal information in the context of digital platforms? And how many people actually see that data set?

So, there are a range of privacy issues, and I obviously don't have time to talk about all of them, but if privacy is of importance to you, please at least read the chapter of the ACCC that deals with privacy. Next slide, please.

One of the issues, the information flow. Now, most of us understand that if we provide information to somebody, they'll keep it. There's an exchange. Usually, there's an exchange of information. There's probably an exchange back of the goods and services we want, and it's what we're used to in a store.

But what the report makes very clear is that there's a whole other set of transactions that is going on here because the party that we're dealing with shares the information not only with the supplier of the products, [but] advertisers. There's a whole set of transactions. It's largely

hidden, not understood. But this is where the transaction happens, and this is where our data that we freely give to one person, we think, actually becomes part of a very big financial chain. Our data is worth money to all those people, and that's why this description is simply inadequate of what happens to our personal data. Next slide, please.

Another issue that the report pointed out was how many people actually read the privacy policies. And if you look at the graph, the answer is not many. This dark purple is the people that never read the privacy policies. You add that. Yes, people rarely …

So, it looks like over half never or rarely read the policy anyway. And the people that read it every time is this tiny little section on top. Interestingly, the 18–24 year olds are the ones who mostly or always read privacy statements, and they're only 10%. Next slide, please.

Consent. What did I say about the complexity of giving consent? This is a chart that was drawn up—it's in a part of the appendices of the report—to show why people, in the end, put their hands up and just say, "Yes." Because if you want to read a policy, you start with a bit about your Google account, a welcome to it, and, "By the way, link on our privacy policy."

So, you do and suddenly you find yourself reading a whole bunch of stuff that you don't have time to read. And if you want to know about what happens in the online tracking, what happens to your data. And if you're really interested, you're going to be there for half an hour. And none of us are going to do that, are we? What we're going to do is exactly what Google wants us to do. And it's not just Google.

We're going to read these statements. We might stupidly pick to choose this bit about the privacy policy and go, "I don't have time." So, we're going to go down, "Yes, okay. Of course, I consent." And by the way, I have to agree because if I don't agree, I'm not going to get the product anyway. And so, this chain is why people don't read the policy. Or if they do, they only skim it. We've kind of been trained not to read it, not to understand it. Simply to consent because we don't have the time. We don't have the energy. And we're not going to get the products anyway.

So, those are sort of the three main issues that I highlight in terms of privacy: what it means, whether we care, and whether we're actually taught not to care. Next slide, please.

The key findings are not going to surprise anybody. In Australia, we do have privacy legislation. We've had it since 1988. Originally, it just covered governmental instrumentalities. But in the past several years, it has been extended to the private sector, particularly for credit reporting.

The findings of the ACCC were that if you have strong privacy protections that actually tell people and empowers them, that it would be very useful in promoting not only competition and innovation, but the welfare of the individual. In other words, there's a win-win here if privacy protections are there and strong.

And finally, they had a look at our regulatory framework. Now, our framework was modeled on the 1983 OECD privacy principles. They have the usual things about the restrictions on collection and use of

data, the need for consent, all the sorts of headings that you've come to expect.

But the findings of the ACCC, when they looked at the regime, were simply that our framework with the collection, the use, and the disclosure, simply don't effectively deter the kind of data practices that the platforms are using. They exploit the information. Asymmetries. There's a bargaining power imbalance between us and between consumers.

So, the findings that the ACCC came up with is that there is enormous need for reform. And so if I talk about the privacy regime of Australia, it's in flux. Next slide, please.

What did the ACCC recommend? First of all, our privacy act is no longer good for purpose. It simply does not capture the sorts of threats that the digital platforms pose.

First, the definition of personal information. Our definition was tested in our Administrative Appeals Tribunal and found that it didn't cover the sort of IP addresses or online identifiers. So, the first thing that the ACCC says is, "You have to redefine personal information to cover the things that actually identify you."

We have to be notified about where our data is going. The consent. You've seen the graph that they drew about how hard it is to consent, and they said, "That has to change." And we have to have a genuine opportunity to understand what we're consenting to, and then to provide genuine consent.

And there has to be a way to say, "I really want my personal information deleted." Facebook, for example, says, "Well, yes, we delete your personal information." What they do is they hide it, but it's not deleted. And that was criticized.

There was a broader reform agenda that was suggested. Now, the privacy code. We have provisions for the privacy code in our privacy legislation, and if there's a privacy code that's approved by our privacy commissioner, then that gives the commissioner power to do certain things.

One of the recommendations was that the platforms need to come up with a code. They need to register it with our privacy commissioner, giving the commissioner of privacy more powers to enforce new privacy rules.

Finally, there needs to be … And for those who don't study tort, it's a civil wrong. You can take people to a civil court for … And this is for the serious invasion of privacy. We don't have one now. We've got other torts that possibly cover some of the issues, but not all of them.

So, this is a big reform agenda. Where we're up to now, the government—after the release of the report which was well over a year ago—said, "Well, actually, what we're going to do is take on board the suggestions." They had issued the first paper on the reform of our privacy legislation. Comment periods closed at the end of November. There will be a discussion paper and further opportunity for comment. So, we're on the way to deciding what to do to reform our privacy law.

The digital platforms are developing digital privacy code, and there will be legislation. Obviously, our legislative process has been held up because of COVID, but the statutory tort is or will be developed.

So, we're sort of on the road to adopting many of the reforms that were suggested by the digital platforms report. We're not there yet. Next slide, please.

So, just to recap. The review. There was already some social media reforms anyway. We have strengthened a lot of our provisions for, particularly, online criminality. But some of the …They're not crimes, but wrong. We are in the process of looking at a lot of that legislation, and some of it has actually been updated.

A review of the privacy act. The first phase is over, but there is another phase coming. Again, we're waiting for the legislation to respond to the first round of comments. The second round of comments was supposed to be February. It's now March. It hasn't happened, but that will happen. And we're expecting that to happen.

So, we're not there, but we have a lot of information that we didn't have before about the privacy issues, about the privacy regime in Australia. Hopefully, if we have this session again in a year's time, I'll be able to give, perhaps, a brighter and clearer picture of where we're up to. But in the meantime, it's a work in progress. So, thank you. Next slide, please.

It simply says, "thank you." And, "questions." Happy to take questions now or later.

LAURA MARGOLIS: Okay. Well, thank you very much, Holly. Really very interesting inputs about her country. And we have a couple of questions. We will read one. So, please, I'm asking the staff if you can read the question or should I read it?

HOLLY RAICHE: I don't care who reads it.

TANZANICA KING: I'll be happy to read it for you, Laura. So, the first question, and I hope it is actually the first, that I see here is, "Did the ACCC review the previous Australian Law Reform Institute reports on privacy as part of this review?"

HOLLY RAICHE: Yes. I'm not sure I should say more. Yes, they did. They certainly made reference to the fact that reforms have been suggested. And what they're saying is, "Well, in fact, what we've got to do now is look at the situation of the digital platforms and the new and different situations posed by the digital platforms in terms of privacy."

But, yeah. We've got a thing called the Australian Law Reform Commission that has done more than one review of privacy and, as part of the background reading to this report, by and large read the ALRC reports. There's also a productivity commission report that touches on privacy. So, there's a lot of literature that's referred to. These are

recommendations that certainly reflect what's been said, but do it in the context of digital platforms.

Any other questions?

LAURA MARGOLIS: Okay. Thank you, Holly. Yes, we have one more question, and it will be the last one for you because we are running out of time. But if you want to make more questions to Holly, please [say and] we will post on the chat our e-mail, so you can send them to us and we will answer them shortly.

So, please, Tanzanica, can you read the following question for Holly? Thank you.

TANZANICA KING: I'm sorry, Laura. I'm not seeing the question that you are asking me to read.

LAURA MARGOLIS: Okay. Should I read it?

HOLLY RAICHE: Go ahead. Read it.

TANZANICA KING: You can go ahead and read it. Hopefully, they can understand it.

LAURA MARGOLIS: "Did the ACCC review the previous Australian Law Reform Institute reports on privacy as part of this review?"

VANDA SCARTEZINI: That was the same one.

TANZANICA KING: Yeah. That's the same question.

VANDA SCARTEZINI: This is the same one. Laura, this is the same one. For the benefit of the time better to move—

LAURA MARGOLIS: Yes. Let's move on. I'm sorry. I had it copies and pasted. Okay. Well, now I will be …

Thank you, Holly Raiche, for your inputs. Now, we will be moving on to Romina. So, I will switch to the Spanish channel in order to present Romina.

Romina Cabrera, good evening. Welcome to our panel. Romina is from Argentina. Romina, the floor is yours. Please, bear in mind that you have eight minutes and then a few more minutes for questions.

ROMINA CABRERA: Thank you very much, Laura. I'd like to thank everyone for having given me the opportunity to share some very brief ideas with you about data

protection in Argentina and the relationship with the global village, so to speak, in terms of the history of ecommerce and everything related to the industry and digital economy, protection of personal data.

According to the Spanish Data Protection Agency, this is an independent fact. What has happened with the pandemic? Our lives have changed due to the extended lockdowns, but there are some positive things that have come up, too. E-commerce has really bloomed.

Oh, thank you. I've just found my PowerPoint in English. This is my information. And electronic [inaudible].

But what has happened in terms of data protection. Many people were not aware of where their personal information was going to because, as my brilliant colleague said, G-mail and WhatsApp services are not free. We're giving them our personal data. We're giving our personal data so that they will send us information. Next slide, please.

And they're selling products to us that we need or that we may not need in exchange for our personal data to create consumption profiles. In Argentina, for example, we have the Personal Data Protection Law. And as my colleagues have said, and will say over and over again, we have to adjust to this new digital environment based on the social demand. This is key because the different societies evolve according to their own needs. And they also create new profiles and new customer channels as well as new perceptions of what e-commerce is.

We've seen that during lockdown. We've been bombarded with information, and this has frequently worked because online stores have become the key players. What has happened with the personal data protect law in Argentina? Next slide, please.

Obviously, it meets the requirements of the European GDPR. In that international transfer of data, some conditions have to be met in terms of protection as well as in terms of the rights that are included in our national constitution. That also followed basic human rights principals which are based on the worth and dignity of human beings as set forth by the Vienna Convention of Treaties in Section 22.

And what happens, for example, in terms of new criteria? I am part of the Ibero-American Observatory for Data Protection of Madrid University, Spain. We get awards and we issue statements in different countries and we publish books. But our main goal is to merge cultures and different legislations in order to standardize legal criteria for personal data protection so that people will become aware of the fact that they have to take care of their own personal information.

This is fundamental because education is the best tool to protect our data in the digital society because Internet is just a means. It is not an end. It's the most wonderful means there is for those of us who have a healthy mind. But this information is also used by cybercriminals, so we have to take into account IT security. We have to follow good practices. We have to raise awareness so that we will have an open and secure Internet. Next slide, please.

I think this is the message we are all sharing. I was going faster than the PowerPoint because I have to meet my time. But basically, what we're looking for is to raise awareness in terms of good practices. We also want to have peace on the Internet as well as tolerance, freedom of speech, trust end users so that—thank you.

Here, you can see the main criteria. Trust end users, e-commerce, and prevention. Prevention is the best tool. Do we have a secure, reliable e-commerce? If we want that, we have to follow good practices, and especially consider IT security concerns so that we will have transparent platforms without any incidents as we have already seen during the lockdown times.

We've seen different types of attacks. Even critical government infrastructures have been attacked. So, prevention and cybersecurity has to be emphasized, as well as cybersecurity, cyber-defense, and cooperation between the public and the private sectors. This is key in order to raise awareness and follow good practices. Next slide, please.

International cooperation, ethics, value, and especially the hope that, as Holly said so clearly and brilliantly, in a year when they will meet again, we hope there will be more efficient and effective reactions because the pandemic has made us all come together. It has helped us grow as human beings. And we have really taken the Internet as an endless source of possibilities.

The last one. I'm getting to the end of my presentation. Next slide, please.

Well, this is information. I was going faster than the PowerPoint presentation. But basically, what I'm saying is that … Well, this is more specific information about the data protection law in Argentina, [Law No.] 25, 326. Argentina meets the minimum standards according to the European GDPR. Next slide, please.

And specifically, we're raising awareness in order to achieve a much better environment. As we have already said regarding value, culture, sensitive data. In the light of COVID-19, we have to emphasize health data issues.

This is the end of my presentation. I'm willing to answer any question you may have, and I'm also willing to make contributions to the Internet at the regional and global level. Thank you so much. This is the end of my presentation. It's been an honor and my pleasure.

LAURA MARGOLIS: Thank you, Romina. I don't know how you made it just on time. Thank you so much for your presentation. It's been great, and there are some questions on the chat. Do you want me to read the questions? Or, Tanzanica, are you reading them? Because I am in the Spanish channel right now. Tanzanica, what do you think I should do?

TANZANICA KING: It's up to you.

LAURA MARGOLIS: Okay, perfect. Thank you. Great. There is a question here by Eduardo Tome. "What type of penalties are included in the Argentine Data Protection Law?"

ROMINA CABRERA: Well, there are some penalties included which are usually based on the minimum standards which are related to the European Data Protection Regulation. We're always trying to raise awareness and to act in a preventive manner.

LAURA MARGOLIS: Thank you, I'll read the next and last question because we're running out of time.

ROMINA CABRERA: Yes, I know. I know that we could talk much longer, but I'm trying to be respectful for other people's time.

LAURA MARGOLIS: Thank you. This is a question by Pablo Rodriguez. Pablo says, "Which are the tools and regulations [here considered] in Argentina to follow good practices with users?"

ROMINA CABRERA: Great question. In Argentina, we have an effective legal action which is *habeas data* which is included in section 43 of the national constitution, paragraph 3, which sets forth that general rights in the case of personal

data issues, you can resort to this legislation to protect your rights. And the city of Buenos Aires, a few days ago, passed a collective process called … This is really a new thing related to commerce, to consumers.

So, imagine if we were able to transfer e-commerce concerns to a collective process. It would be very interesting, but this is something quite new. But we could work on this in the future. Even though I'm process-based, I think there would be a lot to work in terms of collective processes and *habeas data*.

The same thing regarding medical records. We have had a painful COVID-19 time, and many issues will come up in terms of the information of people who got sick. Should that information be reported to public health authorities, that would be a very interesting issue to deal with.

VANDA SCARTEZINI: Laura?

LAURA MARGOLIS: Thank you, Romina. We will have a lot of to say about these very interesting subjects, but we are running out of time. So, now I will switch to the English channel again to welcome Karla.

So, Karla Valente is from the U.S.A. So, Karla, the floor is yours. You have eight minutes. Thank you.

KARLA VALENTE: Thank you very much, Laura. So, data protection professionals around the world dream of having an internationals convention; something that would address privacy and data protection, maybe inspired by the Patent Convention [3T] or the Madrid system of International Registration of Marks. But so far, alas, there's no such thing.

In the U.S., we have a much more modest dream. We dream of having a federal data privacy protection law. Here, things are, I think, quite complicated because the U.S. does not have one single law that addresses this topic. It consists of numerous federal- and state-level laws which regulate data across many sectors. For example, health, finance, and credit; education, marketing, children, and so forth.

Although there have been discussions and there were, over the years, abuse presented and considered before the U.S. Congress, progress has been overshadowed oftentimes by some political issues, and we are still waiting for something to come up. In 2021, there's a very good likelihood that we're going to see something come up on a federal level.

As Romina mentioned, COVID-19 had cast some light, or some additional light on this important issue. So, businesses, or I've noticed, have made a wide range of changes in data protection. In their practices, they have adjusted priorities. They have adjusted their activities. There are some new obligations that are being watched for in case of, for example, contact tracing. There are some new cybersecurity practices due to the remote working conditions. So, this is on the federal level.

And in addition to having these different kinds of laws in the different sectors, in the federal level, you then have the layer of state laws. And state laws, 50 states [in the right states], and many of them have different privacy laws. Some of them are in a very early stage of trying to introduce a bill. And some of them are reintroducing bills or improving whatever they have upon. But, there's no standard across the states either, so that brings businesses and consumers as additional challenge to the issue. Next slide, please.

So, we have here the FTC on the federal level. In general, this is the organization that is empowered to bring enforcement action against organizations for violation where it is considered to be Section 5. In Section 5, it basically prohibits unfair or deceptive acts in/or affecting commerce.

And this resulted in a body of case laws and settlements over the violation of consumer private rights and failure to maintain security and sensitive information to consumers. Next slide, please.

So, here are some specific departments that have different kinds of laws and regulations. So, the Department of Health and Human Services. And then another one that controls finance, and so forth. So, as you can see, it's very compartmentalized. Next slide.

Here, I just give you some examples of some laws at the federal level that address privacy on specific issues. I am not going to go over all of them because there are too many and we don't have the time for that.

But for example, the Children Online Privacy Protection Act (COPPA) that, since 1998, imposes requirements of operators of websites and online services directed to children under 13.

You also have the Video Privacy Protection Act from 1988. And this notably creates a private right of action and allows courts to award statutory damages upward of $2,500 per violation [as well as attorney fees].

That is [inaudible], but is one of the strongest protections of consumer privacy against a specific form of data collection [for each of the virtual] [data collections].

[inaudible]. Meaning that states are free to enact broader protections for individual [records]. So, you have that [inaudible] to think about.

Then we have here for examples. One of them is [HIPPA] [inaudible] this privacy form, and you hear some penalties that it carries. And another one is the ESIGN which is a federal law that applies to interstate commerce, namely the transactions across states in the United States and with foreign [natures].

Nearly all commercial [contracts in the] United States fall under this umbrella. And here, electronic signature is defined as "an electronic, sound, symbol, or process attached to or logistically associated with record and executed or adopted by a person with the intent to sign the record." So, as you can see, it's also not very easy to follow.

And there are other federal-level laws that I don't list here. One of them is the Telephone Consumer Act of 1991. The TPCA restricts

telemarketing calls [in] use or automatic dialing systems, artificially pre-recording message. I live in California and receive them on a weekly basis, so I just wonder why this law exists. Next slide, please.

On a state level, it's really a patchwork of state privacy laws to add to the complexity of the discussion. And across the 50 states, generally there's a requirement of notification of breaches of personal data to affected residents, and in certain cases, to the state Attorney General who has the enforcement power over the laws.

Now, there are other kinds of privacy issues addressed that are very specific like biometric data, medical records, etc. But we are very far from having a state-level standardized. So, you have the federal level and the state level, and states that differ from each other which, it's very different for businesses. Next, please.

I, here, have only two examples of state-level laws. I included because it's probably the most comprehensive state privacy law in the country and provides consumers with rights over the use of the personal data, personal information, places, certain obligations on business who collect, sell, share certain types of information. The CCPA from 2018 was amended in 2020. There was a ballot here in November, and there's an amendment that follows that.

The two major developments are the CCPA entering into effect on July 1st 2020. The final regulation was issued in 2020, but the CCRA that passed a November ballot will become operative in January 2023.

And it will largely apply to personal information collected from January 2022. So, a lot of businesses are very watchful here in California on how they're going to do that.

And there was also a California Privacy Protective Agency appointed with five members to the board and some additional CCPA regulations approved.

And here you have some examples of fines and what those legislations at the very high level cover. Next slide, please.

So, what do we expect in the future? We expect to have an increase on privacy to state laws. As I said, different states introducing or reintroducing bills. And we expect to have an effort in Congress to pass something at the national level to help U.S. businesses to do better in a global market and to help in some way to ease the confusion around the world. Next slide, please.

A lot of people are talking about, so, what [are we doing] with all of these different layers of complexity. What we need to keep in mind is that they have some things in common. And these are some of trends that I've seen not only in the U.S., but across different countries, is the existence of a privacy officer, the introduction of penalties, the introduction of comprehensive private [forms], consent, [inaudible], and breach management and [authentication].

So, this is it for me. Thank you. I'll be happy to take questions. I will tell you, though, that even though I gave you just a very high-level overview of what we have here in terms of laws, I mainly work on privacy

programs helping companies to introduce or manage their privacy programs on a day-to-day and navigate the ecosystem on a global level. Thank you.

LAURA MARGOLIS: Well, thank you very much, Karla, for your presentation. We have a couple of questions in the chat, but if it's possible for you to answer them maybe in the chat because we have to give the floor to Fatima because we are out of time. I'm sorry.

KARLA VALENTE: No worries. We will do. Thank you.

LAURA MARGOLIS: If you can. If not, maybe we can send them by e-mail, the answers. If they are longer, maybe.

KARLA VALENTE: If I don't answer in chat, I will answer via e-mail. Thank you.

LAURA MARGOLIS: Great, thank you. Okay. So, now I will switch again to the Spanish channel. I'm sorry for the interpreters, that I'm switching between languages.

Fatima, are you there?

FATIMA CAMBRONERO: Yes.

LAURA MARGOLIS: Hello.

FATIMA CAMBRONERO: Here I am. Hello.

LAURA MARGOLIS: Welcome to our panel. We give you the floor so that you can tell us about the data protection laws in your country. Thank you very much.

FATIMA CAMBRONERO: I promise I won't bother the interpreter, so I apologize if I speed up. Thank you very much for the invitation. I would like to tell you that in Mexico before 2010, we had the scenario Karla was describing in the U.S. There were state laws. Each state in Mexico had its own legislation for data protection. Not all of them, but many. This became a nation, until in July 2010, the federal private data protection act was passed to regulate the issue of data protection when the data belonging to a natural person.

And in 2017, a new act was passed for the protection of private data in the hands of subjects who have to report this. The difference is who is holding the data. In the case natural personal, were they people? Processing the data is natural person. And in the other case is …

In the second [case] we have organizations in the public sector and the three powers. And the new thing in this act is that those people responsible for [inaudible] political parties, trusts, and unions. I don't know if I've mentioned them. These laws are the main laws for data protection and [they're a] comprehensive act. They don't apply to one sector as Karla was saying in the U.S. They are comprehensive acts that are mandatory and binding in all the territories of Mexico.

Now I'm going to talk about the federal act on private data held by natural persons, which is the most important for companies. In this act, we have three categories of data: 1) personal data, 2) standard data such as I.D data, name, address, nationality, marital status, financial personal data, bank account, credit card information, and the sensitive personal data defined by the law as the data where the improper processing may cause harm to the data owner. And this classification is similar to the one in the GDPR from Europe which was amended recently.

And 3) intimate category which is biometric data. In Mexico, they are considered sensitive data if, according to the way they are used or processed, they may cause harm or discrimination to the owner.

The act sets forth some obligations by those in charge of controlling data, data controllers. And it's similar to the GDPR. So, data controllers have to abide by the principles of responsibility, proportionality, quality, purpose, etc., and the additional obligations. The obligation of security and confidentiality. These are obligations for the data controllers, and if they don't abide by these commitment, they may be

punished by the corresponding agency in Mexico, agency in charge of protecting private data.

The rights for those data controllers are the ARCO Rights, and people that have supplied data may remove their consent. Some rights that are present in other legislations [are] the right to data portability. That is not included in Mexico for data managed by private persons. The right not to be the subject of automated decisions. This is not included in the acts in Mexico.

The right to pay a compensation where there has been an improper use of personal data, though this is included in a different act or treaty that is applied to all American states.

And the right to be forgotten is not included n our legislation either. What we have, which is similar, is the right to cancellation. Should the rights of the owners be affected, there are three things people might do when … They may go to the authorities to report this so that the people who have breached their data privacy may suffer some penalties.

And for us at ICANN regarding personal data and the WHOIS or the WHOIS protocol, in this case, it's important to stress that according to the amendments of the GDPR the results which we get from WHOIS in the gTLDs now … Personal data should not be included when WHOIS information is shared, according to the new amendments of the GDPR.

And we should bear in mind what happens with the ccTLDs or the .country or the managers of the ccTLDs. In the case of Mexico, the .mx registry manages [inaudible] Mexico [in] the country. And the WHOIS

protocol, when it was developed, it wasn't created for data privacy purposes. It's just, it was there to share with users information related to a domain name that has been registered.

Regarding Mexico, the .mx registry is a Mexican agency and it has to abide by the Data [Protection] Regulations in Mexico. In Mexico, there are no limitations regarding the information that might be shared after a WHOIS search. So, in our searches launch in Mexico, we get personal information about registrants.

For us working in the IP arena, it's very important to know who is a registrant and what has been the history of a domain name, who it was transferred to, especially when there is a case brought to justice.

It's also important to stress, and we have this in ICANN, that WHOIS is going to be replaced by a new protocol, RDAP, which is different from WHOIS because it shares sunrise resets for all domain names. And it's run on a web standard which is easier to understand for machines, so the results may be standardized.

And this may also include … The system will now share information about internationalized domain names.

LAURA MARGOLIS: Fatima, sorry for interrupting. The interpreters are asking you to slow down.

FATIMA CAMBRONERO: Sorry. Finally, in closing, we should review what would happen if this new protocol is deployed and if the results, once standardized, will have to abide by certain limitations set forth by GDPR for gTLDs; and if this will also be applied to the ccTLDs.

Several colleagues from the ccNSO are here, and they have already been discussing this issue. We don't know whether it will be mandatory, whether some amendments have to be introduced, or if they will only have to abide by the legislation related to personal data in the country where they are operating.

LAURA MARGOLIS: Fatima, thank you very much for your presentations. And we could talk about this for ages, but we have a few minutes left and I would like to give the floor to Vanda. I will switch to English again.

VANDA SCARTEZINI: Thank you. Sorry the time was so short for so many interesting things. So, please change the next slide, please.

So, I'm talking about the Brazilian law that will be, that is [start] to be valid from September last year. And the sanctions will be [validated] from August this year. But you're going to see that is not exactly the case.

So, we already have a Data Protection National Agency like all those in Europe where our legislation is based on GDPR. Next slide, please.

So, you can see all the green are similarities. And the difference that we have regarding GDPR, so we have the right to access, the right to be informed, rectification. Most of the rights that Holly and Karla and all the others have been talking about. You're going to keep these slides after the meeting, but I will [inaudible]. Next slide, please.

So, what is the difference? So, the difference is the right to be forgotten. Why? Because our constitution prohibits anonymity. So, it's impossible to be forgotten. We can delete the name, but not [forget it].

The right to have restricted processing. LGPD does not provide, but it's possible to conclude that our persons have this right. We have the necessity that limits the treatment to a minimal necessary and agreeable [purpose] for those [access].

The right to not subject to automatic decision, we don't have either. But we have the right to obtain information about the criteria and procedures that guide the ultimate decision, have request review.

And about the harmonization between actors, GDPR does not require it. But the last e-mail [inaudible] during last July shows a possible meeting in the future. The problem that we have here, that when we have harmonization, you give the opportunity to all public organizations to process the companies before these sanctions that are subjected in the law are …

It's possible for the agents that are responsible for the protection law in the country to really process any company for leakage or for any problem that will come for not obeying the law. So, that's what we are

having now here. That is quite complex. So, the next one. Please, the next slide. The next one. Yes.

So, all this change is … Well, both are global. We can have less time to answer the owner of personal data for any questions. We have the same agents. The DPO, for instance, that is the Data Protection Officer, is mandatory in the GDPR for public organization and only large personal data treatment companies. And in Brazil, it's mandatory for all. Maybe the agency change that, but nowadays is for all.

The report about data leaks for the agency, for the GDPR, is within 72 hours. We don't have it yet, this defined. The agency will define this year, but it's open now.

Controller. We have demanded a contract between the controller and the operators. Maybe [inaudible] the other problems regarding other laws. And for the GDPR, we don't have this requirement.

And, of course, our sanctions are high like the GDPR. Of course, in our currency. And instead of 4%, it's 2%. Next slide, please.

So, this is what happened in our country, reference for August last year. So, we have a survey in our software association, together with Ernst & Young Global Limited company. So, we have a survey with all sides and all sectors around the country—more than 10,000. And that is the result.

At that time, average compliance with the Data Protection Law was just 40% of the companies. And if you see the different aspects of this process to keep the compliance, technology is the best one. But process is the last implemented, and personal data is also low.

So, the risk data. About 30% had data violations since the approval of the law in 2018. And 75% of those organizations deal with personal sensible data like [medical] data, children data, and other like race and sexual options. Those kinds of things that in our law are considered sensible data.

So, that is all. Next one. Thank you. And I believe, for me, this is that, and we are finished with that.

And since we are in the end of our time, I'd like to thank you again. Here is my e-mail. Any other questions you have, you can address to me. Not only for me, but I can deliver it to the other panelists. So, I'm in charge of this panel here. So, please feel free to address me any questions to me or to all other.

I would like to thank you very much for your presence today with us. And we will certainly repeat this kind of experience under DNS Women the next ICANN meetings or even in the independent webinars. So, thank you.

I open then floor to everyone if all members want to just open your video just to say thank you to our audience. Thank you, everyone.

LAURA MARGOLIS: Vanda, [inaudible]. Thank you. I want to say thank you to all the staff and the interpreters who made a great job for us. And from my side, I wish you a very successful ICANN week. And I hope to see you soon, in real life. Thank you.

VANDA SCARTEZINI: Okay. Thank you.

KARLA VALENTE: Thank you.

VANDA SCARTEZINI: Thank you, everybody. Bye-bye.

[END OF TRANSCRIPTION]