ICANN
Transcription ICANN Barcelona
GNSO – NCSG – Can formal standards simplify 3rd party access to registration data?
Session 3
Sunday 21 October 2018 at 1700 CEST

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page: https://gnso.icann.org/en/group-activities/calendar

Ayden Férdeline: Thanks for recording John again. Sorry about that.

Patrick Fältström: Yes, so this actually matches quite well. And I'm a little bit surprised how well things fit together. But on the other end, I should not be surprised because we come from the same kind of organizations and do similar things. Patrick Fältström. I'm technical director and head of security at NetNod. We've incorporated that is owned 200% by non-for-profit foundation. We do various things including running server, running DNS for 30 countries in the world. And we're responsible for among other things distribution of time infrequent in Sweden.

So we are trying to things the right way. If we look at - so on base since we've done of course everything I do in based in European and Swedish jurisdiction, although I've been working in the global environment. But this is sort of more - it's quite European view. In some kind of order I think - what is most important is just like Rod said, the most important thing for an organization is not to screw up. Okay? You want to do whatever you're doing. That's how you make money. And that's how no one comes up to throw you in jail or whatever. Help people not get mad at you.

So it's really simple, but for a business continuity standpoint, you need to have good process internally and not do the wrong thing. And I was here earlier today and heard you talk about and discuss the ISO certification and whatnot. And we have to remember that many of those certifications doesn't really say on – say how good the process are, just that you have processes. And I think that was something you touched upon earlier today.

So, it's also the case just like Rod said is that certification is actually helpful to an organization itself. But it doesn't really say much about how high the quality for an external party how good the organization is. So in various legislations and oversight that we have in Sweden, there is a very strong recommendation from the authorities that do approve certain activities for organizations.

For example, like us that can handle classified information. But as an organization, you should have ISOS 7 or 27,000 like processes. So there's not a requirement. So that you're having the frame on the wall doesn't help. If they want to do an audit of your organization, they will do so and you can fail or not fail regardless of how many certifications you have. Because whether you pass or not, if there is a formal audit, it's how you do things. It's that simple.

It's also of course that the recommendations are also help for the organizations to actually - to not screw up. The second - so that's the first thing. You have to do things in the correct way.

The second thing which is also important that Rod also brought up is that when you have come up with the processes that you use, you're not done. You need to improve the processes. You always have something that might either be everything at Graystone from just a bump in the road. Stars found that something was complicated. You're either unclear, decision that had to be made internally. To actually sort of incidence. And with incident, doesn't have to mean something actually impacted the customer's data. It just has some kind of incident.

You need to have a continuous improvement of your processes. That's the second thing I would like to say. Really really important. And not only improvement based on incidents within your organization, but also what you hear about others. And that's why I will come back to that in a bit. On information sharing, it doesn't only have to do with pure information also on how you do your business. Because learning how to do your business in a more efficient way, in a more secure and stable way. It's also something that is interesting to share.

The third thing which is important which is also now with this various legislations is by legal means, even more important has to do with information classification. And unfortunately, there are too many organizations in the world that today overclassify information. You need to keep track of what's really sensitive and then keep track of that.

We are in Sweden. Now, at last for us to make next year changing our legislation around the information classification mechanisms as systems. So we are doing things in the same classifications schemas. NATO’s doing this. Military's done so. Now also all of Sweden is moving to that direction. And that is something that is taken over. So in many parts of the world, so I think that's a good thing that we start to take a harmonized information classification system in the world. Because otherwise, you just cannot share information with each other. And so, multiple parts to make sure the bucket with the most information is really really small and keep track of that.

The fourth thing has to do with trust. And this comes to not to translocate - okay, you have some information. Who do you share the information with?

And to some degree, one could say that trust is the same thing as authorization or what you base authorization on. Or approval process or whatever.

One of the key things that we are discovered when working with securities is that you cannot - seriously you cannot be told who to trust. Whether you trust someone is a decision you make yourself full stop. And that is both an individual or organization level. And one of the things that we're fighting with on the cyber side and Rod and (Greg) and others in the room can correct me if I'm wrong.

One thing we're fighting with is how to translate trust between individuals to trust between organizations. And trusting organizations is pretty damn difficult. And specifically in the new world where historically we think that we always have trusted the government which makes the policy and law enforcement. But we actually now in the global environment have a different sort of designation of trust between organizations. And I think we should think about that much more carefully.

Now in organizations supposed to sort of do things between each other. But baseline, it's very very difficult to be told who to trust. And that's why some sorts work. And some sorts do not. And specifically when governments tell companies you must trust this cert. You should share everything you know, everything that is bad in your organization with this organization. Like why should I do that? I don't trust them.

So, to be told who to trust and it's difficult. To make a decision on who you trust based on various (disencountered) data, that works. Next thing. When information is shared on the sort of cyber information security. and I'm a little bit hand waving because as Rod said, there's multiple definitions of these things. Whenever you talk about cybersecurity information, security needs to define the terminology. One mechanism that is used because we don't have any global classification is something that is called the traffic light protocol or

TLP. Which individuals specifically when - because ultimately even though organizations share information, ultimately there are individuals that do the actual information passing.

There's a very simple way with red, yellow, green or red, amber, and green that you can use to inform how it's receiving (unintelligible) and share information. The - and then the information sharing itself is of course used in cryptography of different kinds. When even - when encrypted information can be shared, because in many cases we have information that is classified in such a way so you cannot store it on anything that is connected to the internet. And of course, then you cannot really share information that way. But PDP is used heavily.

And then the last thing I wanted to say about trust of course, it doesn't really scale to have trust between like all parties in the world that works with these issues. So there are transitive sort of trust networks that have been built and are built over and over again where you have the vesting scheme, that for example. If I have five people that I trust that I know trust another person, then probably I can trust that person.

And then you can build sort of a network of trust. And that way, you can communicate with people that you in a trustworthy way even though you are not - you don't directly know about that entity. So, there are various ways of transition of trust that is in use in practice. Otherwise exchange of data would not work. But to start with, as Rod said. Good processes and continuous improvement of those. Thank you.

Ayden Férdeline: Thanks very much Patrick. Do we have any questions? Collin.

Collin Kure: Collin Kure for the record. So the first question was a clarification question. By what you were referring to when you said sensitive data?

Patrick Fältström: It doesn't really matter what is sensitive. What is sensitive to me is something that I have classified to not be something that be shared with everyone. And it could be anything from contracts to legislation to - are the canon of laws that say decisions on my own, that this date they cannot be shared. So sensitive data means data that cannot be shared with everyone.

Collin Kure: Thank you. Yes, I think that that highlights the (intuity) of having these kinds of cross community sessions. Because when I heard sensitive data, I was thinking like GDPR definition, like religion, gender, you know? Things like that.

Patrick Fältström: No, well it might be. It doesn't really matter. It's just some - it's some data that I have that I'm in possession of that is stored in system that is mine. And I have the responsibility to make sure that that information is not leaking to someone that should not have access to it.

Collin Kure: Thanks. So the second comment that I wanted to make was kind of a broader observation. I was interested in what Rod was talking with the certification to standard certifications. And then kind of linking back to when Marcus Fee was mentioning that Microsoft kind of had been a real proponent of GDPR and pushing the envelope for privacy. I was thinking in the policy space, particularly in ICANN as we're attempting to develop these global policies, then it could be interesting to explore the notion of GDPR compliance as some sort of certificate that is reached a level of privacy protection that perhaps could signify something across the board in terms of protections for registrant rights. Just throw that out there.

Rod Rasmussen: Since you mentioned my name, I figured I'd ask a question back. Who would actually be able to give GDPR certification? Because if we can find that entity, I think we can short circuit a whole lot of discussions around it.

Collin Kure: I guess it would be the absence of fines?

Stephanie Perrin: Hi yes, Stephanie Perrin for the record. I think this is really really interesting input here. I mean I have questions for all of you. So I - and I don't want to keep Reg waiting too long. To respond to the question about GDPR compliance, I mean the whole point of article 43 was to come up with some standards that would at least define the management practices that they're looking for.

Because as we hear from (Erin) all the time, well we keep asking them what they want us to do. And they don't, you know - they're not clear enough. So, as you say procedures doesn't mean compliance. And it doesn't mean your vulnerabilities are all covered. But it's better than no procedures. Right? Usually.

Patrick Fältström: I think the situation is that - it's like asking the Olympic committee how high do I have to jump to win the Olympic gold at the next Olympic games? and expect an answer. I think the thing with the compliance is that the way legislation for these kind of things is written, me not being a lawyer, is that it just explains under what circumstances there is a breach or a leakage from my systems and if there is such a breach, then it's my fault. It's not the case that it's not my fault if it's the case that I have fulfilled whatever kind of rules there are. So asking someone some detail or something, okay how - what kind of defense mechanism is needed? The answer will probably always be enough. Yes.

Stephanie Perrin: Or it depends. Well and that brings me really to my question. I'm wondering in terms of the application of standards, because you all use them, and I'll give you a hypothetical here. Canada, one of the departments lost their hard drive full of sensitive medical data of citizens, right? Now in Canada, if somebody leaves one of those things lying around on an open office desk, the odds are pretty good it got put into the recycling. Somebody thought it was junk.

That would not be the case in countries where the corruption index is - puts them in the top 10, for instance. Or where the economy is so bad that people will be scrapping things for spare parts and selling, you know, for the mercury in it or whatever. How do you a risk assessment about compliance with Management standards? And how do you rate that globally? Because in ICANN, of course we're talking about global access requests, right, to who's data?

Rod Rasmussen: So, this is Rod. A lot of the reason for - well there is a couple main reasons. I think I touched on them earlier for getting certifications. One is to meet the standard so that you are given access to some data of some sort.

Another is for insurance. So in other words, I want to get insurance. I need to prove that I can - I have the certification in order to lower my insurance rate or even get the insurance in the first place.

If you think about both of those circumstances, there's usually some sort of audit process that goes on along with that. Some sort of examination. I think that is where you have to look for that. Again, it's sort of a (unintelligible) as a one-time thing with some sort of renewals. Right? Versus an ongoing operational thing. But at least at some point in time you met that particular threshold.

And the - as a result, you are given some sort of privilege. That doesn't mean you're not going to screw up and lose that. But what it does is makes the risk that you're going to do that much less. And that's the point. Right I think when you especially are thinking about it from an insurance perspective. It really helps bring that home. I think that good analogy to think about in this particular case. It's about risk management.

Ayden Férdeline: Next in the queue is Reg. Thanks for waiting.

Reg Levy: Thanks. Reg Levy from Tucows. I think your point which I think you made about standards compliance not being a silver bullet just because you are a - just because you comply with certain standards doesn't mean you are going to suffer a breach. And I think that that's accepted across the board. Standards are sort of a baseline, a place to start with. That if you don't have at least - if we come up with a standard that we can all agree with, that if you aren't compliant with that, we can't give you the data.

But just because you are, doesn't necessarily mean that we can. And of course, nobody is immune to breaches. What I was hoping to hear from these presentations was what security researchers are looking for in terms of actual data points that absolutely need. Because I hear from the IP community and I hear from security of research community and from law enforcement, we want everything we need to have.

And I would rather start from the assumption that you don't have any of it. What do you need? So are there specific data points that instead of just saying across the board, we need to have all three email addresses because sometimes they're different and that is a big deal. Or all three contact points because sometimes they're different and that's a big deal. Which is another argument that I've heard.

Finally, I'd like to sort of piggyback on Stephanie's comment about trusting researchers. And I'm sure that everybody within this room is probably on the list of trusted researchers.

But when I was running a registry or 20, the centralized zone file system was a mess. And we had to give access to anyone if they gave a valid reason and a valid reason included research. And so we received requests across the board from people who I would otherwise not allow access to. And for the reason that they didn't give their full name. For the reason that their email address seems sketchy as fuck. Or other reasons. And they just said research. What's the reason you need it? Research. Can you tell me what kind of research?

Some of them even went to say - so far as to say I'm a student and this is research. Which is great, but, like, are you a computer science student? What kind of research? So again, I don't mean this to sound as - like an attack to anybody in this room, but those are my main sticking points and places that I would like comments from. Thank you.

(Greg): Okay, this is (Greg). So of the data that the - for example, registrars collect. We're not talking about the billing information and all that other stuff. We're really talking about the contact information. Name, address, email address, phone number. A certain percentage remains vary in the content of what the registrant contact versus (unintelligible) tech content has.

All that information is used and is useful for the purposes that security people use. It's used for a variety of reasons. One is correlation. Another is attribution which is finding out maybe who actually perpetrated a problem. The information is sometimes verified. In other words as a truthful or not truthful as information that address given the, you know, bogus or not. Those kinds of things.

And all of those pieces of information are used and useful. So that's the answer to that question. The CZDS thing is a little apples and oranges maybe. In that the zone files don't contain personal information. Hopefully the agreements to my recollection allowed some - a little bit of latitude. But it was kind of like you had to prove that somebody was misusing it, which is sometimes hard. But again, that was not non-PII. So I understand where you're coming from though.

Rod Rasmussen: This is Rod, I would like to add to that a little bit. The usefulness of the information depends on the situation. When talking about the contact information. And one of the important ones is actually being - is for contact ability for people who have been comprised. Right? And that's where having - for example, having information that's actually useful in the tech context field or fields can help short circuit our problem much more quickly than just having a registrant contact.

Because you can actually to someone who has hands on keyboards and go clean up something. But at the very least, you can get ahold of somebody responsible for something who by the way has been breached themselves. Right? If their website or so their email or whatever has been compromised, maybe there's a good chance that their own personal information is at risk. So it's useful there. And obviously for contact ability, email and phone numbers is the most important things.

You're not probably going to send a letter to somebody. I think the lawyers like the physical addresses. From cybersecurity perspective, it's much more of a what can you do in real time? Or semi-real time to answer things. As far as correlation goes, I would say there is a spectrum. All the information is useful but some of it is more useful than others. Right?

So an email address which is a unique identifier is the most useful information. A phone number may or may not be, you know, that's also a unique identifier, but there is far - those are typically not as useful for correlation because the nature, the way people fill those out versus how they fill out emails. Because the emails they typically want to work. If it's - either a good guy or a bad guy, right? They want them work. Because that's how you control the main name in the first place.

And then oftentimes the organization/registrant name type fields are very useful because those get filled out in certain ways by automated systems and things like that. So that you can either A) establish all these things are the same or B) they're using a pattern. So both of those are useful. But the utility value goes down. But again it depends on each case. I dove in the weeds a little bit there because it's not - there's no simple answer to your question there. And I just want to make sure that you have a full answer to that.

Ayden Férdeline: Thanks Rod. We have a small queue. Rick followed by Patrick and Stephanie.

Richard Wilhelm: Sure, this will probably be a quick one. Just a brief clarification on some terminology. We've been using the term sensitive data a fair bit. I don't know of any concise consistent and anything approaching global definition of that term. Although we all have kind of a good idea about what it means. It does not stretch very well. Which is - so it's fine for casual conversation but we all just need to be aware that it doesn't really scale.

And even ironically Patrick had mentioned that traffic wide protocol. There are at least three of those that you're probably aware of, right? So it's just interesting when you get into this stuff. Consistency is a hot button here.

Patrick Fältström: Yes, what Rick said. Yes, let's see what I want to - okay. Oh yes, one thing that - there are two things I would like to say. The first one revolving your question, what are you going to go after today and use the data for? To go back to what Rod said. I think from a security - it's hard for me as a security person to say beforehand what data I would like to request from you.

But when I work on a specific thing, I can most certainly ask what data it would like to have in that specific field. For the various kind of incidents that I work with, because I don't deal with for example, collecting statistics to detect what is good or bad. I work personally with specific incidents. So I can go directly to you and I can say I specifically would like to have this subset.

And the reason why I wanted to say that in how I work and how we work, we deal with things that way is that from our perspective, we like very much the transparency reports that are written by the - created by various organizations. So we don't - (unintelligible) not having problem with, for example, whoever we are requesting information that they record what we have asked for. And under what circumstances. So that can be known.

For various kinds of types of incidents, it could be the case that, for example, we are requesting - it happens quite often that we request a silent parade on that data for six months or something so it's not disclosed during the period its investigated. But then it can be released. So don't have any problem with that. So the people can use as part of their determination of whether they trust Netnod.

Because as I said, whether you trust someone or not is a decision you make yourself. Okay. Resulting in the traffic light protocol, you are absolutely correct Rick. And people diving into this understand that Rick. And they all - we all remember when one certain organization changed the definition of traffic light protocol. And all over - all hell broke loose. But anyways, so trust (unintelligible) reports I think is important. And also that people clarify what information they want when they actually - when they are looking for data.

Richard Wilhelm: Thank you.

Ayden Férdeline: Thanks. Stephanie, then Rich.

Stephanie Perrin: Thanks very much. Stephanie for the record. Every now and then when I look at this problem. Because obviously the only reason - I mean it's not just finding the rhetoric that's been dispensed since (unintelligible) went dark. But I do understand we need you guys to be doing what you are doing - fighting malware and botnets and all kinds of things.

And there is a lot of crime out there. And guess who has the research budget to be doing research? Yes that would be the criminals. So every now and then, I think maybe we just ought to - sorry breach security folks. Rather than try and - I'm getting stares from my colleagues here. Rather than try and impose standards. I mean standards would be some of the things you would discover in an audit that you are complying with. That's sort of a no brainer. But would that be a way of handling it?

The only worry I have is what exactly would you audit? Because when they did the financial crimes reporting center in Canada and defined they would let them do data mining, they had the privacy commission do - I think is by any old audits. And I was tearing my hair out because it's not the financial crimes reporting center that needs the audits. It's the guys who were feeding the data to them who were insecure. And who were reporting. And who are, you know - so what would you - if you were to put up your hand and say audit us, and just give us all the data? What would it be?

Patrick Fältström: I think we should not only talking about the auditing. I think it's more important to look at what is happening when someone actually makes a mistake. And we all have experience from ICANN compliance just as an example where we actually have very explicit not only auditing - but also very explicit contracts that we all in this room have held right in the contracts. They're supposed to be crystal clear.

And then you have people partners that are assigning those contracts. And then you have disputes and discussions on whether people are compliant or not. So the question is also okay, what do you do? And we have to remember that on the internet, things happen really really fast. We had a presentation in (unintelligible) a couple of meetings ago just to give you a sense of what we're talking about here is that if we look at domain names that are used as source for spam.

And we look at the - if you take the number - if you take the domain names that are used for spam - classified as spam source up to 150 days. Fifty percent of those are already classified as spam source domains by these private companies up to one hour after registration.

So we're talking about here processes that are so fast that we cannot have any humans that do evaluation and checks whether someone has a license on the wall or something. This is something that needs to sort of go electrically fast.

And one simple thing, for example, could be that okay - every domain name and one rule that could be used that some people are in favor of. Every domain name that is in use should be default be classified as a spam source the first week. Of course not many companies would like that, you register the domain name, you would like to be able to send emails. So that's where we are.

So let me take a step back. The only way (unintelligible) trust things work as a (unintelligible) is by having organizations themselves decide who to trust. And the only way to expand that - so that, for example, multiple organizations far away from each other can communicate with each other is by using sort of trust networks where you have some kind of loosely binding mechanism where there's a decision made whether organization can be trusted.

But it might also be the case that people aren't trusted anymore. And this is something that we just don't know how to do. And because of that, I don't think a too large group like this, or even more people can do that in these ways. This is the hard problem.

So I think you Stephanie and others which are trying and trying and you see that you’re banging your head on the wall - or against the wall. Yes you are. Because it is hard. And personally, I don't really know how to deal with the problem. If I knew, I would propose a solution. But ultimately, there is a question of who you trust? And who can you decide to have access to what data? And that is hard.

Stephanie Perrin: If I could just respond to that. The - I mean countries don't find mlapse with countries they don't trust. And I know everybody hates mlaps but the GDPR has provisions for the sharing of liability from processes to controller and you know, in through the whole chain. You're not going to find one of those shared liability contracts with somebody you don't trust, are you?

Patrick Fältström: That is correct. But this is what I'm talking about. Mlaps is a good relent, works when you have up to maybe 200 participants. What do you then do? Yes. So this is where I'm (unintelligible) so yes, we have some mechanism here. And this is what I think a discussion really should be about.

Rod Rasmussen: Yes, this is Rod. Let me add to that. The mechanisms you use around this or the standard mechanisms you use in other places where data is being transferred between parties, right? And that's contracts and clauses and penalties that are agreed to within those legal documents. Excuse me.

The question is exactly what Patrick was just talking about. How do you scale that when you have, you know, 100s to 1000s of contracted parties? Are they dealing in the ecosystem? And then probably 10s of 1000s of financial institutions, cyber security companies, intellectual property holders of some sort, big brands basically who are being attacked who want to get access to data so they can do something about those attacks.

So you have a - you run into this n-squared problem which we hate in computer science, right? How do you deal with that? You know, and does - we were talking about accreditation bodies, right? As one way of doing that.

You still have to have a legal construct though to get from the person who wants data over here to protect their network or whatever it is to back to whoever has the data in their database right? And where does that - how does that path work? Right? And is - who sets up the contracts? As I come to the middle here, I see ICANN in the middle of that somehow.

So that's something to think about from a scaling perspective. You can do one off's, one to one. And that's happening, by the way. You know, then - there are people out there trying to make it a possible via contractual relationship to get ahold of data. And that's, you know, one way to do that. But it does not scale for everybody who needs to get ahold of data.

And I'll use an example. You are looking confused there. From prior to GDPR where I was involved in setting up deals with various registration entities. I'm not going to get too specific. Where we had access to data. But we had a direct contract with or an agreement with that party. Right? To be able to get access to data that other people in the industry didn't have.

Other people went and set up some contracts that - those same entities. That works for solving particular problems. It does not work for solving an entire industry problem. And both - industry on both sides of the equation. So you need some sort of way to do scaling around this.

Patrick Fältström: Patrick here. One thing that could be done, for example. Given that first problem itself is that they define it and people agree to it. And then I'm actually very happy and positive this session because people are sort of feeling down and meek so that's a good start. When we agree on that, maybe it's the case that we just draw straw to look at what mechanisms do we actually have?

And why don't we, for example, start to get just like you yourself did. What do we do with real crime? We have real analysts between certain states. Which is based on jurisdictions. We're a corporation. We're Interpol. Which is also marked by default that everyone trusts everyone. And you still have agreement there.

We have the Budapest convention in which we have certain mechanism where we can improve those bilateral agreements between jurisdictions. We have the network of firsts which are the incident response teams in the world which also have indirect sort of approval mechanisms and stuff.

Maybe it's the case that we can sort of investigate how those work because we know that regardless of what we come up with which will suit everyone. These other things will still be used. It's not the case that we'll stop use mlaps for cyber-crime just because we come up with a magic pixie dust for the solution here.

But then of course, okay, what do we do in the meantime? And maybe we can try to identify and minimize the amount of gray zone here. And see what we can do about it. Another thing I just wanted to say that I think is - that I'm also positive to on the discussions the last couple of sort of weeks and stuff is also that people start to -- which I think is really really good -- separate collection from access. And the fact that we here have been talking about access only is I thank you. Thank you. Thank you.

Stephanie Perrin: If I may just comment on that. I mean we started talking about this standards workshop about a year ago. And really I have had nobody beating a path to my door showing interest. Now, thankfully I think we had a good discussion today and (Allie) at Nast was here saying well thank goodness we're talking about real things. Whatever his phrase was. I can't remember. In stark contrast to the EPDP where we're still banging our heads against the wall.

So I mean I don't know what it takes to get real about what we need for compliance. But you know, it's quite - yes we have to make (unintelligible) I guess. Anyway, I'm taking out my spot in the queue here, sorry.

Ayden Férdeline: So we have Reg in the queue next. Then we might look at the agenda again just to make sure we're good to finish at 6:30.

Reg Levy: Thanks. This is Reg Tucows. I've been enjoying the conversation. So I appreciate being able to witness it as well. Thank you to the people who responded to my request for what are the data points that you need. But what I heard was what the data points that are useful.

And I'm sure there's all kinds of information that I could collect in addition to what I already do that would be extremely useful. But that's not what you need. And so at the end of the conversation, what I did actually hear was e-mail and phone number.

And is it the case that if I gave you access to something where you had access to all the email addresses and all the phone numbers but nothing else. Would that be acceptable? I don't know if that's feasible. I don't, you know - nothing else but trying to find out where the compromise is. Because this keeps coming back to trust. Who do we trust? And how far do we trust them?

And as I said earlier, I probably trust everyone in this room. But I'm also the avatar of the trust that my customers put in me. And they don't know who you guys are. And they don't even know who I am. So it's a very delicate balance, I think. And I am trying to get to the right place. To the place where all of us are completely unsatisfied but better than we are right now.

Secondarily, Patrick said that he very often has single instances where he can come to me and say this is exactly what I need and this is why. That is excellent and I love that. And I accept that is not the usual circumstance for security researchers. That's the usual circumstance for NIP lawyer.

So NIP lawyer comes to me and says this particular domain name, give me this information, and I say great. I can see that. Here you go. But I absolutely understand that the whole point of security research is this kind of stuff that can be done in 10 minutes by not a human. So trying to figure out what the parameters we are that we can work into. Thanks.

Ayden Férdeline: Sure. So what we're going to do now is we're just going to look at the agenda to see what we've covered and what we have not covered. And (Dede Campion) from the council of Europe was unable to join us today because his flight was cancelled. But he did send a short statement through that I might read. Yes, sure. Sorry about that.

(Dede Campion) from the council of Europe had hoped to join our discussion today but his flight was cancelled unfortunately. So he did email through a short statement that I will read on his behalf.

And so, he wanted us to be aware that the council of Europe welcomes all efforts made to integrate better privacy and data protection considerations into ICANN policies. And he is also provided a link that we can circulate to a new paper to the council of Europe released last week on this matter. So if we look at the agenda, we have covered the bulk of it. But what we have not covered is the civil society perspective on these issues. And so, that is what we will do now. I'm going to hand over to Stephanie, if you would like to go to Brenda.

Stephanie Perrin: Over to Brenda and Tamir Israel. (Cannot hear him/her.) net policy and privacy.

Ayden Férdeline: And is Tamir online?

Tamir Israel: Hi can people hear me?

Ayden Férdeline: We can. Great. Thank you.

Tamir Israel: I guess I'm here then.

Ayden Férdeline: So did you want to sort of get -

Brenda McPhail: Sure. So Tamir and I are going to sort of tag team just a little bit.

Stephanie Perrin: Just let me introduce Brenda who is in the room. Brenda McPhail from the Canadian civil liberties association.

Brenda McPhail: So very grateful to Stephanie and (Andrew) for having us here today. It's been a fascinating discussion. I have to say that it's difficult coming in as very much an outsider to what is clearly a tight community with sort of longstanding debates and discussions of which I have not been a part. So that sort of, you know, creates a risk of sounding naive and out of touch in this discussion. If I do, I apologize in advance.

To top it off, I am not a technologist. I am the Canadian civil liberties association's director of privacy, technology, and surveillance. And my remit is entirely social impacts around technology. So that's the perspective from which I speak. I just want that to be clear.

Really if part of the conversation before was about mechanism and not policy, I'm completely the opposite. About policy, not mechanism. And even beyond policy is the civil liberties organization. For us to comes down to principles. So we're – a two second version of what the Canadian civil liberties organization is. We're a non-governmental nonpartisan nonprofit organization. We've been around since 1964. So a long history in Canada.

And we do our work through legal advocacies. So we intervene in the public interest at primarily the Supreme Court of Canada but all civil courts. We do policy interventions and we do public education. So that's just sort of the framing of this perspective from me.

I sat in yesterday in the discussions about the transitional policies around WHOIS. And it was fascinating. Because I think clearly if ICANN is taking the position that has a - which it seemed to be yesterday. That it has a role in facilitating or enabling -- there was a debate about those words -- lawful access to who's data.

Then there's a really important question to engage in from our perspective if you are talking about standards or accreditation or audits or anything else. And the question of who a legitimate third party is? Who should have access? and I think that the list that (Greg) gave in another context of things that were predictable, rational, repeatable, and accountable apply to that as well.

We would argue that it's really important if you're looking at this kind of framework to do it in a rights focused rights centered way. And the rights of course that pop immediately to mind are the rights of privacy and due process. Stephanie actually made a comment yesterday that blew my mind a little bit. which is that the WHOIS system before it went dark and how I hate that metaphor.

It’s essentially could be characterized as a system of mass surveillance. If you are dealing with a system of mass surveillance, then you need - then I think it's actually delightful that the system is changing. And you have an amazing opportunity to change it in a way. In the context of GDPR, that all of a sudden can become more accountable from a human rights perspective as well. So that, I know, fly in the arrangement of ICANN.

To me, I see it as an amazing, you know, chance to change a system and make it better. In Canada, Stephanie had asked me to talk primarily about in our response to law enforcement access which is where we do some work. And of course, the civil society perspective to law enforcement access is that it needs to be accomplished within the law.

And this perspective is not just us as sort of a, you know, bleeding heart civil liberties organization. There's actually in Canada in particular very very strong support for this position. And I think as an outsider, another thing that can be helpful to do is just sort of bring the public voice who's not immersed in these issues into rooms like this. And the Canadian public is really solidly against an idea of lawful access that is over permissive. Or over broad.

So we in 2017 had a very significant national security consultation. It was a national, you know - coast to coast consultation. The number one issue that came out for citizens in Canada looking at access to information much more broadly. So than who is information of course. But access to information, personal information, by law enforcement, national security agencies was in fact privacy - respect for privacy and due process.

Participants actually said the challenges faced by investigations in the digital world should never justify circumventing existing rules and regulations. And that if anything in the digital world, they wanted to see more oversight and more safeguard mechanisms. I think the real - one of the most interesting results. Seven out of 10 Canadians actually indicated that they felt that their basic subscriber information so similar to the WHOIS -- name, phone number, home address, email address -- was as private as the actual content of an email.

And they wanted to send - more than four and five said they wanted to be able to expect greater privacy in the digital world or at least as high as they would in the physical. There was no distinction between digital and physical privacy. And they were all, you know- actually the stats were remarkable.

Primarily when you hear about the death of privacy to see how very united participants in this process were in demanding privacy in connection with law enforcement activities. We also have in Canada a relatively recent decision from the Supreme Court of Canada called (arbor sustentor).

As is often the case in these kind of cases, the facts are horrible. It was a person who was downloading and distributing child pornography who was on trial. But the police used - went to an internet service provider without a warrant to get IP information and basic subscriber information which they tend used to get a warrant to go search his house.

When the case went to court at the level of the supreme court, the court looked at the facts and under our charter, the section that protects privacy which is against unreasonable search and seizure, the court determined that because of the connections that could be made to the intimate biographical core activities of the person linked to that basic subscriber information that in certain cases there can be a constitutional right to privacy in that form of information.

That was a game changer sort of in the legal context in Canada. Law enforcement hates it. But the reality is now warrants are required for that kind of information. And ICANN deals with the global context. But we can't be the only country in the world that has that kind of legal limit on this information. So it's a piece of context when you are looking again at sort of a global standard. That's something to take into consideration. Tamir, do you want to kick in on some of the other bits and pieces? Are you there?

Tamir Israel: Yes sorry I was in a meeting. Can you hear me?

Ayden Férdeline: Yes we can hear you. Thank you.

Tamir Israel: Just to pick up from where Brenda left off. I think part of the historical reason why WHOIS has been an open system was because early on in the days of the internet, registration data and then identification data was computed as not very sensitive. I think that's starting to change.

We have worked the United Nations recognizing important anonymity. We have the supreme court decision in Canada that Brenda mentioned. And there's a recent decision from the European court of human rights that's very focused on a national regime within the EU. But it did imply that open access to subscriber data - without - from law enforcement in particular - without some sort of safeguards in place.

Maybe even perhaps a court order might be necessary is arbitrary and not consistent with the European human rights framework. So I think there is definitely a shift and justification for more. I think they'll view that - the open WHOIS that many of us have become accustomed to is in a way a mass surveillance system that does implicate privacy in ways that weren't necessarily anticipated when it was initially set up.

So there is definitely a justification for a more restrictive regime in place. And regardless of whether that regime becomes tiered and or layered for other entities in the food chain like researchers or even individual cyber security analysts, I think for law enforcement in particular there is a strong case that at least some identification data in some context should be behind a very rigid case by case assessment wall I guess. Maybe the best way to describe that. So just - so okay.

So, I think that's one challenge that is important from a civil society perspective to maintain especially since this is an emerging kind of recognition in the case file that and in many jurisdictions that this is a legal requirement perhaps to have some sort of official authorization for some sorts of online identification data.

The other one has already been touched on a little bit which is law enforcement means different things in different jurisdictions. And there is definitely law enforcement agencies that have both legitimate and important to these. But also some that might be considered infringing what are most widely recognized human rights.

I don't think that excluding or including specific agencies is going to work per say. Because even the - even agencies that have law enforcement tasks that we - that may be viewed from the United Nations perspective as implicating human rights. Will also have in addition to those legitimate roles that need to occur in some matter or another.

So you're going to need an avenue that accounts for all of these. And it's only the worse actors that are going to get excluded from the accreditation process itself. And excluding from data collectively. I don't think very much police agencies are going to get categorically (unintelligible) that way.

So I think I like the discussion earlier about drawing lessons from the mlaps regime. That does (unintelligible) entitled assessment for law enforcement. One is, you know, if a state's (unintelligible) framework doesn't necessarily align with another country's, you know, constitutional and human rights conviction, then they (Cannot hear him/her.) mlot agreement. But more frequently what you have is mlot agreements with many different types of policing agencies. But then a kind of case by case - a more rigorous case by case analysis is done. It's done on an individualized basis.

I think this is where the mlot regime attract some of its criticism. Not so much for the types of mechanism that are in place that you need to go through to get an mlot. But more because the volume of request that go through it and the amount of resources that many states kind of invest in their domestic mlot regime are not necessarily equal to the task of the volume requests they're getting.

So they don't get processed fast enough. But I think the core way of addressing with law enforcement requests in a cross-order context that symbolizes the mlot regime is simple sound. A matter of making it flow quickly. Ultimately then I think, you know, with this in mind a two-tiered sort of - well I shouldn't use tiers because we're using that term in many different ways. But I think in addition to deciding which having a mechanism for deciding which types of law enforcement bodies can access data at all.

There needs to be an additional mechanism that has more fine-grained assessment to ensure that data is being accessed in accordance with legal standards but also not in ways that would implicate human rights. So, we - Brenda and I were just discussing this a bit before the talk. And we were exploring the concept of data trust. As an EDM vehicle for facilitating which would be a lot of the mlot concerns.

So I'm going to just go through some of the features and processes that I think this data trust should be entrusted with. If it's going to civil society concerns in relation to accessing WHOIS data. And then Brenda's going to, if there's time, talk a little bit about what a data trust is. And why it might be an appropriate mechanism in this context. Does work? Sorry I'm also on a big of a lag so.

Brenda McPhail: You're good.

Tamir Israel: Okay, so a lot of the data trusts. I think the idea would be - I mean it would essentially be kind of like the WHOIS central depository. They -

Stephanie Perrin: We lost you. Sorry Tamir, you cut out.

Tamir Israel: Oh. So I guess what I was saying was the idea would be that the data trust would be essential depository that all the registrars would feed whatever criteria decided upon. It would enter the data trust. The data trust would have its own governance and its own criteria.

But some of the functions that it would be able to facilitate once all the data is kind of - it'll be accessible through one vehicle. It will be able to accredit - do the accreditation process for a body as well as other types of bodies if we feel the need for those. It will be able to do the cyber - the privacy and security certifications as well.

If people are able to come up with a certification process that is - that operationalizes some of the ISO standards. Because I know that many of those are sort of self-certified as we've mentioned. But I think it's possible to build a certification process around them. It would be able to conduct audits once we have -- As Stephanie mentioned audits are not helpful in S-track but once there is specific reference criteria in place it would be able to conduct audits if necessary on a case by case basis. Receive privacy impact assessments.

Again once there is criteria to assess in advance. It would be able to manage an anonymous contact mechanism. This is something that we use in our - in Canada's -- which is we're I'm based -- CCTLD's Sira. Sira does allow for anonymous (unintelligible) for some types of domains. And what it has is - it operates an automated contact mechanism.

So if I find out that, you know, goodguy.ca is sending out a lot of spam and I want to let them know that I'll take a look at their servers, I can contact them without actually needing to know, you know, who owns goodguy.ca. I can just use the portal and be like here's what I found. Contact me if you want more information. But we think you need to take a look at your servers.

And I think that takes care of at least of a - of volume of the considerations around, like, you know, losing people's email addresses if it the internet goes dark. It could control - it could conduct the analysis - the case by case analysis that would be needed in some instances to decide whether request are legitimate from accessing data from law enforcement for those that are deemed necessary.

It could also decide to do the processes that are deciding when that type of more rigorous (unintelligible) is needed. Like when a court order might be needed. Or where a more kind of rigid individualized standard of access would be required. So for example, where more sensitive data is going to be exposed. Like someone's personal anonymous blog about their, you know, whatever experiences in life.

As opposed to, you know, if it's something less - much less innocuous. Like I can't think of an example. But like a movie review site that has a copyright infringement (unintelligible) against it. Or I don't know. There is definitely tiers of access that are more or less rigid.

And the (unintelligible) could both decide what those tiers are. And also, you know, assess whether those particular criteria they put in place is met or not.

It could also operate in a API - and operator and kind of oversee an API based - not API based access. Apologies. But more like API based analytics mechanisms so that - and that would let law enforcement do broader based investigations where they're looking across several, you know - they don't really know what they're looking for but they kind of have the - still looking at maybe traffic loads or relationships between various domains that aren't very high level. But do it without having the entire database in their - like on their own server.

Which is where auditing safeguards would become difficult to manage. It could also - more generally monitor for human rights abuses by recipients. And maybe like oversee some sort of accesses suspension mechanisms. And it could set operation transparency mechanisms. And set as a vehicle for recertification if that becomes an issue.

So okay, those are the kinds of roles - some of the roles that we envision. A centralized entity like that being able to do - I think it would be difficult for every registrar doing their own thing under their own national laws and fielding international (unintelligible) and I think that would also allow for a way of doing the more tiered - sorry tiered is the wrong - maybe some combination of layered and case by case access for law enforcement without slowing everything down to a standstill.

But - and then the particular features of a data trust are being explored in a number of context where different entities are trying to figure out how to get data to the public in ways that don't rely on the historical models which have - are either giving them full access or having a very kind of selective process that isn't necessarily - that ends up being arbitrary sometimes. I think Brenda was going to talk a little bit about why - how data trusts work and the concepts and why they might be amenable to this kind of role.

WoAyden Férdeline: Feeling like we're out of time.

Tamir Israel: Or not.

Stephanie Perrin: Go ahead. We stole your time. So few people are not going to give a big long wrap up. I'm just going to say maybe we'll do this again.

Brenda McPhail: I mean really the idea of the data trust is an idea of guarding data with a public interest component. Which makes it seem sort of appropriate within the ICANN mandate. And also is a sort of umbrella structure that would include the concept of certification but include other, you know, elements as well. Such as, you know, the focus on human rights.

The ability for different stakeholders within the trust to take responsibility in a shared way for the Management of the data, the safety and the security of the data, the privacy of the data, the legality of the processes. So it would be an umbrella type wrap around. In relationship to the concept of certification. And the other, I mean the other piece that we would be very worried about with a straight up certification scheme.

From my perspective at least is that you wouldn't want a scheme particularly to the extent that it was self-regulated to take the place of other established legal mechanisms that are designed to provide privacy protection and data protection. So in particularly in relation to law enforcement, you really wouldn't want this kind of structure to give away to circumstantial standard protections that we have in place like subpoenas and warrants in particular. Because the information can be gained with less friction through a different system.

So the data trust would also be a structure within which that could be - you could (unintelligible) for that. It's an idea that was - that we're thinking about in Canada because it was proposed in relationship to a smart city project. The particular (extensiation) of concept as proposed in Toronto is highly fraught.

And we - it's not trite. This is not something that we've done. This is not something that we know. It's an interesting concept. I think (Andrew) might have some comments on this if there were time. But it's just sort of a thing to toss out there as part of this brainstorming process that might be a way to bring public interest into this kind of process.

Stephanie Perrin: Thanks very much. It's unfair to ask you questions like this when you've only been at an ICANN meeting for a day and a half really. But you might have caught the tone at the EPDP meeting yesterday that ICANN is offering to the central access point at least for law enforcement. Or at least they're not offering their investigating these possibilities. I don't think there's a whole lot of trust, not at least in our constituency for ICANN being a data trust. would this be workable? I wonder. If there was a data trust in each country, how difficult would that be for cyber security folks to gain access to the data?

Tamir Israel: Extremely. I think a centralized one would make sense. There's always the tones then of which jurisdiction it’s in. But if it has its own checks and balances much like ICANN itself, I mean you guys could tell us how that works or doesn't work. But that might be - I think it's actually better not to have it in every country in the world who's going to be a recipient of the data. That's probably going to be more problematic than having just one.

Rod Rasmussen: This is Rod. Just want to point out because a lot of the investigations that are being done often end up leading back to state actors.

Stephanie Perrin: And - Stephanie Perrin again for the record. This is part of our objection. At least my objection. I shouldn't speak for NCSD because we don't know the position yet. But this is why I think to have ICANN run it is crazy. Because they're trying to -- in a neutral and unbiased way -- run a domain name system globally. They therefore cannot start picking who they're going to trust and who they're not among nations in terms of giving access to data.

Tamir Israel: But then you can't do it at all.

Rod Rasmussen: I'm confused as to why would ICANN not be neutral - when would ICANN pick and choose it.

Stephanie Perrin: If ICANN were running the access point as opposed to registrars, they would have to make the determination as to accreditation of the lawful entities that were looking for the data and why. And if it was state actors doing the crime in the first place, then you're not going to give them access right?

Tamir Israel: I think the idea is - go ahead.

Rod Rasmussen: No go ahead.

Tamir Israel: I was going to say maybe the data trust would be set up by ICANN but run independently. So there would not be direct access. It would be set up and apply to criteria set up. I think that intermediary point is what lets you get around some of what might otherwise be a challenge to do it directly through ICANN.

Rod Rasmussen: And my point was that you have people all around the planet trying - doing investigations. They're going to have a bigger problem trying to get some sort of access from an individual country. Doing some sort investigation. And so, you know, you begin to have the problem of who gets access to what regardless. Even if you don't have an intermediary, you have that problem with the registries or registrars already. And that's even worse. Because you have it in that multiplicative way we were talking about which you can't scale to.

So, from a perspective of having ICANN play this role, I mean there is a lot of - its solves a lot of problems. So it should be I think, looked at. The question is around trust and how do you do that? And that’s where I would suggest that, you know, having the capabilities as a community to actually create policy n then enforce mechanisms for that policy is an advantage to be taking advantage of. Where you don't that capability within individual governments, you know, especially from the outside. If you're not in that country, you have no chance of really creating change or setting something up.

So, you know, don't throw out the ICANN idea just because of a trust issue. I think that can be actually dealt with. It's more around does this even solve the problem? And is it feasible?

Tamir Israel: So –

Brenda McPhail: Sorry. I'm going to go. Then you go. The idea of it being centralized as Tamir said as opposed to nationalized which was actually not our intent. That came up in questions. Would be ta ICANN would be a stakeholder in this but there would also be other participation from security researchers, from whoever the community is.

And this is a good place to sort of identify who the community is. Which means that some of the concerns that Stephanie is expressed and I admit I share after listening to some of the conversations yesterday about whether ICANN should be the only one to control this would be alleviated. It would be – there still would be a centralized process. But it would be slightly more open to participation from a group that is not closed and doesn't have the legacy of a commitment to everything being open all the time. Which I sense is a real tension in the conversations around GDPR in this community right now.

Patrick Fältström: So, (unintelligible) I think we all start to get a little tired. I suggest we're trying to we're not as careful with the wording now as we were some time ago. For example, I think we need to separate these various different kinds of sort of decision making that ICANN might do, for example.

We have the legal construct of ICANN according to the GDPR to be a data controller. That should be mixed up to where the data is stored. Which should not be mixed up with who is sort of vouching for another one to an entity to be trusted to not be mixed up with whoever makes the final decision of whether someone actually do have access. And all of those things are separate and must be kept separate.

And the architecture which I think which Rod says – I completely agree with him. That architecture only mounts the stakeholder discussion like the communities and ICANN can come up with, but we need to keep these things separate. And I don't see that one might not collude the other question if you try to keep things separate. I think what we must do in order to move forward is to keep them separate.

Rick Woodhelm: Rick Woodhelm for the record. Plus one to what Patrick said, very good point. I would also offer that one of the things about having ICANN involved is that one of the things that is – eliminates the need for trust is a contract. And contract of ICANN provides a contracting – contract anchoring point. And when Patrick and Rod were previously talking about the difficulties involving in trust. The kind of trust they were speaking about there frequently involves entities between which there are not contractual relationships. And they are truly trusting relationships. Where entities are sharing frequently. Not always frequently sharing data where there isn't a contract involved.

Patrick Fältström: That is correct. And I also – when I talk about trust, I also include the trust to actually go into contract because you still must trust the other party for not breaching whatever contract you're assigning. So we really talk about intermediate level trust issues here as well.

Stephanie Perrin: I was just offered the problem that ICANN is a monopoly so any power of a relationship in any contract with ICANN is not great. But like me and my phone company, I don't like them. I don't know whether they like me or not. But I don't trust them. But I don't have any options, you know?

Rod Rasmussen: Yes, I think the analogy is tempered by the fact that you do have government oversight, in theory. And with ICANN, in theory we have community oversight and could actually as a community work together to address that which is fairly unique. So I think there is some – yes, the fact that we've created this bottom up stakeholder process manages to come to our advantage here in solving one of the issues we all have.

Patrick Fältström: And regarding contracts. Remember the CC's are not contracted parties.

Stephanie Perrin: Thanks. Thank you very much and we really appreciate you spending the time today. We're all triple-booked. But it was very interesting. Ok, Tamir are you still there? Any thoughts on this? Maybe not. Guess we lost him. Tamir? He's disconnected. Oh dear. Oh well.

Well, I think it falls to me to thank everybody. The folks who are still in the room, thank you for your tenacity. I think it was a very interesting day. I think we will probably be doing a summary and if anyone is interested in continuing this, we could probably do it at the next ICANN Meeting. Maybe not all of this, but some of this. Because we will be proceeding with some of the standard activity that I talked about. It's not of course clear that standards are the answer. But we have to keep working on it to see what might be useful.

So if anyone has any final thoughts? Okay, well thank you everybody for their flexibility. Particularly Brenda and Tamir who kind of got pushed to the end. I'm really sorry about that. But I wanted you to also have heard everything before you got to talk. Tamir, you're back online? Any other thoughts? No? I guess not. Okay. So, anyone else? Any other thoughts? Aiden? Well, thank you very much for moderating by the way before I –

Patrick Fältström: It's been my pleasure. Thanks for staying through to the end. And thank you Stephanie for all the work you've been doing on this project almost single handedly.

Stephanie Perrin: Yes I was whining about the lack of enthusiasm earlier but I’m really really gratified with the interest jump today. So that’s great, thank you.

END