# ICANN
# Transcription ICANN Panama City
# GNSO: RrSG GDPR: Tucows' Lessons from 1 Month into Tiered Access
# Wednesday, 27 June 2018 at 09:00 EST

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
http://gnso.icann.org/en/group-activities/calendar

Man: It is Wednesday, June 27 at 9:00 am. This is the GNSO RRSG GDPR Tucows "Lessons from One Month into Tiered Access" at 9:00 am at ICANN 62 in Salon 7.

((Crosstalk))

Elliot Noss: Hello everyone. Thank you for coming this morning. While we're working out a little of the AV, you know, I'll share a couple things with you I think. The first is that I really encourage people in the room - you know, I'd like to make this as interactive as possible.

So I encourage people in the room if you have a question as I'm going through, that is what I would call an "I don't understand" question, then please ask it. I'm going to try and leave some room at the end for questions that are more, let's say conversational or interactive.

But usually if somebody in the room has a question that is of an "I don't understand" nature then there's another ten people who have that same question, so I'd really encourage that. Zoe you want to just give it a go with where we are?

Zoe Bonython: (Unintelligible).

Elliot Noss: Yes. We apologize for this. The deck is on a PDF right now. So the production values will suffer but hopefully the presentation won't. Thank you.

So I wanted to start right - Zoe the one other thing I'd ask you is as much as you can, could you just go to kind of the line? Leave the top slide as opposed to centering it. Do you follow what I mean? No, right, right. You want to kind of - right. Yes, as little of the next slide as possible.

So I want to start with this quote because it's sort of framed the way that I'm viewing the challenge that's in front of us all. So this is a quote from Techdirt and it was about - it was in an article about our litigation with ICANN.

Because it's Techdirt, you know, it contrasts with security researchers. We could substitute law enforcement for this just as easily. And, you know, the point that I really want to draw out with this quote is that this is about balancing rights. This is not about whether rights exist in any sort of binary fashion.

You know, as I was doing this, what became clearer and clearer to me was that, you know, it's a challenge on both sides of this issue for all of us to move from what we've been doing for 20 years with WHOIS, you know, which is kind of taking binary positions and then, you know, being entrenched in them and move to recognizing that this is about compromise.

And in that context, either side saying, "This is what I had; this is why that was good," really just doesn't serve. Thank you. Next slide.

The next thing I really want everyone to hold – you know, this is a process that we're in together – is that this is the beginning. And a big part of that challenge is going to be because we were somewhere. You know, if you think about WHOIS and you think about the ecosystem that had built up around WHOIS, it is an adult.

You know, I was around very much, in fact responsible in some ways, for what I would call the alpha of all of the robust WHOIS tool sets that are out there today. Those tool sets have had 15, 17, 18 years of iteration now. They are an adult. We are starting again.

And so I think when people have frustrations, and they will, on all sides of this issue, they need to remind themselves of where we are. So next slide.

So tiered access is live. Now this is our Web site, TieredAccess.com. It's not working yet. You know, we were busy with GDPR implementation. And now we have started to turn our turrets towards this problem.

You know, ideally - and I would be sympathetic with people who have frustrations who say, you know, you should have been ready with this for GDPR. It just wasn't possible and I wish we were too. I think, you know, you want to imagine that as in the building.

You know, me saying "why aren't we ready," we would have liked to as well. But this is where tool sets will be built out. There is tiered access available today. Some of you have applied. Not very many but that's understandable. Next slide.

So I want to contextualize where we are with some data. Next slide. The gTLD space very typically – we're just going to play with big numbers because people hate math – has a 70% renewal rate. That's certainly lower in the new gTLDs, higher in the older TLDs. But, you know, this is an important frame. Next slide.

That means that we are degrading the historically based tool sets which relied on, you know, from my perspective stolen data at the rate of 2-1/2% a month. So what that means is where we are today one month into GDPR implementation is the tool sets that those who like and want and need tiered access are using, are still 97-1/2% accurate.

If I was any of you, that's what I'd be using is those old tool sets. You know, I talked yesterday about that being about 7 million domains a month. That's 7 million domains in the context of 330 million domains.

And what's helpful to me as an analogy here is browser compatibility. If you have a cert, a digital certificate, that has 97-1/2% browser compatibility, you've got a business. Next slide.

But if you have a digital certificate that has 70% browser compatibility, you don't have a business any more. That digital certificate borders on worthless. So after one year, that data set, the historical data sets, are going to be only 70% accurate.

I think that that frames our challenge here and, you know, again those data sets are based on stolen data so that can't be all in a bad thing. But it does set our challenge. Next slide.

After two years we're at about 50%. Next slide. And after three years, 35%. And I think that that - these are all numbers that we need to keep in mind in framing our challenge. Next slide.

Now I want to have a little bit of a discussion on something that we haven't seen but that we don't talk about in this community, and I don't think we've effectively talked about it in this community for 20 years. I must say that in preparing, you know, lots of us have talked about little bits of this. Yes Rich.

Rich Merdinger: Rich Merdinger. Elliot, I apologize for interrupting.

Elliot Noss: No, no, if you weren't here at the beginning I encouraged that for don't understand questions. Go ahead.

Rich Merdinger: I'm curious about your degradation numbers. And do they include simply the lack of renewal or do they also include registrant change/transfers, et cetera?

Elliot Noss: They don't include those things and I didn't have a rate for that.

Rich Merdinger: Right.

Elliot Noss: You know, I wanted to just - that's a great point. That degradation rate is going to be even greater. And, you know, anybody who's - because I think we should all be working with real numbers. We should all be shooting with live bullets.

So anyone who can, you know, take a swag at that data or provide accurate data in that regard, that would be fantastic. In fact, you know, the folks who run the degrading tool sets are the ones who would have the most accurate information there and they should provide it to us.

So I want to talk about damage. And this is damage that a free and public WHOIS has cost us. I was really struck in preparing for this presentation how we have done a terrible job of communicating this in a formal structured way. Next slide.

Because I think this is the nature of these dialogues. You know, I just threw this in because this is not a problem that is exclusive to the ICANN community. The balance and the challenge in finding an effective balance between security and privacy is present in many, many other industries as well. Next slide.

So, you know, here's the first big block of damage we all - anybody in the domain name industry who's been around for any length of time has seen these. This is a DROA scam renewal notice. This is a very lucrative business that has existed now for about 14 years.

We're aware of that because right at its onset these were resellers of ours that we kicked off the platform pretty quickly. I couldn't give you even a guess as to the magnitude of individuals affected and dollars defrauded based on this range of scams, the fake renewal scams. And this hasn't stopped. Next slide.

You know, here's a ripped out of the headlines article from Domain Name Wire from a week ago. So this is still going on today. Next slide.

And that's one category. Second category of big generic scams are SEO scams. You know, anybody's who's registered a domain name would have seen these hit their inbox. You know, you've registered a domain name. We're going to get you on the top of the search engines.

These are very often shady and scams. And I'm going to talk about the continuum of, you know, what I'm calling scams and, you know, sort of what's right or wrong here in just a few slides. Next slide.

Of course we all know – what would I say – less harmful. Just takes a second to delete it. Way more prevalent. Anybody who's registered a domain name and has provided a public e-mail address has immediately not only been inundated with spam from that registration and at that time, but their e-mail address goes on the big seed lists and will be sold forever more. So it does not go away no matter what you do. Next slide.

And, you know, something that's been more prevalent in the last five or six years, you know, we've fought lots about having to have phone numbers that were working in public around, you know, when we're talking about WHOIS accuracy.

And anybody who's registered a domain name has now been inundated with calls probably in the tens, maybe hundreds, offering things like tech support and real estate services, you know, and, and, and, and. And, you know,

again one of the hardest sets of problems to deal with are those problems where you have, you know, small deeply interested interests and the damage is diffuse.

You know, damaging tens of millions or hundreds of millions of people by wasting, you know, 5 or 10 or 15 minutes or 5 or 10 or 15 cents on their cellular bills is tiny and diffuse. But it is a huge loss nonetheless. Next slide.

And here's something that I don't remember us ever talking about in this community. You know, we have seen the organic development of rich, robust tool sets. Those are - I've played with them. They are very powerful data managing and slicing tools.

Far as I know, there is no jurisdiction in the world that has "know your customer" legislation or requirements or anything for those tools vendors. We all know that cybersecurity and cybercrime is a cat and mouse game that has been going on and never stops. It just iterates.

We can be - and I think we all know anybody who's on the cybersecurity side well knows that cybercriminals are not stupid. They are clever and they iterate. We can be sure that lots of them are also customers of these tools.

So it's great that a lot of people – certainly the people in this room – are using this data for positive purposes. But we also need recognize that extremely high likelihood that there are thousands of people who are using this data and those tools, which you've all contributed to developing and are customers of, for nefarious purposes.

And I want to talk here about the continuum between good and bad. You know, we could walk down a continuum from, you know, law enforcement probably on the one end to pure cybercriminal on the other. But boy, in the middle there, there is a wide swath of ad tech.

Somebody's personalizing ads, probably not so bad. Drive-by downloads that hijack your desktop, really painful. And then using data like this potentially to alter an election, fundamentally need be dealt with.

So I just - you know, there is such subtlety and gradation in these interests and along this continuum that we have to recognize, despite all the costs and all the need to balance, that taking this data private has a fantastic outcome in regards to cutting off sources of data for the bad guys. Next slide.

This has clearly over 20 years cost billions of dollars. Next slide. This is so much better if I'm tapping myself, so I apologize for that. Millions of hours. Next slide.

And now we're seeing that degraded at 2-1/2% a month. So every month with all of our frustrations – and believe me, people who want tiered access, you know, it's frustrating for us to not be able to provide it in the way that'll end up being provided – we are getting benefit at the rate of 2-1/2% a month, and as Rich points out, even greater. Next slide. Next slide.

One back. Sorry Zoe. I'm probably going to have to do that a little bit. You know, I do want you all to know that at this point, and this is - you know, what I'm going to say next has been checked with a number, a pretty broad number of our registrar colleagues. We are not seeing applications for tiered access in any volume.

Now I should qualify that by saying we weren't seeing that in any volume. And by the way, yes we've got about 25 million domain names on the platform. You know, we saw sub-ten applications until I guess people were preparing their sound bites for this meeting, during which all of a sudden we had over 100 primarily from one party which was then used to present data publicly this week.

So what I want to point out there, you know, this ties back up into that 2-1/2%/97-1/2% number. You know, we have time to improve these tools now. And I don't know a registrar who's not - registrar here representing, you know, the significant majority of the registrations in the gTLD space whose not similarly minded. Next slide.

One more, sorry. So, you know, really this is just when we sort of look at where we are. Now I want to do a level set and take us into tiered access. You know, this was a historical anachronism that provided public information in a way that was unique to this industry.

You know, we have many lines of business. They are as connected to regulatory frameworks as this one is. And there's of course no requirement for personal data. And think about that for a second.

You know, can you do more damage with a domain name or a home computer connection? Can you do more damage with a domain name or a cell phone? I think they're arguable but I think you can do damage with all of those things. You know, hosting is another example. Next slide.

This has not been driven by our policy. This has been driven by law. And I think we all need to remember that whenever we get into a frame of negotiating. You know, sometimes in some of these discussions to date, what it feels like is people are negotiating as if this is a give and take when on, you know, the side of the contracted parties, this is about law and compliance with law. And that's just non-negotiable.

We can have a robust discussion about interpretation. We can have a robust discussion about what we can do about it. But we can't negotiate law. Next slide.

This is what you see publicly for our output. You know, on the left there you see a standard registration. On the right there you see privacy protected

registration. I'll talk a little bit more about privacy later. And the next thing that - no I'm just going to go to the next slide.

You know, historically, privacy has played a particular role in this industry. So, you know, if anybody wants to question whether there was damage in public WHOIS, you need just look at the existence proof as the fact that the public is willing to pay tens of millions. You know, there's no Forrester or Gartner report on the size of privacy and domain registration.

It's at least tens, potentially hundreds of millions of dollars a year just to keep their information private. Historically we had an approach to when we remove privacy. So that was clearly notice of litigation or UDRP. That's in our terms of service. That is not my chat. Somebody's got a really loud chat.

And, you know, just that's in our terms of service. So, you know, if this privacy is being used to protect somebody doing something bad on its face, we just expose them. No questions asked.

The second point is the more interesting one here. You know, because we would remove with a reasonable belief of wrongdoing from a named party. In other words, a particular party who would identify themself (sic) and say, "Here is evidence of somebody doing something wrong with the domain name."

We have a standard. It's - you know, with any reasonableness standard it develops over time. And, you know, you have internal precedents that you use. And yes those are fragmented and uneven across the industry. PPSAI was intended to deal with that.

I think that what happens now is that that standard of reasonableness becomes a little lighter. With GDRP there is much more privacy per se. So people who will continue to pay for privacy services are those who really want it in a more extreme circumstance.

I don't want to say extreme circumstances because there's still lots of reasons you would want privacy. And so now that membrane must become a little more permeable. It must be a lower threshold. I don't want to say slightly lower or much lower. I have no idea what that looks like.

And it's going to be, you know, one of the many examples you all heard me repeating over and over and over again. We're going to see what happens in the field and it's the only way this can get dealt with.

You know, and I do want to - I'm going to jump out of the privacy piece for a second because I do, you know, want everybody to understand that what we are stuck dealing with is a very difficult challenge that is akin to constitutional interpretation.

And by that I mean, you know, the GDPR isn't a law as much as it's a constitutional document or a statement of principles. The only way we can know how those principles should apply to our industry is by putting fact tests against them.

And then bad news for all of us, particularly for contracted parties. We're going to have to make interpretations. Those interpretations may or may not be consistent with what the courts eventually decide. But we've all got to give our best efforts here.

And I say all this to say in that context it becomes so important for us to take specific situations, specific fact sets and test them. And by test them I mean deploy them and see how that works in the field. We have no other choice. Next slide.

So when we're also talking about tiered access, we wanted to narrow the discussion by saying, you know, here are the nots. So some of these

categories here are things where WHOIS was used previously but that none of them are things where WHOIS data need be used.

We're already in dialogue with certificate authorities around alternatives to the way that they vet domain registrations. You know, it's a great example of a - you know, it's a great example of, you know, people are faced with change. They have no choice. They adapt. We adapt.

You know, one of the – no, not one of the – the defining characteristic of the Internet is its organic capability. The Internet does not roll over change. It routs around it.

And so here you just see, you know, these are all great examples of things that WHOIS was used for previously that it need not be any more. And again all of these are already being - these are all things that are kind of being worked on and are in the field. Next slide.

So we call our tiered access TACO. That's just Tiered Access Company. So I want to - you know, here's really the meat of this discussion. And I'd encourage - now I'm just going to - you know, I thought about doing pretty pictures for each of these points. And if I would have known this was my sort of slide format I probably wouldn't have done the previous ones.

So with each of these, you know, I do want to encourage questions as we go along. I think we've got an hour. Is that correct?

Man: Hour and 15.

Elliot Noss: Hour and 15. So, you know, we're going to start to get interactive here. I want to, you know, talk about each of these, tell you about them from the perspective of our position and our initial implementation. And then, you know, we can talk - you know, I think that it's good to start with questions.

And, you know, we'll just be able to just open it up broadly at the end. So first is different classes of service. I think we all know the three broad categories. I did mean to include a link to a blog post we did on this. It's on the open SRS blog. I think it's June 19.

I know that some in the community were starting to share this yesterday. It describes what we're doing. Apologize for - maybe I did throw that link up. I forget. Anyway, the first is different classes of service.

So there, you know, it's again there's nothing surprising. That's primarily law enforcement that is the security community and that is litigation that's commercial litigation. And I don't say IP there because I think that's too limiting.

I think WHOIS is used for a broad range of commercial litigation. You know, I think that just, you know, we in this community are dealing with it so much in the IP context. You know, so I've really been encouraging people internally to, you know, think of commercial litigation.

And I do that so that they can do their jobs in our compliance group more effectively. You know, they see something. It's not an intellectual property matter. You know, does that mean that's outside of what they should be considering? Well no. So those are those classes. You know, I don't think there's much there.

The second one, you know, I gave this a quick call-out on the panel yesterday. But I think this is huge. And when I say huge, I expect that for the next six months for sure and with a tail that's probably going to be going on five years, this is going to be painful.

So when I talk about a long tail like that I want to make sure you understand that, you know, there's a whole range of people. Could be law enforcement. Could be commercial litigator or intellectual property (czar) who deals with an

issue that relates to WHOIS, you know, once every few years in their practice.

So for those people, you know, oh I did this six years ago. Here's what they did. They try and do the same thing. And I promise you, you know, if I could add up all of the hours that our customer service compliance people, others in the organization - because let me tell you when a lawyer hits the main switchboard they just button mash and take whoever they can get and start yelling at them very often, you know, with a, "Do you know who I am?" approach.

So you're going to have that loss of anonymity. Be incredibly painful. We also as an industry have wrongly cemented a view that using WHOIS is anonymous. Complaining about WHOIS is anonymous. So we've allowed, you know, kind of the, you know, this is the permeable wall and there's contracted parties providing WHOIS over here and there's a community using it over here.

You could do anything you wanted on this side, completely anonymously. We have a WHOIS complaints industry in our community. I would love to hear the percentage of compliance hours over the last five to seven years that have been spent dealing with WHOIS complaints.

And by dealing with, I mean attempting to enforce them against registrars. And when we've complained for years that people were abusing the system and that people were clearly doing it, you know, outside of the original purpose, the answer we got was that's what the community wants. Go and change it in the community.

Try and get that PDP through. Anonymity is going to be painful. The first time I promise you for each of you in this room who wants tiered access and uses it for good purpose, the first time you're asked to identify yourself it's going to be frustrating. And it's also necessary.

Next one won't be quite as painful as anonymity but it will hurt. We require today reasons. Why are you making this request? This isn't a ten-page submission. This is a one- or two-sentence summary of a category. I promise you as we all evolve this together, we're going to develop a set of standard reasons.

We're all going to know what they mean. We're all going to know what fits into them. We're all going to know what doesn't. But that will take time as well. I think in six months we'll get 80% of the way there or some significant percent of the way there. We'll deal with all the hard cases.

The next year maybe, you know, we'll probably have that last 20% and knock off another 10%. And that last 10% again we might be figuring out for five years. That's going to be the nature of this beast. Whether we have a successful policy process that takes, you know, a year, which I am hoping and praying for, whether we have one that doesn't and takes two or three or five years, these things will get solved and they will take time.

Next one is again going to be painful. Need to establish agency. What do I mean? We get requests - if you think about, you know, we see this already, you know, in the very few number of requesters that we've had.

For us at this point, you know, we need to know that a lawyer represents a particular client. We need to know that a security consultant represents a particular company. We have no knowledge of that. We cannot be expected to know that.

That is going to be painful. And again that is just going to be a process. This one, the need to establish agency, I think does get smoothed out overwhelmingly in the next six months. I think all of you who do this on a regular basis will quickly have canned solutions to this. You know, letter from client that's, you know, sort of a demonstrable establishment of agency.

I wanted to - you know what? There's something I forgot to add I see on this slide, that in our launch implementation there's a separation between access to the system and using the system.

So the first thing you do before you do your first request, before you make your first tiered access request, is you qualify as a requester. That is fee based and rigorous. So what do I mean?

You know, you say I am law enforcement. I'm not going to deal with that case because it's probably the one that gets solved first in the field. You say you're a cybersecurity consultant. I'm not going to deal with that case because it's - just in this session I mean. We have to deal with it in the field. We have no choice but to deal with all of this stuff, sadly. Anyway.

And I won't deal with the cybersecurity side because I think that's going to be the most complex and the one that's going to take the most work for all of us in the community. And I want to make sure that everyone here hears me signing up for that work because I think it's really important.

But I'll talk about that sort of middle case around lawyers. So there you need to authenticate yourself. Here's who I am. Here's my jurisdiction. Here's my address. Here's my phone number. This will depend on jurisdiction but here is my legal qualification.

These are all things that when we're authenticating you and issuing you access to the system, we will check. That is very important for the integrity of this system. Then once you have access to the system, now you have some of the gating that I've already talked about around requests. So need to establish agency.

You know, again, I think in six months a lawyer who's qualifying for the system is going to come in. They're going to set their access. They'll

establish their access and they'll probably provide us with a canned solution. Here's all the clients I'm representing, so that we now can create a data set that we can refer back to whenever they're making the specific request.

And with those - you know, when I'm talking about solutions that are going to evolve in the market and I'm talking about them, you know, we'll get a long way down the road in six months and there'll be pieces of it trailing five years. Let me tell you the biggest difference between six months and five years.

That'll be the willingness of the people in this room and in their broader communities to communicate that information, to share that information, to iterate on that information. The more intransigent people are, the longer that's going to take. The more solution-focused and the more cooperative people are, the shorter that's going to take.

Next one. Transparency in reporting. So we are going to - there's no question by the way, this is not talking about privacy. So now I'm talking about metadata. The integrity of the system depends on the integrity of the system. How many requests are being made and the categories that they're being made in is all useful data to share.

That metadata that comes out of what I imagine in the transparency and reporting – and there are discussions happening in the community now about this on the non-commercial side – the data that comes out of that I think will help us at a policy level broadly because, you know, this is pointing to the prevalence of, you know, problems in the DNS.

You know, the transparency in reporting that can come out of this GDPR process and us all working together can really get us out of think of the children and, you know, doxing to death and, you know, each side just talking about the ills that they experience.

There are a couple other elements in this. You might lose your credentials. How might that happen? Well I'm a lawyer. I'm in a firm. We believe that this need be individual not entity based. We do not subscribe to corporations are people. We think people are people.

And I'm a lawyer and I share this with my colleagues. And believe me things like I don't want people to freak about, you know, we're a thousand-person partnership and how are we going to authenticate each person. We're going to have to work that out. Of course that's going to roll into pricing.

Of course that's got to be reasonable. But I share it with my partner who represents different clients that we didn't know about. I'm some other party with tiered access. I'm a lawyer. I'm a law enforcement agent. I'm a cybersecurity researcher. And I share it with my buddy who's a real estate agent. That now need be policed.

When I talk about and more, you know, that's the Mike Palage, Philly Special, fines on the other side. I thought, you know, Mike's comment yesterday around fines as a forcing mechanism was incredibly accurate. You know, we can look at - you know, you can connect data points that are deeply embedded in our community dialogue.

You know, Stephanie talking about repeatedly - I think it's 127 different pieces of security legislation around the world. This one has a fine and it's significant. And look at what that did. It took a 20-year intransigent battle and here we are now working it through.

So I think that that part of it, you know, is certainly not a launch piece for us, but I think it's naturally going to be part of the system.

And I want to be explicit about this last point on this slide. You know, I like to think out. I like to think a year and three and five years down the road. I like

to pull myself up from, you know, today's battle. This is really going to suck for the security community and particularly around security research.

I just feel like that transition from where we are to where this is going to get to is going to be the rockiest for that group.

And I think that that group is so heterogeneous that we're – we might have two or three or four different sets of solutions, you know, cybersecurity consultant, cybersecurity government entity, a cybersecurity researcher at an educational facility.

You know it is so complicated so I'd really – what do I want to – all I want is to – for all of us to hear that, for all of us to be sympathetic towards that, for all of us to recognize, you know, we don't have the luxury of ignoring our problems now.

And for all of us to recognize it there's just a boatload of work that needs to be done there. You know, and I want to say that in the context of being able to say, you know, "Boy that work is important from my perspective."

You know, I am not a privacy advocate. I am an open Internet advocate. I am a healthy and strong Internet advocate. That's my center of gravity and I know all the good stuff that goes on there.

You know, we work with cybersecurity folks every single day. We have to in our seat and it's going to suck and there's nothing that anybody, you know, you can yell at ICANN.

You can yell at regulators. You can howl at the moon. Nothing is going to change that. Next slide. And this is my last slide and I'm going to open it for questions after this.

You know, I hope that - you know, but yesterday when I was just making little call outs and today when I've been trying to contextualize my thinking around the need to work together, that you all can appreciate that, you know, this really is going to be something that, you know, is such a "made history."

So by that I mean every time we do something constructive in this particular process we're going to be shortening the timelines to efficiency. Every time we do something counterproductive - and the things I identify as counterproductive are shaming, are win/lose advocacy, are binary arguments.

Tiered access is good. Tiered access is necessary. Every time energy goes down that road it just lengthens the process because all it does, you know, there can be some people who can hear those arguments and step back from them.

But there are some people – it is the human condition. We see this in politics all over the world right now who will just bark right back, and then you're going to have a chunk of energy just going into two dogs yapping at each other.

So this is really a made history. I deeply believe – first of all I deeply believe in multi-stakeholderism. I deeply believe we are on an inexorable trend in a direction.

For me 20 years from now when this history is told/when we look back on it, it's going to be this particular process that is going to mark the change in direction.

And with that I'm going to open it to questions. Zoe you have the first – oh I have one more slide? Yes. No I have one more slide. I was fooling.

((Crosstalk))

Zoe Bonython: Do you have another slide? Well actually…

Elliot Noss: Yes sure, that's what it is.

Zoe Bonython: …I have questions from in the AC room.

Elliot Noss: Let's – show it to me.

Zoe Bonython: I don't – yes I don't think you have another slide. There's nothing. Just questions I have.

Elliot Noss: Do you have – question?

Zoe Bonython: Not personally. I understand everything. So our first question is from John McCormack and that is, "What is the minimum data set in WHOIS that is or will be available without talker?"

Elliot Noss: That's the one that we showed on the earlier slide. I apologize if the slides weren't there.

Zoe Bonython: Yes I apologize for…

((Crosstalk))

Elliot Noss: Yes so I think the slides are posted and available, you know, and so I wouldn't suggest just sort of running through it. It's way at the beginning and it's a preview document, so that's a pain in the ass but that slide is there. You can see it or you can just go look up a name today.

Zoe Bonython: Okay the second question is from Bonnie Mtengwa. "Are you also pushing in place measures to make sure the information that LEA wants to access on your system is genuine?

If there is – if there are processes to vet LEA are there processes to vet information provided by domain registrants?"

Elliot Noss: Well see, you know what? Right away – and I – it was Bonnie?

Woman: Bonnie.

Elliot Noss: Bonnie. Yes.

Zoe Bonython: Yes.

Elliot Noss: I apologize in advance. I want to call out that the tone of that question, you know, is if you're doing this then why aren't you doing this. I think that's the wrong frame.

It's totally a fair question. What are we doing about WHOIS accuracy? But to put it in the frame of, you know, "Well you're doing it here. Why aren't you doing it there?" is just wrong.

And so I do that – again Bonnie I apologize in advance. That's what we've all been doing for 20 years, I'm sure me included, in transcripts on public records going back to, you know, whenever but we all have to stop.

So are we doing that? There's nothing different that's being done around WHOIS data collection today from what's been done in the past. You know, I think that - and what we can do there is, you know, we have a pretty robust regime right now for inaccurate WHOIS.

That's followed. People regularly lose their domain names because of inaccurate WHOIS. So right now where we are is a fairly robust, definitely imperfect regime for vetting WHOIS data and we're at Step 0 in terms of vetting requesters.

So, you know, I think that there's going to be a lot of work that goes on on the requester side, you know, before we start turning our minds to the other question and it's a fair question. To the mic.

Ching Chiao: Thank you Elliot. This is Ching Chiao from Brandma for the record. Thanks for the presentation. I think…

((Crosstalk))

Ching Chiao: …another question for me but the experience sharing…

Elliot Noss: That's great.

Ching Chiao: …based on what you just mentioned - from the security standpoint of a corporate client and that I'm helping with is that - because of past five to ten experiences of their names got stolen for any reason.

So the corporate clients for – once again for the security purpose now these day they would like to get a copy of their WHOIS data from different, you know, registrar just around the world.

So I think one of the thing I'm seeing here is a good, stable access, you know, the client that they are able to see their digital assets being managed well by each individual registrar, you know, based on their WHOIS, you know, I mean, information so just to share that.

Elliot Noss: I think that's great. I think there's three things that that actually calls out for me - one that I should've probably mentioned in the answer to Bonnie's question.

You know, I deeply believe that just by doing what we've done with GDPR, taking WHOIS dark, creating the start of – very start of -- remember the baby

slide -- tiered access, we're going to start to also get more accurate WHOIS data.

The overwhelming incentive for inaccurate data goes away and that will become very interesting to watch over time. Like the second point that I'd pull out of your comment is around fragmentation.

I again think the better we work together, the faster we move along the continuum around each of these five or six or ten different pieces of work, the more we start to isolate and make clear, you know, the common number one lament from business interests/IP/law enforcement.

You know, it's not you guys who come to the ICANN meeting. It's these other bad registrars. I think that all of this process is going to serve to make clearer/shine a brighter light on who those bad registrars are.

Ching Chiao: Can I quickly…

Elliot Noss: Yes.

Ching Chiao: …ask two?

Elliot Noss: Please.

Ching Chiao: I – so I love the taco – the idea. I even first, you know, what – as I see this maybe like a source, I mean, open source code kind of a project so I'll be happy to help on that.

Elliot Noss: Oh awesome.

Ching Chiao: If you can throw this through a gate lab and then we can have our engineers to look at it and…

((Crosstalk))

Elliot Noss: That's sweet. You know, so the two thing - so first, thank you. Second, I now get to do my second congratulations. You were the first one to formally offer your assistance.

Thank you very much for that. And third, you know, we kicked around as we were rolling this out – no I shouldn't say that. That's unfair to the people in the building.

I kicked around before we rolled – before we kind of got to where we are today I kicked around just offering this for free to other smaller registrars. I deeply appreciate that, you know, boy if you're a small registrar this sucks.

This is terrible. You know, it eats up so much engineering time and people just don't have it and that – that's kind of a finite resource, you know, and so we kicked that around.

And it was just simply the overwhelming amount of work that we had to do with GDPR compliance for May 25 really precluded, you know, anything other than me being able to say, "Hey this is a great idea.

Should I call some people?" you know, because that's the, you know, classic CEO. Just sort of throw the pile in the center of the room and leave people to clean it up.

So that, you know, that kind of turning this into – turning this piece into more of a community effort. You know, it has some centralized elements because there's governance.

There's rules. There's fees, right, so, you know, but working through some of that stuff is great. Thank you. (Colin)?

(Colin): Hi Elliot. Thanks for your presentation.

Elliot Noss: Hi. Thanks.

(Colin): Things are moving really fast and that's scary but it's also quite exciting because it gives us…

((Crosstalk))

Elliot Noss: Yes it's a roller coaster.

(Colin): Yes because it gives us an opportunity to make new tools. And I really subscribe to what you were saying about the need for collaboration and for multi-stakeholder involvement and to produce kind of binary or opposition relationships.

So this won't – this might not surprise you but I'm really interested in transparent reporting so I just wanted to underscore that I think this might be only one of the many opportunities for the private sector, for NGOs, for academia and maybe even law enforcement themselves to come together to build a new framework or to mimic best practices in other sectors.

Elliot Noss: Yes.

(Colin): So I just wanted to underscore and maybe hear your thoughts about that.

Elliot Noss: My thoughts are simple. You know, you're the one who's doing the – you're leading the transparency in reporting work right now so kind of we are as a community wherever you are.

And so, you know, just let me give a shout out to that work and, you know, that's the, you know, kind of the seed or the germ of, you know, where we'll get to.

So – and, I mean, I say that if – I apologize if there are others in the community who are doing that work now. It's the only…

(Colin): Fine team.

Elliot Noss: …body I know about. Yes.

(Colin): We're doing that work. Find me.

Elliot Noss: Yes. Yes that's great.

((Crosstalk))

Elliot Noss: Thanks.

Ching Chiao: Just one…

Elliot Noss: Zoe you got – you have one? Yes.

Zoe Bonython: So I have – first of all I have a comment from Benjamin Akinmoyeje from Nigeria. "I just checked my WHOIS on one of the Web sites I registered. All of my data is available to the public."

Elliot Noss: Yes that's…

((Crosstalk))

Zoe Bonython: There's too much data.

Elliot Noss: Yes. Well, you know, what would I say? I don't know the privacy laws in Nigeria. I don't think that's a GDPR violation because he's in Nigeria. I don't know. You know, please ask a lawyer.

But I think that that start – some of the unevenness that we're going to start to see. And I want to – Thomas or Zoe just before I go back to you I am worried because I'm not seeing enough IP and LEA folks asking questions.

Steve I don't know that I've seen you, you know, sort of less in the line and a chance to make comment and that worries me because I really, really need us all to be in this together. So yes guy – I'm going to skip you Thomas for a second and go to Margie.

Margie Milam: So thank you for this presentation. I think I can share a little bit of what's been going on at Facebook since May 25. We as you know are a very large platform.

We represent millions of users that come to our platform and it's first and foremost our responsibility to protect the integrity of our platform. So since May 25 we've been sending a – notices to registrars to unveil the who – full WHOIS record with respect to domain names that incorporate our major brands.

And we've received mixed results with that and it's in the neighborhood of about 50,000 that we're currently working through. So this – even though it has been staged in the sense that we haven't had the ability to send them all at once because of the change in procedures, it is something that we're actively doing as part of what we need to do to protect our brands and our platform.

And so part of the frustration that you may hear from the IP community about your proposal is really the timing issue, because of the length of time that it takes to get the information back and to prepare our cases for litigation or for whatever else we need to do to protect our brands.

And so I think that's something that the community really needs to understand that while all this dialog is happening and all this GNSO policy work or whatever it is is going on, we still have to do our work to protect our users and protect against cybersecurity threats and we need to do whatever we can including litigation or other UDRPs or whatever, you know, the law enables us to do.

And so what it – what it's going to mean for registrars and for registries is that it's going to probably be more cumbersome, because it will involve a lot more back and forth with the IP holders and the cybersecurity interests that are really going to try to protect it.

And so I just, you know, as we work through this we're going to have to think about the timing issue.

Elliot Noss: You made some public comments. You, Facebook, make some public comments about us to the GAC yesterday. Do you consent to me sharing our experience?

Margie Milam: I'm sorry. Those weren't my comments.

((Crosstalk))

Margie Milam: …too?

Elliot Noss: They were Facebook's comments.

Margie Milam: I'm sorry. What's your question?

Elliot Noss: Well I – do you mind me talking about our experience with your submissions?

Margie Milam: Sure.

Elliot Noss: Great. Thank you. We all saw informed consent there. So we had a – again as I mentioned earlier up until this Friday less than ten submissions. Over Friday to Monday we received over 100 submissions from a party purporting to represent Facebook.

We responded to the first of those submissions and provided in one case the data that had been requested. When additional data about payment information and other peripheral domain names was requested we said, "Get a subpoena," because that's the rule.

That's data that we're – that we're not providing on the basis of this issue today. But what we did do was respond and provide the core information that was requested.

Whether there's more that's entitled or not is something we can all work through together. Working through together looks like somebody reaching out.

You and I have known each other a long time. Denise and I have known each other a long time. Susan and I have known each other a long time. Anybody can reach out but instead went in front of a mic in the GAC and misrepresented what happened.

And to say that around trademark stuff that submissions that are put in on the Friday through Monday before an ICANN meeting have not been responded to in a timely fashion – and again let's remember that you now represent over 90% of our tiered access requests.

So, you know, I really want to say and I want to – it – what - I've passed on three occasions to respond to what happened today or yesterday. This was the fourth and I asked you for permission before I did it.

It is the first best example of if you want that time to be shorter – I want to repeat what I said earlier. If you want that time to be shorter work productively together.

If you think that your shortest path to getting what you want is to lobby governments, to lobby ICANN, to issue a temp spec, to get enforcement I just think you're wrong.

I think your shortest path to getting what you want, which we want to provide you in a reasonable way/in a balanced way, is to work with us together so thank you. Thank you…

((Crosstalk))

Elliot Noss: …for letting me…

Margie Milam: We've certainly done that though.

Elliot Noss: No you haven't. No you haven't and…

((Crosstalk))

James Bladel: Can I jump the queue for a second here because we…

Elliot Noss: Sure.

James Bladel: …were named in this intervention yesterday as well and it did not sound right at all, and so I went back and had my team while that session was going on pull those submissions.

Now we've received just for disclosure 135 submissions in the immediate run-up to this meeting and…

Elliot Noss: James you didn't ask for consent first.

James Bladel: I'm sorry. I didn't ask for consent first. I thought we just kind of cracked…

Elliot Noss: It was a…

James Bladel: …that one open.

((Crosstalk))

James Bladel: But here's – the thing is those were not requests for WHOIS data – nonpublic WHOIS data. Those were requests for a whole bunch of additional data…

Elliot Noss: Yes.

James Bladel: …and our response I believe…

Elliot Noss: Yes.

James Bladel: …was appropriate. You need a subpoena for us to turn over that data to…

Elliot Noss: Yes.

James Bladel: …Facebook. And I'm saying this because, you know, I think Elliot's point stands – is pick up the phone and give us a call. But I – but my question is did it stop there? Did it…

((Crosstalk))

Elliot Noss: James I'm not going to let you ask a question because…

James Bladel: All right.

Elliot Noss: …I cut into Margie…

((Crosstalk))

James Bladel: But I just – but one question, okay, which is that we have a contact form for each of those records. Was that used? Was that – or did it just go right from that to the GAC? I don't understand the process…

((Crosstalk))

Elliot Noss: And you know what? And Margie I want to apologize because it was Denise who did that yesterday and you're bearing the brunt of it today and I, you know, I think that's what – I'm not, you know, that's – doesn't feel great to me but, you know…

Margie Milam: Sure. But I expected a reply. I mean, what you're seeing is a – because of the change in May 25 you're no longer able to do the correlation analysis that we used to be able to do.

Elliot Noss: That's great. I want to stop you there. Just…

((Crosstalk))

Margie Milam: And so – no, no. But if you're going to make…

((Crosstalk))

Elliot Noss: Margie I totally…

Margie Milam: …you know, bring this as an issue I'd like to - at least to clarify what's going on here.

((Crosstalk))

Margie Milam: Should I have a liberty to do that?

Elliot Noss: Let me make your point for you. You aren't able to do that correlation data. I agree. Hold on. Hold on. I just want to – because we – it's – and I just want to be fair to people that, you know, so we can do others. I'm not dismissing that point.

Margie Milam: So…

Elliot Noss: Correlation data is so important and yesterday…

Margie Milam: And that relates to cybersecurity issues…

Elliot Noss: Totally.

Margie Milam: …and that – that's really…

((Crosstalk))

Margie Milam: …what's going on here is that…

Elliot Noss: But I want to move us…

Margie Milam: …and no longer can that be done.

Elliot Noss: Okay.

Margie Milam: And…

Elliot Noss: Margie I'm going to…

Margie Milam: …that…

Elliot Noss: …ask you to stop please. Thank you. Correlation data is a really difficult problem and it is important work. And one of the things that we've – we immediately talked about after the panel yesterday was, you know, with some of the cybersecurity and LEA folks, "Hey you guys got to, you know, you guys got to help here because the only way we're ever as a community going to get your correlation data is to get to pseudonymity.

I mentioned pseudonymity on the panel. You know, Margie if you want to take this back to Facebook in a productive way you guys have, you know, among the best engineering teams on the planet – probably top five.

You guys have maybe the biggest privacy problem in the world right now in terms of pressure not, you know, violations. Join in or lead an effort on pseudonymity.

The sooner we have pseudonymity the sooner we have correlated data so I don't…

Margie Milam: There's not a time for that but in the meantime there's cybersecurity issues going on right now.

Elliot Noss: Okay and all I'm going to tell you about is…

Margie Milam: So…

Elliot Noss: …there's a balance. In the meantime we have had 20 years of one side and pain over here. Now we have just had 30 days of one side and pain over here and I want to stop that pain.

And I'm telling you how I'm not going to be able to – you don't have to convince people that's painful. It's exactly – and I'm just sort of using this as

foil so, you know, that is exactly what we have to stop doing because there's no – it's just baying at the moon.

I hear you. I agree with you. Imagine that we both committed today that that's an important problem. Imagine I said to you, "I'm going to be doing everything I can to solve that."

Short of shutting down my business you're going to do pseudonymity in about 1% of the time that I'm going to do it. But it'll take – in other words Facebook will, you know, it'll take me a 100 times longer given my engineering capabilities, et cetera than it will to – for yours.

That's why I'm calling for all of us to do that. You know, we can have a robust debate but we're not going to have it now but - whether you get correlation without pseudonymity.

I think that's clear and I'm happy to talk about that outside the room. Thank you. Thomas.

Thomas Rickert: Thanks Elliot. And in fact you were making a good segue to the question that I was about to ask and that is it's going to be very bumpy -- I think you said rocky -- for the security researchers.

CERTs are affected by that as well as many others and I sympathize with their predicament as well. I see – I personally see no way around good approaches to pseudonymity.

You mentioned that just a moment ago. Have you put some thought into this – how we can best get that done in an industry-wide fashion because I guess that's going to be the major challenge?

Elliot Noss: Yes.

Thomas Rickert: And every single registry or registrar for that matter can analyze their own data pool but it's only meaningful if you actually do it industry-wide.

Elliot Noss: Yes. Yes. I think that – so first of all I do expect solutions to aggregate here. I think that will take time. You know, I like as a nice metaphor here either railroads or energy in the, you know, utilities in the United States as opposed to many other countries in the world where those were done on a national infrastructure basis.

In the U.S. that was all very local and regional at best and then there was a period of aggregation, and that's what I think we're going to see here with these data sets.

And I want to just – I want to stress, you know, that we don't – I get that that – though that feeling of we don't have time - here's something happening today.

For 20 years there was something happening today over here. You know, one of the things I left out of this presentation because I felt it was too emotional and inflammatory was doxing.

And, you know, that has been demonstrably, you know, WHOIS has been used by political death squads to threaten people demonstrably. We don't know if it's been used to kill people because they're dead so they didn't get to report the problem.

The – there are problems on both sides of this issue and this is a balance and we all need to hold it that way. And, you know, choosing not to is a choice but it just kind of – it doesn't move the ball forward so thank you. Yes Zoe. Sorry.

Zoe Bonython: Two things. First of all we're running out of time.

Elliot Noss: Yes.

Zoe Bonython: And we need to – and we're – kind of need to stick to a break time so…

((Crosstalk))

Elliot Noss: We have eight minutes, right?

Zoe Bonython: …break at exactly…

Elliot Noss: Yes. Yes.

Zoe Bonython: So I have two questions…

Elliot Noss: Yes.

Zoe Bonython: …in chat and I've got Erika Mann with her hand out. I'm just going to read steadily through one of the questions in chat.

Elliot Noss: Yes.

Zoe Bonython: So this is from (Jonathan Matklowski). "By when will you have an anonymized means of contacting a registrant so that we can contact them in tandem without making or with making a legitimate request – access request so that they can exercise their right to object under the GDPR?

We didn't even need any personal data but only to confirm that a domain is no longer registered as part of our clients' digital footprint, and we couldn't send a notice to the registrant or copy the registrant to make our request."

Elliot Noss: Yes I'm going to stop you in the interest of time. Too specific – don't know who the registrar is. Don't know what the facts are. I think that those are the

types of things that, you know, take something like that. Feed it into the system.

When I say that, you know, there's going to be lots of places to participate and those are exactly the kind of problems that we have to deal with in the field. Next question.

Zoe Bonython: Okay the other one's from (Akin Remy) and (Peter Tao). "Does it mean GDPR viewpoints are not really that of field viewpoint?"

Elliot Noss: Sorry. Repeat that.

Zoe Bonython: "Does it mean GDPR viewpoints are not really that of the field viewpoint?"

Elliot Noss: What's those last few words?

Zoe Bonython: Of the field…

Elliot Noss: Okay.

Zoe Bonython: …viewpoint.

Elliot Noss: And I don't understand. I apologize to the questioner. Maybe they can submit it outside. Is it – or Mike or - Erika is at the microphone or Erika…?

Zoe Bonython: It's Erika at the microphone.

Elliot Noss: Okay. No.

Zoe Bonython: Oh.

Elliot Noss: Anyway go ahead Erika.

Erika Mann: Erika Mann…

Elliot Noss: I'll get yours for sure. I promise you.

Erika Mann: …GNSO Council asking question in my private capacity. Elliot I think I agree with you – description. I have just one question and this is you are responding currently as an industry to a threat – a regulatory threat which comes from one part of the globe: the European Union.

So what are you going to do if you respond to it in a globalized fashion and other regulators will tell you, "No sorry, we don't like this. We want a different approach?" Are…

Elliot Noss: Yes.

Erika Mann: …you then responding again?

Elliot Noss: You know, I think the short answer is maybe because we don't know what happens on the regulatory side. You know, we're seeing that in, you know, we're seeing that morphing all over the world and it'll, you know, the answer to that is no to the extent that other countries kind of queue to a GDPR model.

The extent – the answer to that is yes. You know, we have – we will maybe have to respond to – differently depending on whether other countries, you know, maybe even go to a higher standard or alternatively go to a – sort of an opposite direction, right, required disclosure.

So it's just impossible to say and the one thing I do want to be explicit about that is underneath that question is this is an inevitable outcome of trying to solve a global problem through a national lens or even a regional lens.

That inevitably leads to fundamental disconnect and I think that's our greatest challenge as a community. I think it's multi-stakeholderism's greatest challenge and so, you know, it's not limited to this problem. Thank you.

Alex Deacon: Hi Elliot. It's Alex Deacon. First, I want to encourage all registrars to publish the process for how to access nonpublic data prominently. Maybe use the blink tag on your home page or put a link in the Port 43 response, because understanding how that works is important for people like us who require access to that data.

Elliot Noss: Yes Alex I want to jump in. I don't know if you were in a – the session before yours yesterday. We…

Alex Deacon: Yes.

Elliot Noss: The registrars are going to publish something. It's probably not going to be definitive. It's going to be a start and so…

Alex Deacon: And I appreciate that.

Elliot Noss: …you know, and then feedback on that.

Alex Deacon: Yes.

Elliot Noss: Hey, you know, here's what more you can do.

Alex Deacon: And I appreciate that. It's important. And then the – a question I had. You talked about accrediting lawyers and allowing them access to the system. You know, the guys that I represent, copyright investigators and copyright infringement investigators – these investigators aren't lawyers.

They're investigators. They're, you know, trying to figure out what's going on and protect the IP of the people they work for. So how is that going to work?

Are they going to be able to access this data kind of under the umbrella of their boss who probably is a lawyer or someone…

Elliot Noss: Yes.

Alex Deacon: …the GC? How's that going to work?

Elliot Noss: That to me is the agency problem so – and that's the, you know, to me the way I think that works at first instance is that the party who wants access – the, I mean, the way that we're going to roll out at the beginning – the party who wants access to - tiered access will require, you know, sort of a - clear evidence of agency with the eventual – with the client throughout whatever layers that is.

What form that takes, you know, it's a letter. You know, yes that can be easily defrauded. Maybe there's some elements on that we start to check if that becomes a problem, right.

You know, give us a contact at that company. We can call. So that's going to be a great example of something that, you know, happens in the field. And just think about it, you know, simply in the way that you'd approach your work.

You know, we get 100 statements of agency. They're letters and we have one problem. Well probably that's okay, right. That's an acceptable error rate.

We have 100 letters of agency. We have 20 problems. Well probably now it's a letter and a phone number or something like that.

Alex Deacon: Right.

Elliot Noss: So I think it's just, you know, that's the – and it's so, you know, I really want to go back to that metaphor of this is a baby, a fresh infant, and the regime around existing WHOIS is an adult. It's an adult.

Alex Deacon: Right. And I think what we're willing to, I mean, we understand the world has changed. We're willing to identify who we are and give you the purpose for requesting…

Elliot Noss: Yes.

Alex Deacon: …all these things you mentioned before. We're happy to do that. I think just – we'll work it out with you and we're willing to work with you to figure out…

Elliot Noss: Great.

Alex Deacon: …how to make it easier for you so it's easy for us and, you know, it's a win-win situation and then I hope the rest of the registrars do something.

Elliot Noss: That's great. Thanks for that. And I want to stress, you know, and this is a call out, you know, to Alex or Ching Chiao or anybody who's helping here. It's like, you now, and I am - and when I say I this is not Tucows.

This is me. You know, I'm personally willing to help you guys deal with bad registrars so what does that mean? I'm going to renew a call that I've made for over ten years now.

You know, when you talk about red – rogue registrars if you have a problem I am willing to kind of link arms with you in that and go to compliance, and I've always believed that if we do that together that enforcement will be clearer and faster and more responsive so, you know, I renew that.

Like we each have to be doing that back into our own communities. Mike? Oh sorry. Zoe I don't – Mike. Great. Mike?

Mike: Thanks Elliot. Thanks for the shout out to the Philly special and kudos to your work with the taco model. So I want to build on your analogy of the baby that we're beginning to raise.

And one of the things you've – do when you have a child is you think how we're going to provide for college education. Earlier in your speech you talked about…

Elliot Noss: Oh I know this metaphor is going to be beaten up. Yes.

Mike: Yes exactly. You talked about rolling it into pricing and in the Philly special I floated the idea of a micro payment. In yesterday's second session Volker talked about the economics and I specifically said that any solution should not create an undue economic burden on any partner.

Elliot Noss: Yes.

Mike: So I think – but going back to our registrar days we were always very careful to discuss price and…

Elliot Noss: Yes.

Mike: …we're not going there but…

Elliot Noss: Yes I think this is – I, you know, I'm okay with that.

Mike: Okay.

Elliot Noss: I'm okay with discussing price but go ahead.

Mike: What I'd like to raise is some of the constructive feedback that I've heard from some of my IP colleagues…

Elliot Noss: Yes.

Mike: …in response to that was the following and I think it – it's something to take note of. They said, "If you – depending upon how that pricing is set you can create an economic incentive where a bad registrar catering to a bad element actually almost will give the domain away for free because they can make more on the queries." And you and I laugh and that's…

Elliot Noss: No it's just brilliant. I mean, it's amazing. Sure.

Mike: Well it – well again it's the ingenuity of our industry.

Elliot Noss: Right. Right.

Mike: But I think I actually took that as a valid comment.

Elliot Noss: Yes.

Mike: And I think…

Elliot Noss: Sure.

Mike: …I don't have an answer. All I want to do is - I heard that from them…

Elliot Noss: Yes.

Mike: …and put that on the table.

Elliot Noss: Yes.

Mike: And I'm not going to go into pricing. I'm just going to say that's – I just wanted to make that statement.

Elliot Noss: That's great. I think that's great. So there's probably three things I want to tease out from that so thanks for that Mike. First of all, you know, wow. That's immediately creative and we're now looking at edge cases and I think that's fine.

Two, edge cases are probably for the second six months or for the second year. I don't think we have the luxury – when we're dealing with something like Alex's question of what establishes agency; is it a letter or a letter or a – and a phone call, that is fundamental.

That's something that's going to affect, you know, a – the vast majority of requests. We have to deal with the center of the highway because it's a baby, so edge cases for now are going to have to be just that.

And three, it really highlights how we're going to have to step up our compliance game in this industry because that's the type of thing that if we're effectively enforcing then it doesn't work because it, you know, it – the economic life span of that opportunity is too short.

So I think those three points are all a – very useful there. Are you at the mic? Yes. Well I'll take your last question until they throw us out. Nobody's beating down the doors.

Victoria Sheckler: This is Vicky Sheckler with the Recording Industry Association of America and I'm also with the IPC. I know we're out of time.

((Crosstalk))

Victoria Sheckler: So I hope that we could…

Elliot Noss: Always have time for you.

Victoria Sheckler: …continue this conversation.

Elliot Noss: Yes.

Victoria Sheckler: Well - and I'd love to continue this conversation…

Elliot Noss: Great.

Victoria Sheckler: …you know, once this is over. Thank you for saying that compliance is important because we very much agree with that. You had said earlier that you thought that privacy/proxy information would become either less relevant or be more accurate.

Elliot Noss: No. I want to – just so I clear that up, make sure you heard it right, more permeable. What I mean is that the standard of reasonableness around an issue in order to say, "Okay we're dropping privacy," is going to become easier.

So for you in your context the standard of, you know, you come to us with a complaint and you want tiered access. You get that tiered access. It's under privacy.

The level of, you know, the burden of demonstrating the harm for you goes down. We think we're quicker to pull the trigger and say, "Yes that's about the standard not – and this is not a - get a subpoena, right."

There's two things: get a subpoena/your clear, demonstrable harm. You know, so that standard goes down for you because privacy already exists fundamentally in the process.

So we don't think that that need, you know, that makes privacy behind tiered access, has to be treated more dearly and saved for those who really need it, you know, political dissidents, et cetera and not for those who are trying to do

bad things. So, you know, you should see that as a positive when I'm talking about that.

Victoria Sheckler: Right. I think James had a response. Is that right James?

James Bladel: As long as I'm not wandering into a minefield I just wanted to qualify…

Elliot Noss: You should – just making sure we're lined up here because…

James Bladel: Well no I don't think we are actually. I want to…

Elliot Noss: And – right. And I'm speaking just for Tucows in all of this and then we'll get to industry standards.

James Bladel: I just want to qualify that…

Elliot Noss: Yes and sorry. One more thing James.

James Bladel: …as it stands right now…

Elliot Noss: We're all talking.

James Bladel: Well…

Elliot Noss: Okay.

James Bladel: …I just want to qualify that there's different implementations of how we've…

Elliot Noss: Yes.

James Bladel: …covered GDPR. It's no secret we've segmented…

Victoria Sheckler: Right.

James Bladel: …our WHOIS database and we are treating our privacy service as a GDPR sort of equivalent. And so I wouldn't say that we're going to raise or lower the threshold…

Elliot Noss: Yes.

James Bladel: …for reveal…

Elliot Noss: Sure.

James Bladel: …versus DBP versus GDPR because we're treating them somewhat…

((Crosstalk))

Elliot Noss: That's great. That's a – the, you know, where we didn't treat geography different that's what I believe happens and with all of this stuff, you know, what I'm trying to do here is sort of, you know, what do I think happens as we go forward? You know, how are we going to manifest that in the way we roll it out?

Victoria Sheckler: Okay thank you. I will follow-up with you after this because I know you need to wrap up.

Elliot Noss: Great. So thank you all and please hear all that I say in a positive way. Thank you.

END