ICANN Transcription

Practical Insights on Data Disclosure from Contracted Parties Webinar

Tuesday, 22 September 2020 at 14:00 UTC

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

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the Practical Insights on Data Disclosure from Contracted Parties webinar, taking place on Tuesday, the 22nd of September, 2020, at 14:00 UTC.

All lines are muted at this time to avoid background noise and will remain muted until the question and answer portion of the webinar. The question and answer portion will take place at the end of then webinar. The webinar will be equipped with a chat feature and Q&A box. The box is found at the bottom of your Zoom window. To chat, please change your dropdown to include

all panelists and attendees to ensure everyone can see your message. Once again, questions will be taken at the end of the webinar. To ask a question, there are two ways. Click on the Q&A box at the bottom of your Zoom browser, or you may also raise your hand during the question and answer portion. This webinar is being recorded and will be posted on the GNSO calendar. As a reminder, those who take part in the ICANN multi-stakeholder process are to comply with the expected standards of behavior.

With this, I'll turn it over to Owen Smigelski. Please begin.

OWEN SMIGELSKI: Hello, everyone. My name is Owen Smigelski. Thank you for attending our webinar. I'm Vice-Chair of Policy of the Registrar Stakeholder Group and Head of ICANN Compliance and Relations at the domain name registrar, Namecheap. With all the activities ongoing at ICANN right now regarding registration data, policy, and abuse, the contracted parties want to take an opportunity to step back and provide some additional background and information related to data disclosure that often is missing from these debates. This includes an overview of the decades of applicable data privacy law, statistics regarding data disclosure requests in small, medium, and large registrars and registries, and some good practices on crafting a data disclosure request. As contracted parties, we take our customers' privacy seriously. We have legal and moral reasons to ensure that, by purchasing our services, our customers are not subject to unnecessary violations of their privacy. As many in the ICANN community are aware, the prevalence of publicly available contact information and registration data has resulted in over 15 years of problems the

ICANN community has struggled to addressed. This includes fake renewal notices to transfer to a registrar without your permission, scam telephone calls to phone numbers that only appear in registration data, phishing e-mail campaigns targeting similar e-mail addresses that only appear in registration data, and solicitations to register ccTLDs or gTLDs or trademarks that somebody may own by fake registrars. These are complaints that show to ICANN as well as registrars and registries soon after domain names are registered.

Before I introduce my colleagues, I'd just would like to go a little bit over the webinar format. We have 90 minutes in total with 30 minute reserved at the end of Q&A. As mentioned earlier, we'd like to wait for questions at the end and have a good discussion with the attendees. We prefer to have you ask questions live, but if you're unable to do so, please by all means use the Q&A pod and we'll try and do our best to answer them. Slides and recordings of this webinar will be posted on the GNSO calendar page after this meeting.

Now I'd like to introduce my other presenters who, like me, are alumni or what might better be said as survivors of the EPDP team, as well as the subsequent IRTs. They've all participated in Phases 1 and 2, whereas I only had the pleasure of joining Phase 2 once I joined Namecheap. They're all in the front lines and do the stuff day in and day out, so they're certainly speaking from personal experience.

First we're going to have Alan Woods, who is the Senior Compliance and Policy Manager at Donuts, Inc., their gTLD registry portfolio operator, including my favorite, .rocks, which is

what I use for my personal domain name. He'll be speaking to the background and the impact of GDPR.

Sarah Wyld be speaking next. She is a Policy and Privacy Manger at Tucows domain name registrar. She will be presenting statistics called By the Numbers.

Finally, we'll have Beth Bacon, who's Vice-Chair of Administration for the Registry Stakeholder Group, as well as Senior Director of Policy and Privacy at the Public Interest Registry (PIR) which operates .org. She's be speaking about how to format a request and response processes.

Thank you. With that, I'll turn it over to Alan.

ALAN WOODS: Thank you so much, Owen. Thank you all for attending today. Briefly, again, to introduce, I'm Alan Woods, the Senior Compliance and Policy Manager for Donuts. I'm also the data protection point of contact as well for Donuts, Inc.

To begin this off, I have the unenviable task of providing historical context to the most beautiful of topics for data protection. Then I'm going to try and link that a bit into registration data directory services (RDDS) or, as we all know, the access protocol of WHOIS. Then I'm going to set up a little bit about the temporary specification and then just touch generally on the EPDP. And I can do that in 15 minutes, apparently. So you're going to have to bear with me.

Also, I need to remember that I am also Irish and therefore I have a tendency to speak quite quickly, so apologies if you see anybody of my colleagues waving at me. That's telling me to slow down.

If we can go to the next slide, please. Thank you. One of the most, I suppose, personally irksome things I've heard over the last few years is a repeated statement. That is that, the GDPR, when it occurred, was a new law and it was a new law that came very quickly and we did not know how to react and we didn't react properly and we had a very short period of time in order to do that and that the [law has] changed overnight. This is not actually true. The law has been very much stable for many years. What has changed is things such as enforcement and the fines and the [reach] that was claimed from that law. So, in order to prove that, obviously I'm not just going to make a bland statement. That's why we're going to have to delve a little bit back into the history of GDPR and the history of data protection generally.

If we could just see there a very large caveat—I say a very abridged history—the history of data protection is far more in depth and nuanced than two points on a slide, but generally speaking, the roots of data protection are traced to World War 2 because, during World War 2, it was the personal data—things that were identifying of people—that were a matter of life and death to people within that particular period of time. Then, post-World War 2, very quickly, in the universal declaration of human rights, it began the beginnings of this right. You can see there on the slides that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, and everyone

has the right to the protection of the law against the interference or attacks. Then that was quickly picked up, I suppose, a little bit closer to the epicenter of World War 2 by the European Convention on Human Rights back in 1950, which made that a bit smaller and said everybody has the right to respect for private life in his home and correspondence. It was from here that data protection began to develop. Also, in the background to this, you must remember that, in East Germany, there was an awful lot of issues about the data about the citizens of East Germany and that they were being monitored and watched very closely, not only by the policy but by informants for the policy. Again, the use that was put to personal data starting becoming an issue to the people that lived in that particular area.

If I can go to the next slide, please? As that's going, as filing systems and computing and storage and communication began to improve, data privacy also then became a much more topical issue. Then I suppose again, considering the proximity with the first data protection law in the world, was was actually in Germany and—pardon my pronunciation of any German … was the Bundestag [inaudible] in 1973 … And it was in the German state of Hesse. It was probably in relation to, again, them being at the epicenter and seeing what had occurred.

Very close after that, Sweden actually came up in 1973. They were put to the post by the Germans, and they came up with the dataligan in 1973.

Now, both these were very basic laws, but specifically, again, trying to ensure that the rights of the private citizen and the private

citizen's data would be protected. It wasn't really until, for a bit of context, 1980 that things made out to change.

So if we're to put the universal declaration of human rights and the European Convention of Human Rights as, say, the water and flour, and the backdrop of World War 2 and East Germany as being a warm and moist atmosphere, well, then the OECD privacy guidelines is the sourdough starter of data protection. And, yes, I have been baking a lot since the lockdown begin. The OECD privacy guidelines established what are known as the data protection principles. It is from these principles that all the rest have flown.

Straightaway in 1981, you can see here the convention for the protection of individuals with regard to automatic processing of personal data in Strasburg, which established a slightly refined set of them. These are the principles that come through today. Beyond that, little laws starting popping up over the place, obviously self-interest. The Irish data protection law came up in 1988. Then the European Data Protection Directive, which tried to harmonize the various laws within the European community at the time was established then in 1995. As an aside, ICANN was established in 1998, and the GDPR began its path to today in 2012 to be commenced in 2018.

Can we go to the next slide, please? Great. I'm not going to put a lot of effort because it's going a lot into the weeds on the data protection principles themselves, but one of the most important things I need to point out about the data protection principles is is it as it applies to the data subject, the person to whom the data relates, not anybody else. The only person who gains right under

data protection legislation is the data subject. So all these principles are viewed through the glass of the data subject: lawfulness, fairness, and transparency. It must be transparent to the data subject, that we are treating their data lawfully and fairly. The purpose limitation means we cannot just take their data and use it for any other reason. It has to be for a very specific reason, and that must be transparent to that data subject. Data minimization means that, when we have that purpose, we must only use it for that purpose and we only must have the amount of data, the minimal amount of data necessary to achieve that purpose. Accuracy I'm going to come back to. Storage limitation means we can't keep it forever. Once we've done or achieved that purpose, we must then get rid of that data. We must delete it. Then integrity and confidentiality is all about the security of that data, that we must maintain the security of that data and guard it. Accountability then is also that one person, us as the data controller, being accountable for what happens to that data.

Now, accuracy I'm not going to wade into too much because it is a very hot-button topic at the moment, but, again, I wanted to remind you that it's through the view of the data subject. So, as a data controller, a person who controls data, we want to make sure that the data we hold is the data that is provided to us and is considered to be clean and correct by the actual data subject. Now, there is a caveat on that in the sense that the efforts of the data controller to ensure that that is correct is dependent on, I suppose, the impact that any inaccuracy would have. But again I must point out it's the impact on the data subject—the impact that [inaudible] not on any third party.

So what I will say to you that there is a legal opinion from Bird & Bird on file from the EPDP, and I would absolutely suggest you to read it all. I would definitely not take bits and pieces out of it. It needs to be read from beginning to end because it sets up the exact reasons and applies the accuracy principle very nicely to the actual DNS.

So the important thing though is that all these principles have not changed. They are the same since 1980, again, pointing out that ICANN was set out far after the data protection principles were established and began to develop.

If I can go to the next slide, please. Let's have a brief snapshot then of what WHOIS was before the GDPR came in. How were we doing? What was our scorecard? To be honest, it wasn't great. We have not formally established purpose for the data publication or indeed for the collection. So we weren't transparent to the data subjects and we certainly weren't working on minimization. We had several things for the same reason. We freely published personal data of all registrants, publicly and open. Therefore, it was impossible for us to limit the purpose for the use of that data. Data scraping—actually, Owen talked about this at the beginning—repackaging and the resale of registrant data for people just [went] to the WHOIS [inaudible] used it for whatever purposes was rampant. We had no control over that. We could not limit the storage. We could not limit the access. That was also very much an issue. We had an inability to limit the use of the public data then when people took it from the WHOIS or indeed when other companies scraped the data and resold it. We could not in any way prevent the other uses of that. So we lacked

purpose, we lacked limitation, and also technically it was breach every single time, and therefore we lacked data integrity and we lacked confidentiality. Finally, we had an inability to apply data subject rights. We could not say to our data subjects where there data was, how was it being used, nor we could rectify if it was wrong somewhere else, nor could we stand over the accuracy of that data as well. So in a way it was a failure for us to vindicate those rights. This is not just me saying it. You can see here—I'm sure you read it already—that back in December 2017, the Article 29 Working Party, who are the conglomeration of all the data—I can't think of their names—protection advisors or authorities around Europe said that they wish to stress that an unlimited publication of personal data of individual domain holders raises serious concerns regarding the lawfulness of such practice under current European Data Protection Directive. That's the1995 directive, not the GDPR. It did not sneak up. It was even before the GDPR. It was an issue that we needed to deal with.

If we go to the next slide, please. This is the point where I tend to probably speed up, going "I'm running out of time." So apologies. So here came the temporary specification then. Because we did not have time to develop a community process in order to put in a policy to prevent this, we have to have a top down effort under the bylaws in order to put in patch, basically—it was a bandage—to prevent us from reaching further as the GDPR came in. That was the temporary specification. Most notably, it put the publication of data, or as people called it, going dark by the WHOIS, and then it established the aforementioned EPDP. Our job in the EPDP was not to rewrite everything. It was to take the temporary specification and affirm it or not with modifications as were necessary in order

to bring us in line with the law as it was at the time. Many saw this as an opportunity to finally set it right. It was an opportunity for us to say let's finally look at the data protection and lets apply that properly to the DNS. But unfortunately it was also an opportunity for some just to go back with what was called the status quo, and that is try their best to bring it or justify posthumously getting back to the way things were, which unfortunately was never going to be a good thing.

Can I get to the next slide, please. Almost there from my point of view—this history lesson. Let's then revisit that scorecard and say how are we afterwards. To be perfectly honest, Phase 1 did what it needed to do. It was good. And Phase 2 is trying to do the same. That is we established and explained basic legal purposes for the collection of registration data, which we had never done. We also considered necessity. Why was it necessity for the purposes? And also minimization, as in, are we getting the data that we deem necessary? That was Phase 1 Recommendation 1. We also ceased with certain caveats: the publication of personal data in WHOIS or [inaudible] will be under Recommendation 5. Also, more importantly, that prevented the widespread mass data scraping and the repackaging and the resale of registrant data. I did put a little note in there that this is even confirmed in the US courts recently, where .nz took one of the biggest companies who were doing this because of the time it was just easy for them to do that and told them they shouldn't have been doing that, that was against the terms and conditions of WHOIS at the time, they should not have repackaged it, they should not have resold it. Indeed, we're not saying that this was people who were with nefarious intent who were packaging this data, but law

enforcement, governments, were beginning to buy this data from certain companies, even though the data itself should not have been harvested by those means. As Owen pointed out, we need to look not only to the good uses of the data, but there were a lot of bad uses of that data as well—again, the renewal frauds, the phone calls, the use of personal data, spam. Good old-fashioned spam would have come an awful lot from the publication of data such as that.

Finally, we tried to establish the means by which request for disclosure may be legally processed. This is a very important one, fully understanding the community understands that there are perfectly reasons to have disclosure of this data, but in order to do that, the controllers in this instance need to ensure that there is a proper consideration rights of the person to whom data protection relates. That is the data subject at the core. So we must ensure there's due process and that we do the consideration that we're expected to underneath. So that's why we put in Rec 3. That's why we put in Recommendation 18 specifically and why we did all the efforts on Phase 2, which we hope will pass and we hope that we keep continue to making better as time goes by. But as a starting point, it's not bad.

We move to the final thing then—I know I'm completely out of time at this point—just to do a very brief on the next slide. There we go. So what are the takeaways from my brief history lesson through European legislation? One, the GDPR was not new. Little change to the substance. Just more about the liability and implications for enforcement. That is a very important truth. WHOIS never went dark. WHOIS, for the first time, probably came into the light. I

know that's trite, but it is true. WHOIS was an issue, and now it's finally being [ranging]. The status quo was never a good goal for us and should never have been a targeted outcome. We should have always said and in effect done a data protection impact assessment—assess what we're doing, why we're doing, and what we needed to do when it comes to ensuring the rights of our registrants and the data subjects are being indicated.

Finally, again, just to carry this on because I haven't said enough, data protection confers rights on data subjects. It does not provide a right to any third party. It doesn't even provide a right to law enforcement. Those rights are provided for in other legislation. That's an important thing, and it is an exception to data protection, not a right for third parties.

With that, I'm going to stop now. Thank you for listening to my tirade. I'll be happy to take questions at the end once everybody is done.

SARA WYLD: All right. Thank you. I'm Sarah Wyld. I hope you can hear me. I'm here today to share some statistics about domain data disclosures. We ran a survey within the Registrar and Registry Stakeholder Groups to gather information. Today I will show you request and response rates, what the outcomes are, and who is asking for information. I'll also talk about what data is actually provided, what the response has been from requesters, typically processing time, and then bring it all together to see what we learn about the effect of public data availability.

Next slide, please. Responders to our survey provided data covering the period from May 2018 to the end of August 2020. We found a significant variance in the rate of requests, with registrars seeing as few as 30 or as many as 3400 requests in that period, while registries had a smaller range. Overall, fewer that 1% of domains under management are involved in a disclosure request. It's interesting to note an increase in requests coinciding with ICANN meetings. One benefit that I think will come from the SSAD is a more standardized reporting process. So getting this type of data should be easier moving forward.

Next slide, please. Now, looking at what actually happens to their requests—these are averages—the most frequent outcome is that the disclosure is either redirected or denied. Next, after that, we see the data is disclosed, which, on average, is the response for about 20% of registrar requests and 40% of registry requests. Finally, we have the Other category. So, when I say "denied" or "redirected," what I mean there is either the request was sent from one party to another—so registry to registrar, or registrar to reseller—because that other data controller is best-placed to review and respond to the inquiry. Alternately, the request may be delayed because the requester did not demonstrate their lawful basis to process the data. Looking at the Other category, this includes a range of outcomes, such as disclosure of some but not all of what was requested, explanation that a privacy or a proxy service is enabled, requests that could not fulfilled because they were incomplete, or explanations that either the data is actually publicly available or that the domain isn't registered or isn't with the provider who is responding.

Next slide, please. When looking at what data is provided, most registrars and registries provide only the registrant data. But about a third also provide admin and tech contact data, as well as registrants'. In cases where data is not disclosed, the responding party instead explains why and what the next steps are for the requester. It's interesting to note that security methods vary. It could be a password-protection file, an SSL-secured platform, or something different. So this is another way that the recommendations from the Phase 2 EPDP will provide some clarity. They'll ensure that the requester is specific about which data elements they need and why, which helps the responder. And it should standardize the security methods involved also.

Next slide, please. Most of survey responders had no appeals or complaints come into them. We did hear from some registrars that fewer than 1% or up to 5% of requests had an outcome that was appealed by the requester. In all those cases, after discussion with the relevant team, the appeal was closed with no disclosure. Appeals typically related to either the requester having sent in the request to the wrong place or situations where this is not the right process, and they should instead file, for example, a URS or a UDRP. So educational outreach should help with reducing that. ICANN Compliance provided some statistics, but their data only covers the period from February through August 2020. ICANN reported a total of 12 complaints about how contracted parties handled data disclosure requests.

Next slide, please. Thank you. Looking at who is making requests, again with averages from our survey, the responders indicated that the vast majority of request related to intellectual property,

with only about 15% coming from law enforcement. The rest is Other, which includes security, requests to contact the domain owner, and requests were no domain is included or the domain is not with that provider.

Next please, Zoe. We have found a statistically significant rate of repeat requesters. On average, for every four requests, there's one requester. But also, looking at that survey respondents who were able to identity that they have a specific repeat requester, we found on average 45% of requests come from that single requester, which, as you can see, is a significant chunk of the request volume overall.

Next slide, please. Average response time is less than three days. We noticed that it's a bit shorter for registries than registrars, and that seems to be because registries do send most of their requests over to the registrar of record. So it's a bit faster for registries to process them.

Next slide, please. Finally, what can we learn? There are obvious benefits to redacting data. The data that was publicly available was a major attack vector. Without it, it's much harder for bad actors to carry out social engineering and other forms of abuse. Overall abuse stats show a real decrease once most WHOIS data was redacted. That indicates that the data was being used for abusive purposes.

A couple other considerations on that, just I wrap up. It's important to keep in mind that a domain could have any number of sub-domains being used for abuse. So it's helpful and actually necessary for the hosting provider to be involved in any abuse

mitigation efforts. Recent COVID-19 abuse-related tracking by individual contracted parties and by ICANN's OCTO actually showed no increase in overall abuse rates during that period. Thank you.

Over to Beth.

BETH BACON: Thank you, Sarah. This is Beth Bacon. I'm the Senior Director of Policy and Privacy with the Public Interest Registry. We are going to talk a little bit about the actual request and response process. That'll include looking at the best practices or the building blocks of what we consider as a controller when we do receive a request. I think it will help put into context how we operationalize what Alan went through—the history and the principles of data protection—as well as put a little bit of context around the things that Sarah just quantified, especially in request to the Other category, when things are redirected and why.

We'll just jump in with Slide 1, which is the request and response process. As you guys know, registries and registrars have data submitted through the domain name registration process, which includes some personal data and, at this time, is governed by the temp spec and soon-to-be consensus policy out of the EPDP process—well, processes; the several phases. Any controller and processor of data is required to provide the ability to request access to data by data subjects as well as third parties. But, as Alan pointed out, the privacy legislation and regulations confer those guaranteed rights on data subjects. For third parties, be those individuals or organizations, you have to demonstrate your

legitimate interests. As we will talk through the process of evaluation, it's not a small task. We would certainly appreciate the challenges, and we're trying to bring down the vale and remove the mystery as to what happens when you submit those requests.

As a baseline, it's important to know that there are several overarching things that impact requests. One of the main things is that they vary upon the requester type. Data subjects have certain rights afforded to them. Law enforcement can also have rights afforded to them in other laws, apart from the GDPR and privacy laws. In addition, contracted parties can be bound by jurisdictional requirements, depending upon where they are located. Third parties have to establish their rights in the data. They aren't just conferred those rights. But certainly legislation provides that opportunity to establish their rights.

The legal basis for the disclosure guides the type of analysis that the controller or reviewer of the request will undertake. Again, that's based upon often the requester type. The nature of the request is also important. This can be, is the domain name infringing a third-party right? Is it for content? Is it services? Again, that impacts, as Sarah noted in her data, the different types of responses. Sometimes the response is, "You should maybe do a UDRP." So it's the type of request that can really impact the type of review we do.

Depending on one or more of the factors, there may be cases where the registrar or registry are required via legal obligation to disclose this data. We may be entitled to do it if we so choose if it's in line with our terms of service or if it's something that is line with our mission or requirements in our registry agreements. We

may also decide to disclose it to avoid liability. So there's all sorts of different factors that have to be considered when the request is received, and we'll talk about that full process below. But I think it highlights the importance of providing the required information as a baseline. It's really the building blocks of the request. Providing the required information and considering all of these factors really helps make the review more efficient, limits the need for additional processing of data because of imprecise or incomplete requests, and limits the contracted party for having to seek any clarity or deny a disclosure simply because we don't have the information we need.

I think we can then move to Slide 2, the required information for the request. Again, these are the building blocks of what makes a good request and why that's important. There are several sources of required information. There's several sources of best practices around submitting requests. We are not going to go through each and every requirement outlined in the EPDP Phase 1 or 2 or the GDPR because we only have until 11:30 and there's not enough time. We will talking very practically about what information helps the receiving party to do an efficient and thorough review.

Let's keep in mind also that, when we say a "good" request, that means it provides the minimum amount of information that allows the receiving party to undertake the requisite analysis. It does not mean that, if a request submits a specific set of data—if you check all the boxes you see on the slide—it's guaranteed disclosure. I understand that is incredibly frustrating. Everybody would like to know, what is that secret sauce? What's the silver bullet? What can I submit to guarantee a disclosure? This is less about giving a

secret sauce because frankly it doesn't exist due to the subjective nature of the review and analysis and this objective nature of, quite frankly, the law which directs that review analysis but also because each party is in a different jurisdiction, a different environment, a different flow in the life cycle of data, we could say. Registries and registrars look at slightly different things or they have the same steps but maybe have a different role in that process. So this is why establishing the baseline data that we will be a good solid request, a good basis for analysis, is really important. What it does is it enables us to review it properly and gives you the best chance of disclosure.

For this discussion, we'll mainly be focusing on third-party, which tend to be legitimate interest requests, simply because those are the ones that are slightly mysterious. Law enforcement and data subjects, as we've discussed, have different sets of rights and legislation that guide disclosure and impact those arrangements. But really it's the third parties' request or the legitimate interest request that require the analysis and have a little bit of mystery to them.

As for some sources of guidance beyond this delightful, delightful webinar that you guys are all subjecting to yourselves to right now, you'll see on the screen the very basics of what's required. There's a reflected in Recommendation 3 of the EPDP Phase 2 final report. It's a simplified version. These are the building blocks: domain names giving us information about the request, information about the legal rights specific to the requests, and legitimate interest and other lawful basis for the request giving us some context. It's also important to affirm that the request is being

made in good faith, as well as identifying how that recipient or the requester will process that data once it's given to you. One of the requirements for a controller is to ensure not only that you are processing it in a disclosure in a responsible way that's in line with legislation and the rights of the data subject but also that the person or entity or organization that you are disclosing it to is going to continue to protect those rights. It's very important and it's a very difficult thing to do. Once that data is out of your hands, you can really only rely upon someone's attestation that they will do the right thing with that data. So that's very important. Also, a list of data elements. It should be specific. It should be targeted. It shouldn't just be "I would like all data on this human." You need to have why the data elements are requested and why they're necessary for this person for the particular request. Then, in the EPDP Phase 2, there are different types of request: being urgent priority levels—that sort of thing. I won't go into that now, but that is something that will be required and you should indicate in your request.

Another source is predating the EPDP Phase 2 work. But you'll see that, because EPDP and this document are based in principles as well as best practices, the Registrar Stakeholder Group prepared a minimum required information for WHOIS data request form as information to provide some consistency and predictability. You'll see that it is consistent with the EPDP work as well. There are a few more things in the registrar document. Again, most of that leads to context and using this minimum data as a means to apply a really good strong foundation for analysis that allows us to disclose in a very informed way.

Now, we have the link in this and you'll be able to link on that once the PDF of the slides are available if anyone is interest. I did say the Registrar Stakeholder Group developed this document, but the registries are in the process of taking a look at that and joining. So the registries and registrars are very consistent and supportive of this particular approach.

When you look at that document, you'll see that's very similar, but one thing that it does draw out is providing a case summary. It's a brief description of the specific issue and the request and what the issue that they are trying to resolve is. This really helps the reviewing party conduct a thorough analysis of the legitimate interest asserted by the requester. We'll talk more about that in the next section, but I wanted to highlight that because it is not necessarily verbatim to the requirements in the EPDP Phase 2 but it is very important. Providing that context to the reviewer is very helpful. In addition, providing any documentation relevant to the requests. That can be specific to what law you're referencing, what requirements you're referencing. In addition, if you've taken any other steps to obtain the data prior to reaching out to the registry or registrar, that's also quite important.

So those are the basic building blocks. We can move on to the review process on Slide 3. Now that we've discussed the building blocks of good requests, we'll walk through the general process of what happens on the contracted party side when a request is received. We're trying to again lift the curtain a little bit and give some context to the role of the information submitted in processing the evaluation of a request. Again, we'll not walk through the particulars of the EPDP Phase 2 requirements, but

we'll mention a few. And these best practices certainly merit what is in the Phase 2 report.

We'll start with receipt. Regardless of request type, contracted parties are required to have that mechanism for submission on their website, as we mentioned previously. In the case of the Phase 2 report, that would also be acceptable via the automated system, the SSAD. In addition, Phase 1 also requires that. in addition, GDPR also requires that. So there is a mechanism for third parties, individuals—anyone who has an interest in data—to submit those requests.

It's important to keep in mind that the registrar is the best party to receive requests, as you saw on our data that was presented by Sarah. A large percentage of the other section of requests are registries redirecting that request to a more appropriate party. Registrars maintain the mechanism to contact the registrant, and registries have only the data provided to them by the registrar. This highlights, again, the importance targeting the correct party. Requesters should also keep in mind that, for registration data subject to privacy or proxy registrations, only the privacy or proxy provider would have that underlying registrant information, and the registrar again is required to maintain some form of contact. In addition, as we noted, the timeline can be a bit longer for review. Sarah noted that, again, in her data, we highlighted that, for a registry, it's somewhat shorter. The registrar may have that extra step of interacting with or passing that request on as well. So, again, the receipt is highlighted by the importance of contacting the most appropriate party.

Then we would move on to actual review. This is the fun stuff—the secret sauce, as we would say. Initial review is for completeness, purpose, and to understand the type of requester. This lets the reviewer know if we have enough information to even consider the request and then what kind of process to apply to the review. For example, are we looking at data subject rights? Are we looking at a legitimate interest test? Is it a court order? All those sorts of different scenarios. If there are any deficiencies that are easily resolved—for example, if I receive a request and I would like to confirm the identity—I can reach out to the reviewer, or the reviewer could reach out, and request further information, like an ID or "Please confirm these are the data elements you would like." You can ask for more information. It's not a requirement right now. There are some requirements in Recommendation 8 of the EPDP Phase 2 that touch upon when that can and should happen, but I will say that, in practice, I do think, with the colleagues that I work with, that that happens. Clarifying the request is very important. Following the initial review, the reviewer will determine whether the party has a lawful basis for disclosure, whether all of the data elements are requested are necessary, and whether that balancing test or legitimate interest test is request.

To get into the actual discussion of what we do to review and what guides are review, we'll focus on a third-party request, and that requires a balancing test or a legitimate interest based request. If it is a legitimate interest request, the reviewer then examines the request based upon the three parts of the legitimate interest test. Those are the legitimate interests, necessity, and balancing. The balancing is the balancing of the rights of the data subject against the request. All three parts of the test have to be passed in order

to support the disclosure of personal data. You can't fail necessity and pass legitimate interest and balancing and get the disclosure. So unfortunately it's all or nothing on this one. The good thing is that these things are broad and they are subjective. So that provides some flexibility for us to consider each request individually. That's important. We don't blanket just look at things and bulk and say, "These are probably the same." Each controller looks at each request individually and thoroughly.

Walking through the consideration of the three parts will help put context around why it's important to us to provide as much specific information to the specific request as possible. Not only does it help make the review more efficient but it also give the reviewer the best chance to make the most informed decision. Quite frankly, if your building blocks are good and that foundation of that request is solid, it makes the chances higher that you will receive a request because it allows the controller to justify that disclosure based upon a lot of information or clear information. So, again, it's not a guarantee, but it certainly helps.

So this is where you can start to see how the request provides that information for disclosure. If the information received is simply in generic form language—you're trying to cut and paste, if you will, you're just checking a box—that doesn't work. It won't support the specific request. It will not provide the specific support you need for this three-part test. A request that doesn't show or provide sufficient support for the legitimate interest or the legal basis or doesn't demonstrate other efforts or mechanisms considered to obtain that data doesn't generally support the claim.

So these are things that we're going to discuss and put into a little bit of context for you.

Getting into the parts of the legitimate interest test, on the first bar is legitimate interest for the stated purpose. A wide range of interest may be legitimate. Quite frankly, legitimate interests is very broad. The interests don't necessarily have to be compelling. It does not rule out interests that are a little more light. They don't have to be that you're changing the world to get this data. However, you do have to be very specific. An interest that could be seen as trivial or controversial could still be legitimate for these purposes, but please keep in mind that, if they are a little more trivial, they're also more easily overridden in the balancing and necessity tests. So this is why a strong legitimate interest with support of your purpose is very important. Again, the foundation of your request is establishing your interest in the data. So simply saying "I have a legitimate interest" does not cut the mustard on this. So showing you have the legitimate interest does not mean that the requester has to have a clear, specific outcome, but you cannot rely on vague or generic language. You have to be specific.

For example, saying, "We have a legitimate interest in processing this customer's data," doesn't clarify a specific purpose or outcome. Being more specific about the purpose, saying, "We have a legitimate interest in processing customer data because we want to market our goods and increase sales," is better. In this case, it would be, " I have an interest in your customer's non-public WHOIS data because I would like to purchase that domain name (or I have an interest in their business or I think I have a

legal claim against them)"—something more specific other than "I have legitimate interest." I'm stressing this because a lot of the request we receive say, "I have a legitimate interest," and that is all.

So, in addition, the requester still needs to identify a purpose and show that it is legitimate in the specific circumstances. Again, that means it can't be a cut-and-paste or a form language sort of request if you're a routine requester. All this is to say that legitimate interest is not the highest bar of this test, but if your stated interest is supported well, it adds weight to and supports your request in the necessity and balancing test. It's the foundation.

We'll move on to necessity. This is an interesting one. We've had a lot of conversations within the EPDP, within the community, discussing if a request on the WHOIS data is the most appropriate source of the data. Are there other ways to get the data? For necessity, you need to demonstrate that it is necessary for the purpose of the legitimate interest that you have identified in your request. It should be targeted and a proportionate way of achieving your purpose. So that's another reason you should list the specific data elements you would like instead of saying, "I would like all data." It makes a lot easier to argue that it is proportional if you are not just asking for a blanket amount of data. if you do need all the data, support that claim.

So this is especially important again when you're contacting the correct party. The reviewer will look at the elements of each case and whether the processing is proportionate and targeted enough to meet the objectives you stated. The reviewer also thinks about

and is required to think about, is there a less intrusive way to get this information? Could the requester achieve their purpose through some other reasonable request for processing? If you could achieve your purpose in a less invasive way, then the more invasive way is not necessary.

For example, if you request this data of a registry but the registrar is the more appropriate contact because they maintain contact with the registrant themselves, that is less intrusive. So that's just an example of what I personally think about when I look at these requests.

You should be careful also not to confuse processing that's necessary for your purpose with processing that's only necessary because of your chosen method of pursuing this purpose. It's a little bit convoluted sounding, but you have to make sure that you aren't only saying it's necessary because you've chosen to go this route of asking the registry or asking the registrar. Is it necessary for your purpose in general?

If you're unable to demonstrate that the processing actually helps meet the legitimate interest, then again you would not pass the necessity test. That does mean, as it's a three-part test, you would not pass the legitimate interest test. If there's another reasonable and less invasive way to meet your interests and achieve the purpose, you're going to be asked that question and it would likely not pass this particular part of the test. So this is where necessity, while a smaller portion, really becomes an important part of the test. It's a challenge. It's something that demonstrates why including the information in your request, such as, "I have also tried this, this, and this to get the data," or, "This is why I cannot

obtain the data elsewhere or in another way," really bolsters your request.

Then we'll move on to balancing. This is one of the more subjective sections, and it is frustrating to no end, I'm sure, for requester. Again, we're trying to show a little bit more of how we as reviewers and controllers of data think about this. Balancing is when you consider the request with the rights of the data subject. The rights of the data subjected, as Alan highlighted in the background, is the basis of our whole endeavor here. The data subject has rights conferred to them by legislation, as well as, as Owen said in our opening, just our mission and our moral objective to protect our customers. So this is a big one.

It's also very interesting because this entire balancing test, as well as the other parts of the legitimate interest test, are subjective. The rules governing, the laws and regulations, are broad. They are not super specific. So that provides flexibility but also provides a little bit of a question mark. It provides a higher bar. You have to justify very clearly as a controller why you think it's okay to disclose because it is broad.

Moving on to the different elements of the balancing test, this will be a focus on any potential impact on individuals. This can be any type of impact—physical, financial, if it would impact the ability of a data subject to exercise their rights, if it would indicate a loss of control over their personal data, if it would in some way economically or socially disadvantage. There is not a finite list of what would impact, but if you look at the rights and data that are conferred upon the data subject, you can get a flavor for what privacy legislation is meant to protect. Also you can look in

fundamental rights and freedoms documents. That's what we consider: those sorts of impact.

Not only does balancing think about the impact to the data subject but it also has to consider the expectations of the data subject. This is one reason all organizations work so hard to establish really clear privacy notices and terms of service for all of the activities and services that would process personal data. It's another reason in the EPDP Phase 2 report why it's vital that we talk about terms of service and privacy notices for any party or any service that would touch or process personal data. So it's all about setting those clear expectations. We try and do that so that we can be clear on this part of the balancing test what the data subject can expect from our service that we provide.

Legitimate interest is more likely to apply where you have a relevant and appropriate relationship. So, again, when we redirect to a more appropriate party, it's not necessarily a now. It's notice that there's another less invasive or more appropriate party with which to request the data. The level of analysis involved in a legitimate interest review highlights why it's important to provide as much information as possible. I know I've said this ten time, but again it's the building blocks and it allows us to support our claim when we do disclose. Again, we have to clearly support our claim when we do disclose because the guidance is very broad. We are meant to think about this very carefully, and it's meant to be a high bar. That is why it's not as specific as some of us may wish it were. I can guarantee you that I think every requester wishes there was a secret formula or a checklist, and I can guarantee you

that every controller wishes there was a secret formula or checklist. It would be a lot easier.

So we have also seen requests come in that are not crafted for the receiving party. They don't include the necessary information. It doesn't show a genuine effort to pursue other means of contact. So when these things aren't included, it's really hard to support a disclosure that could impact the data subject because, if you're disclosing personal data, there is a guaranteed level of impact on that data subject, and it's all about balancing if it's an appropriate level of risk.

So that is the balancing section. We would move on from that test. Once we've evaluated the necessity, the legitimate interest, and the balancing of the rights and freedoms, that's when we come to the decision where we either provide a disclosure of all or part of the data elements requested or a rationale as to why we did not disclose. I think that, for those of you that have submitted a request and perhaps have received a rationale for non-disclosure, it's thorough but it's not a treatise. You're not going to get four pages of rationale. I don't think that's what anyone wants. We do provide a very clear reasoning as to why you either didn't meet the legitimate test/satisfy that test or if you're request is in some way deficient. That again can say we don't have the required information to properly review this request. So where they are denied, we do provide a rationale. Where we perhaps disclose part of the data elements, we will also provide a rationale as to why not all data elements are disclosed. If you receive the data elements, you also receive the data elements you requested as well as information as to how we reviewed that request.

Following disclosure, the record of the request—it's just a simple housekeeping. There are requirements in GDPR as well as in the Phase 2 with regards to SSAD. The SSAD system would collect a record of the request, the rationale, the discloser, the recipient—all of these required information—should a data protection authority come in and ask questions about a request or should someone come back and say, "I disagree with your decision. Could you please review the request again?"

So it's really important, again, so we can A) understand how we'll we're doing. We can provide the types of snapshots of the nature of requests, as Sarah did, and we can see if we are improving. I think that all contracted parties are always looking to evolve. I know that I often take a look at how we're looking at our process for review as well as our responses and rationales to make sure that we're providing as much information as we can without, again, providing a three-page treatise on my legal analysis of the request.

So following the record of request, we consider that timeline for that request closed. Again, as noted by Sarah, it's generally about three days for a registry, a little bit longer for a registrar. Technically, if we're going by the GDPR, we do have 30 days to process the request, but I don't think there's a contracted party on this call or in the environment that endeavors to take that full 30 days. We want to close these out and we want to either disclose the information or provide that rationale.

I will stop talking there. I know I've taken, I think, my full 15 to 20 minutes. But we want to make sure that we have another half-hour and we want to make sure that we leave a lot of time for questions

and answers because that's the whole reason you're here. Thanks.

OWEN SMIGELSKI: Thanks, Beth. So will jump right in here to the questions that we received. First we're going to start Fred [Felman], who says, "Alan, I don't understood. If the—" apologies. My dogs are barking here. The joys of working from home. "If the basis of GDPR was established in World War 2 and we know that there are millions of global online businesses managing the personal data of billions of people, those businesses use technology and user-accepted terms and conditions to manage the collection and use of personal data in full compliance with GDPR and local laws like those in California. Why is it so hard for registrars to collect this data and maintain it responsibly with decades of precedence at other online companies?"

His follow-up—we'll combine them together—is, "Absolute personal privacy is a right guaranteed by law and common decency. However, so is consumer protection. With respect to commercial enterprises, they have no right to privacy. In fact, they have an obligation to be transparent. So why not disclose the registration contact data automatically and transparently for commercial activity on the web including registration data and anticipating a potential response. For individuals that chose their own name or manage their own personal data inappropriately, isn't it the responsibility of the business owner to protect their own personal data with respect to their contact data with the business? Do their rights trump the potential harms to consumers by allowing

them to cloak the actual identity of the business?" I think, Alan, you're going to respond to this one?

ALAN WOODS: I am. Obviously there's a few theories and questions in there, but I suppose the first thing I'd say is I absolutely agree, Fred. It shouldn't be hard. In fact, the reason why it is hard is probably a question that we need to answer. We should probably be asking that question because I think the simple and probably flippant answer for today because obviously we only have a short amount of time is that, in the ordinary course of us being a controller, if we were not in the ICANN community being a controller, we would set those rules and we would be able to be far more direct in the rules that we're setting. To be honest, there wouldn't be much people coming back to us on that because that is the job of the controller: our legal obligation to set those rules. So that's not the situation we're in as a contracted party, in way.

I think, also just going to your point about billions of people being protected online, you're again overstating the amount of complaints that's out there, to be perfectly honest. All you need to do is look at [Shrems 2]. That is a very large, very public online company that is consistently before the courts and finding it. There's their prerogative to do it. It's not straightforward. It's not easy. But to be perfectly honest, I don't think that is true.

The next thing to see about is, again, we are not setting our own risk. The community is kind of setting our risk in this. We are advocating as data controllers for our data subject rights and for our registrants rights. The EPDP is exactly testing to that. Please

look at the transcripts of what we said, what we've been doing, the path from which we're on. But we are also bound to listen to the community, and not everyone in the community's interests are focused on protecting the data subjects rights. In truth, they're looking at it for their own specific interest. It's a very difficult proposition for us to do that. We have to play ball and we are very happy to do so to bring the best possible policy.

On your second point, very quickly, as I do not want to take up a lot of the time, the reason why legal versus natural has been a difficult one—again, I would urge you to go back and read all the transcripts of both Phase 1 and Phase 3 of the EPDP—is because our system was not built with privacy by default and privacy by design in mind. We can't just patch the system to make sure that we can perfectly delineate between that which is legal and that which is natural. We have said this many times. It needs to be rewritten from the start. That was never the job of the EPDP, but absolutely more than happy to start at the beginning and approach it from a privacy by design and privacy by default point of view, where we are protecting those who are protected and not putting those protections on people that do not have it under the law. I'm talking specifically legal persons on that one. So it's not black or white. Again, it's something we need to be very mindful of.

What I'll also say about as well is that you make a point about consumer protection. Look, somebody pointed that out to me during one of the EPDP meetings: clearly I was against consumer protection as well. It was annoying at the time just purely because, one, breaking the law for consumer protection processes is not a very good path to consumer protection. Also, if you look at it from

an LEA point of view, if somebody was using ill gotten gains data which was obtained illegally, well, then that will go to the very end and probably would effect fruits of the poison tree as the doctrine in law.

Finally, what I will say as well is, are not our registrants consumers as well? We are protecting those consumers as well, and we are absolutely bound to protect them.

So, for many reasons, this is much nuanced case. There's so many major discussions that need to be had on this. There are my initial, off-the-cuff remarks.

OWEN SMIGELSKI: Great. Thanks, Alan. Next question we have here is from Simon [Raveh.] "How do you deal with language if you get a data disclosure request? Do you enforce everything to be in English, or other supported languages? If not, how would you handle requests in languages not supported by your company, which can be as common as Spanish or French, or as uncommon as Korean? In EPDP Recommendation 3, it says, "Must be in English." I think he's referring to Phase 2. "But is it accepted in real life."

Who's going to answer this one?

BETH BACON: Owen, I happy to do that.

OWEN SMIGELSKI: Okay. Go ahead, Beth.

BETH BACON: There was a Beth in front of it, so I feel I might as well respond. Thank you very much for the question. It is a challenge, considering the domain name system is global, our companies are global, and the laws are global. So, yeah, it's a very important question.

Recommendation 3 does say that requests must be in English. That provides a level of consistency, and that is unless the recipient indicates another language is allowed. But that's just specific to the baseline request. It was intended to ensure that we don't end up with requesters expecting services in a language that the registry or registrar just simply doesn't have the expertise or operate in. But I do think that all contracted parties have the flexibility to allow or work with other languages.

I will say that I have seen requests and I know that the colleagues on this call have seen requests come through in varying languages. I will each out to staff. I know that others reach out to staff on the teams who actually speak those more common languages, as you say—Spanish, French (I guess the UN languages). We can usually find something. If it's a less common language, quite frankly, I Google translate. I do my best to at least get a flavor for what they're asking. If I can't, I certainly will respond and say, "Can you please provide this in English?" or, "I'm unable to translate this request myself." In the registry and registrar minimum document, we do talk a little bit about providing

translations where requested by the controller or the receiver of the request.

So I think the long and short is, yes, the recommendation does state a preference for consistency in English, but I don't know that there's a contracted that won't be flexible and try really hard to respond and understand a request. So hopefully that answers your questions.

OWEN SMIGELSKI: Thanks, Beth. We're going to give—there's another question outstanding for Beth. We're going to jump over to a question for Sarah here. Sarah, go ahead.

SARAH WYLD: Thank you. Hi. I'm responding to Laureen's two questions that are in the chat pod. Laureen, thank you so much for asking those questions. I anticipated that somebody might, and I kind of thought it might be you. So it's good to see you here today.

The first question is, "How many people participated in the survey?" I will say that we did have a small sample size of responders, but it was representative of a range of registrar and registry sizes, from small up to very large, and represents a significant portion of all gTLDs that are registered. This was our first attempt at gathering this type of data. We hope that, in the future, we will have even a broader pool. Right now, there's not uniformity across contracted parties about how or which data elements are tracked. So we did what we can with the data that

we had that lined up, and I think the SSAD reporting will be useful in that context.

Laureen's second question was, "For the 66% of requests that were denied or redirected, what was the breakdown for each subcategory?" That was something I was thinking about also. I think I wish I would have been more specific about that, but regarding this breakdown of denied and redirected, unfortunately we did not a get a lot of detail around that in the responses to our survey. So what I found was that, from all of our responders, it was all one or all the other. So we had some contracted parties say that they denied most of their requests, and we had some say that they redirected most of their requests. But we didn't really get responses saying "Both these outcomes happened. Here's the breakdown between them." It tended to be one or the other.

So, again, hopefully the reporting from the SSAD will allow us to have more detail around those outcomes so we can have even more clear reporting in the future. Thank you.

OWEN SMIGELSKI: Thanks, Sarah. Now we're going to a question from Brian Beckham. "What guidance or criteria are used to assess those in particular balancing?" I think, Beth, you said you're going to take that one?

BETH BACON: Sure. Happy to. Hi, Brian. Thanks for joining. I think that is an important question because, as I may have mentioned a few times, the baseline guidance in the law is vague. Again, the nice

thing is that it provides some flexibility for contracted parties and any other controller who's doing a review, but it also introduces a lot of uncertainty. So, when we do consider the balancing tests, it's always best –what I do and I know my colleagues also do—to look at those sources that are designed to provide authoritative guidance on these issues. So the European Data Protection Board. There's the EPDP. I'm sorry. The European Data Protection Board and the EPDP have way too similar an acronym. The European Protection Board has provided guidance in several of their publications. The ICO has also provided an extensive array of practical [ends]. If anyone has questions, I do recommend the ICO as a great source for any sort of guidance on evaluating requests, submitting requests—any sort of privacy questions. They're detailed. They're practical. They're put into practical examples as well. We also look at court cases such as the [Regis] case, and outcomes. Again, the European Data Protection Board, as well as the European Court of Justice will provide rationales and guidance that apply to the balancing test there that we can provide. In addition, the particulars of the case and the requester's reasoning, the nature of the data being revealed. Again, the balancing test is, is there a possibility for impact? It's not necessarily harm but an impact.

So I think those are things that we keep in mind and do a check on. So again, it's not a check-the-box, but it is flexible and we try and be very well-informed with those things that we consider.

I see that you would like to follow up, so I will let Owen work you in if there's others.

OWEN SMIGELSKI: [inaudible]. I think, Brian, we do have time. I don't know if you want to raise your hand to speak or if you just want to type it into chat. It's your call.

BRIAN BECKHAM: Thanks, Owen. I think I'm unmuted now.

BETH BACON: Yeah, we hear you, Brian.

BRIAN BECKHAM: Okay, great. Thanks, Beth, for the follow-up. What I wanted to ask was basically: recently there's been some blog posts, for example, from Tucows, which seem to hint at where there was a fair use question, for example, where there's an assertion of claim of potential trademark infringement—that this test would err on the side of non-disclosure. The way I heard you describe it, frankly, is what I feel matches more closely the intent of the regulations, namely that the good privacy laws that we now have in place aren't meant to immunize people from having to potentially defend the legal claim made against them. So I'm just curious. I appreciate you said that this can be subjective, that could be across registrars, or even across individuals, but to the extent that there could be some efforts within the Registrar Stakeholder Group, etc., to harmonize those, that could be really worth looking into because I think the benefits of consistency speak for themselves. But one thing that would, I think, be worth preventing is something of a, if I can put it this way, race to the bottom or forum shopping where registrants would register domain names

with registrars that they knew would not disclose as a matter of practice in these types of specific examples where there was a legal claim, even if it involves fair use. That really should be decided by a court or a UDRP panel and not, in my view and at least what I understand for the relevant guidance of these regulations decided in favor of a non-disclosure. Thanks.

BETH BACON: I think I'll start and then I might through it to Sarah, who happens to work at Tucows, since you did specifically mention that. I think that your question is well-taken and I understand your particular focus in that you're hoping that it doesn't become a suite of registrars who just lean on the side of denial or non-disclosure. Sorry. I apologize. My computer is freezing a little bit. I apologize. I do not think that we can provide, again, an authoritative checklist, but I will point you again to the registry and registrar document that notes the minimum—well, currently registrar but soon to be registry/registrar—data and the importance of providing the context. I think that's what allows folks who are doing the analysis to see what exactly you're asking about. Is there information? Should it be a different process? What's the problem you're exactly trying to solve? What is your purpose? What is your legitimate interest? So, again, it's all about providing the right amount of information. I think that really, really helps us understand If you've contacted the right party, if we can disclose and it's a legitimate disclosure based on that balancing test, and if you display those interests really thoroughly, I think that really helps.

Then I'm just going to, because you did talk a little bit about Tucows and her article, throw it to Sarah to close that out. Thanks.

SARAH WYLD: Thank you. Hi. Well, a few thoughts there. That was a really interesting question. I don't agree with characterizing a registrar who errs on the side of privacy as being a race to the bottom, and I also don't think it's accurate to say that the Tucows blog posts indicated that. So I know this webinar is focusing on more general contracted parties statistics overall, but, specific to Tucows, since you asked, if you review our numbers, you'll see that we do disclose data in response to the majority of requests and also that the overwhelming majority of request are related to intellectual property concerns. This was the case for the overall contracted party responses to our survey as well. So I don't think it's the registrars job to adjudicate trademark issues, as you say, but it is absolutely our obligation to follow data protection regulations and to make sure that we consider the full context of the request before completing a disclosure. Thank you.

OWEN SMIGELSKI: Thanks, Sarah. Thanks, everyone. We've got a few minutes left. Anybody else have any other questions? Feel free to put it in the Q&A pod or, if you like, raise your hand and ask your question live.

All right. Can we unmute Franck?

FRANCK JOURNOUD: Hi. Can you hear me?

Hmm. I'm not sure you can hear me.

OWEN SMIGELSKI: Yes, we can hear you, Franck.

FRANCK JOURNOUD: Oh, sorry about that. Hi. Thank you for this webinar. I just wanted to ask a follow-up question to Sarah. In literally her last sentence, she said something like, "Tucows happens to disclose data in response to a majority of the requests," or something like that. But earlier, I think it was Beth who was presenting statistics across, I think, all contracted parties or at least contracted parties that responded to the survey, and there the rate of disclosure is significantly lower. I appreciate how not every contracted party can have exactly the same rate of disclosure and non-disclosure and redirection or whatever as every other contracted party, but can you explain why there might be significant discrepancies between the stat of one versus the stat of another?

SARAH WYLD: Yes. Thank you, Franck. There's kind of a lot there. Firstly, I will say you're right—thank you for pointing it out—that I did misspeak a little bit. So when I was referring to the similarity between the Tucows stats and the overall stats, the similarity specifically is about the type of requester that we are getting. But indeed, on average, Tucows actually disclosing in response to more requests than the industry average.

I'm really sorry. Now that I said all that, I forgotten what your actual question is. I'm so sorry. Can you type it down for me or something? Or can somebody remind me?

FRANCK JOURNOUD: I don't know if my mic is still on.

SARAH WYLD: Yeah.

FRANCK JOURNOUD: Okay, it is. Well, my question was, appreciating that not every contracted party can have the exact same stats as every other contracted party, still, with the fact that there can be significant differences—for example, Tucows, I think you said, positively discloses in response to a majority of requests, versus, I think, the stats for the rest of the industry say it's a much lower rate of disclosure—how do we explain such significant discrepancies?

SARAH WYLD: Part of it is that Tucows, as Graeme just put in the chat, has a really good relationship with most of their requesters that come to us. So we've educated them and seen a real increase in disclosure rates due to requesters understanding the process and understanding how to make requests and what is legitimate. Other than that, I think the variance really comes from just that there's the pool of responders that we had. Some of them denied the vasty majority of requests or redirected the majority of request,

and I think that results in stats that just show it's just so different. Different parties respond so differently. Yeah, it's hard. It is hard to correlate and explain. Again, I know I've said this one already, but hopefully, once we have the stats from the SSAD, we'll have even more data to pull from, so we'll have more accurate information or more robust information. I hope that helps.

BETH BACON: Owen, would you mind if I also just offered a small follow-up?

OWEN SMIGELSKI: Sure. Go right ahead. Then we'll go to Ashley and close out. Thanks.

BETH BACON: Thanks. Sarah's answer is 1000% correct and wonderfully thorough. I did want to note however also the things that impact, apart from Tucows, on those on the other stats in the other parties in the ecosystem. I mean, humans are reviewing these things. We have different requirements. Each company has different appetites for risk. There's different jurisdictional requirements that can impact disclosure. Certain companies have different relationships with either law enforcement or the requester, as Tucows does, that can increase or decrease their ability to disclose on a more routine basis.

In addition, with regards to registries, there is a high percentage of what looks like a no, but I will say, from a PIR perspective, that the vast majority of those—I don't have that specific stat because,

again, we don't have consistent stats across; we don't all record exactly the same things or we're not able through our systems to pool those particular stats, so we worked with what we had—no's are "Please see the registrar. It's the more appropriate party to discuss," or, "The discloser we will able to disclose because it was a privacy-protected registration and there was no PII. So we're happy and can easily disclose that. There's no personal data."

I will offer—maybe this is something for the registries and registrars to think about so we can get that snapshot of the ecosystem of what we're doing across the system—is [that we] think of a set of stats that maybe we could as a group focus on so that we could provide updates or insights. Again, that's just an idea from myself. I'm not speaking on behalf of registries or registrars. But maybe that's something we can think about that would be a service to the community. Thanks.

OWEN SMIGELSKI: Thanks, Beth. We've got Ashley in the queue, and then after that we're going to have to close it out because we're approaching the end of our allotted time. Ashley?

ASHLEY HEINEMAN: Hey. Thank you. I just wanted to note for everyone that I think it's important to note that we're still learning as companies, as registries, as registrars. I think this is a good opportunity to give a baseline of where things are before we get into the full-blown implementation of the EPDP Phase 1 policies. I think this is an honest attempt to show where we are, how we're going to evolve,

and that we really are trying to make this work and help people help themselves to make this work. So I'm hoping that this can be something that we can continue to build upon, find additional ways to share information that we have but also find ways to improve the process overall because I think there's a lot of education that needs to happen on all sides, whether it's the companies figuring out how best to deal with this balancing test, getting used to it, getting comfortable with it, but also those individuals and companies who are making requests. It's not going to be perfect from day one, and I think that's very obvious in what we're saying in these stats. I just hope that we can work together and continue our commitment to make this a good process overall.

So I just wanted to add those few words and put a little bit of additional context on this. Thank you all to the folks who presented today and participated. Thanks.

OWEN SMIGELSKI: Great. Thank you, Ashley. With that, I really don't have much more to say that wasn't planned this way, but Ashley came in and did a great summary and ending for this. So thank you, everyone who attended and participated and asked questions. I hope it was informational. This will be posted shortly to the GNSO calendar—both the slides as well as the recording. Thank you. All right, thank you everybody. I think we can end the recording now. Thanks.

[END OF TRANSCRIPTION]