Summary of GNSO Public Forum on Whois

São Paulo, Brazil

4th December 2006

Author: ICANN – Maria Farrell

Version 1.0

Table of Contents

Introduction by forum Chair, Rita Rodin (Board member representing the GNSO) 5

Section 1 Preliminary Task Force Report on the Whois Services 7

Presentation by Jordyn Buchanan, Chair of the GNSO's Whois Task Force 7

Presentation by Ross Rader, GNSO Councillor and Whois Task Force member, Registrar Constituency 13

Presentation by David Maher, Whois Task Force member, Registry Constituency 25

Presentation by Steven Metalitz, Whois Task Force member, Intellectual Property Constituency 27

Open microphone session 35

Nils Montan, President of the International Anti-Counterfeiting Coalition 35

Ross Rader (in response) 35

David Maher (in response) 35

Bruce Tonkin, Melbourne IT 36

Danny Younger (written comment) 38

Steve Delbianco, Netchoice Coalition, member of the Business Constituency. 38

David Maher (in response) 38

Steve Metalitz (in response) 39

Ross Rader (in response) 39

Steve Delbianco (in response) 39

Ross Rader (in response) 40

Rita Rodin (in response) 40

Jim Reid (Telnic) 40

Jordyn Buchanan (in response) 41

Jay Westerdal, Domaintools.com 41

Kieren McCarthy, journalist (written comment) 42
Amadeu Abril i Abril 42
Steve Metalitz (in response) 43
Amadeu Abril i Abril (in response) 44
Steve Metalitz (in response) 44
Wendy Seltzer, ALAC 44
Margie Milam, MarkMonitor 45
Ross Rader (in response) 45
Margie Milam (in response) 46
Ross Rader (in response) 46
Margie Milam (in response) 46
Marliyn Cade, GNSO Councillor, member of Whois Task Force, Business Constituency 47
Bob Hutchinson (identified self later as with Dynamic Ventures) 48
Person unknown (in response) 48
Bob Hutchinson (in response) 48
Ross Rader (in response) 49
Bob Hutchinson (in response) 49
Ross Rader (in response) 49
Steve Metalitz (in response) 50
Jordyn Buchanan (in response) 50
Mawaki Chango, GNSO Councillor, Non Commercial User Constituency: .. 50
Avri Doria, GNSO Councillor, member of the Whois Task Force 51
Kristina Rosette, GNSO Councillor, member of Intellectual Property Constituency 52
Steve Metalitz (in response) 52
Kristina Rosette, GNSO Councillor, member of Intellectual Property Constituency 52
Ross Rader (in response) 53
Kristina Rosette (in response) 53

Ross Rader (in response) 53
Jordyn Buchanan (in response) 53
Robin Gross, IP Justice, GNSO Councillor, member of the Non Commercial User 54
Section 2 – Draft procedure on potential conflicts of Whois requirements and privacy laws 55
Presentation by Kurt Pritz, ICANN 55
Marilyn Cade 62
Kurt Pritz (in response) 62
Marilyn Cade 62
Kurt Pritz (in response) 63
Marilyn Cade 63
Kurt Pritz (in response) 63
Marilyn Cade 63
Sharil Tarmizi, Government of Malaysia, Chair of the Governmental Advisory Committee 63
Jordyn Buchanan 64

Introduction to Public Forum Summary

This summary has been prepared by ICANN staff to maximize access to and awareness of the presentations and public comments made during the GNSO Public Forum on Whois on 4th December, 2006. It incorporates the presentation slides made, along with other comments by the presenters. It is hoped that this summary will enable members of the Whois Task Force, GNSO Council, and the ICANN community as a whole to understand the current state of play regarding Whois policy developments in the GNSO.

Procedurally, the public comments received during this forum and on the ICANN website will form part of the public comments report in the Final Task Force Report on Whois Services to be submitted by the task force to the GNSO Council in early 2007.

The full text of the proposals / draft procedure discussed in this document – and a further opportunity to provide public comments - can be found at :

Preliminary Task Force Report on Whois Services
http://www.icann.org/announcements/announcement-24nov06.htm

DRAFT Procedure for Potential Conflicts between Whois Requirements and Privacy Laws
http://www.icann.org/announcements/announcement-2-03dec06.htm

Introduction to the GNSO Public Forum on Whois by forum Chair, Rita Rodin (Board member representing the GNSO)

We need to think more about how we foster some compromise in some of the diverse positions on Whois. This panel will educate you about the status of the work and facilitate dialogue and information from the community. Questions and comments from the audience will facilitate the continued work of the GNSO.

We will address two topics: first, the preliminary report that the Whois Task Force has completed which has been posted for public comments, and second, the draft procedure on conflicts between Whois requirements and local privacy law.

The Preliminary Task Force Report on Whois Services is the result of a process begun in 2003 when a multi-stakeholder GNSO task force was convened to study Whois issues. The comments and information received on this report today will be considered by the task force, starting the 16th January when the public comment period closes.

This task force has been chaired by Jordyn Buchanan who will talk about the task force report and the process. You will also hear from Ross Rader of the Registrar Constituency and David Maher from the Registry Constituency about the OPoC proposal, the operational point of contact proposal in the task force report. Then you will hear from Steve Metalitz of the Intellectual Property Constituency about Special Circumstances proposal.

Section 1 Preliminary Task Force Report on the Whois Services

Presentation by Jordyn Buchanan, Chair of the GNSO's Whois Task Force

Presentation slides are reproduced below with speakers' comments on each slide.

Terms of Reference

- Define the purpose of the contacts displayed in Whois
- Determine what data should be displayed for public access in Whois; determine how to access data not available for public access
- Improve process for notifying registrants of inaccurate Whois data, and improve process for investigating and correcting inaccurate data.

We are currently looking at three principle items in our terms of reference. The first of those items is to define the purpose of the contacts displayed in the Whois; to figure out what those people in the Whois –the registrant, admin contact and technical contact - what it means to be one of those people.

The second goal that we have is to figure out what information should be displayed in the public access version of Whois. Right now there is only one way of displaying information in the Whois and that's to display a bunch of contact information about all of these various contacts. The other part of that discussion

is to decide whether if any information is removed, how people should be able to get access to that information if it is not made available through the public Whois.

The last area we are focusing on is improving the accuracy of the Whois data. If there is inaccurate Whois data, there is an obligation for registrants to keep data accurate -- not only do you have to provide it at the time you register but you also have to keep that information up to date over time. We are looking at ways to make the process of improving accuracy of Whois data more effective.

Timeline

- Preliminary Report was published Nov. 24
- Public comments taken until January 15
- Final Task Force meeting on February 12; Final Report is Published
- Council consideration
- Shortly thereafter: Board consideration

We published our Preliminary Task Force Report on November 24th for public comments until 15 January. (Link: http://icann.org/announcements/announcement-24nov06.htm) We encourage people to make written public comments regardless of their participation today.

We have recently put together a calendar for completing the rest of our task force work. The goal is to have a final task force meeting on February 12th, 2007. At that point, we would publish our final report which will hopefully incorporate all of the feedback we have received as part of the public comments. The Final Task Force Report will then be submitted to the GNSO Council.

Policy Development

- For a while, Task Force work was focused on using OPOC proposal as a template
- Recently, Special Purposes proposal was introduced as well
- Other discussion:
  - Display even less information
  - Allow registrant to delete domains instead of having information revealed
  - Some tiered access discussion

For quite a while, the task force used the OPoC proposal as a template for most of our discussions. Fairly recently, the Intellectual Property Constituency introduced another proposal called the special purposes proposal. Both of those proposals are included in the current Preliminary Task Force Report.

We have had some other discussion about various other topics or proposals as well. One idea in that area is that the OPoC proposal would remove the information about the registrant's name.

Another similar idea that's more privacy focused is if there is a complaint about some bad use of a domain name and the complainer wants to get access to the contact information of the domain holder, instead of turning that information over to the complainer, that the domain holder will have the option of saying "I would rather delete the domain, I will not use it for bad things anymore but I want to keep my information confidential."

Outstanding Issue: Access to Data

- How do people get access to data removed from Whois?
- Ideas:
  - Contact registrar
  - Mechanism for information to be revealed in a UDRP dispute
  - Request access if removal is no longer valid, or domain is used for bad purpose
  - Anyone that signs a contract agreeing not to use the information for bad purposes
- We need your input! What makes sense?

The most important outstanding issue we have right now in addition to the conflict between the ideas of the OPoC proposal and the special circumstances proposal, is access to data. If information is removed from the Whois, how should interested parties get access to that data?

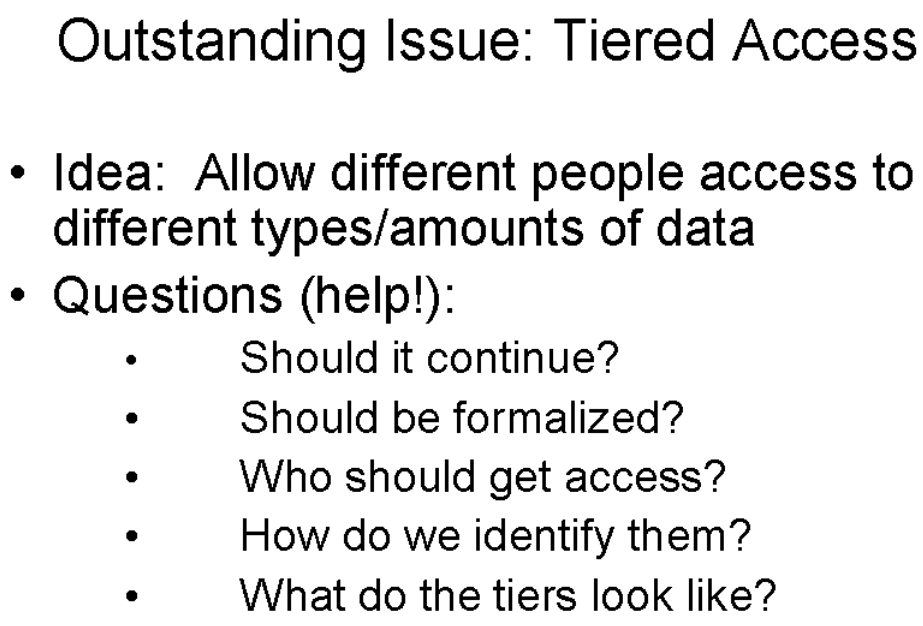
One idea discussed for accessing unpublished data was to simply contact the registrar and ask them for it and work with the registrar to get that information. That mirrors the status quo because there is no formal mechanism to get access to data that is not published in the Whois today.

The next mechanism is to make sure that if data is removed, that the UDRP still works. The UDRP generally requires some knowledge of the registrant contact information to file the complaint, so working out some sort of mechanism within the UDRP to accommodate for any information that might be removed.

The third idea is if you had information removed, but the reason it was removed is no longer valid, someone could complain and have your information put back in. Or, if you were using your domain name for a bad purpose, then there would be some adjudication process by which they could complain and get access to your information. We haven't defined what "bad purpose" means.

The last idea is that anyone that signs a contract saying they are not going to use the contact information for a bad purpose would be able to get access to the information. So you would have one tier of data that's available to everyone in the public and that would include some limited set of information. Anyone that agreed that they are going to use the information safely and carefully could get access to a richer set of information.

We haven't really actually explored any of these ideas particularly carefully. This is one area in particular where we would heartily welcome input.



Early Whois work focused a lot on tiered access. It's appealing because a lot of this discussion focuses around personal contact information in Whois in some cases, and people have privacy concerns about that.

On the other hand, there are a lot of very legitimate needs to get access to some of this information in certain circumstances. So if we have a way of limiting that information to just the people who had these strong legitimate needs, that might be a nice solution to this problem.

However, as we discussed tiered access, we realized there's actually a lot of access questions that arise that we haven't been able to successfully grapple with in the task force. There are typed of tiered access that take place in the status quo today very informally. And should we even continue, get rid of the tiered access that happens today.

If we are going to allow it to continue, should it be formalized and if so, who should get access to the information?

One common idea is that law enforcement should get access to this information. How would we identify that someone is actually a legitimate law enforcement agent?

And the last category is, once we resolve all these other questions, what sort of information do we provide to what people?

Presentation by Ross Rader, GNSO Councillor and Whois Task Force member, Registrar Constituency

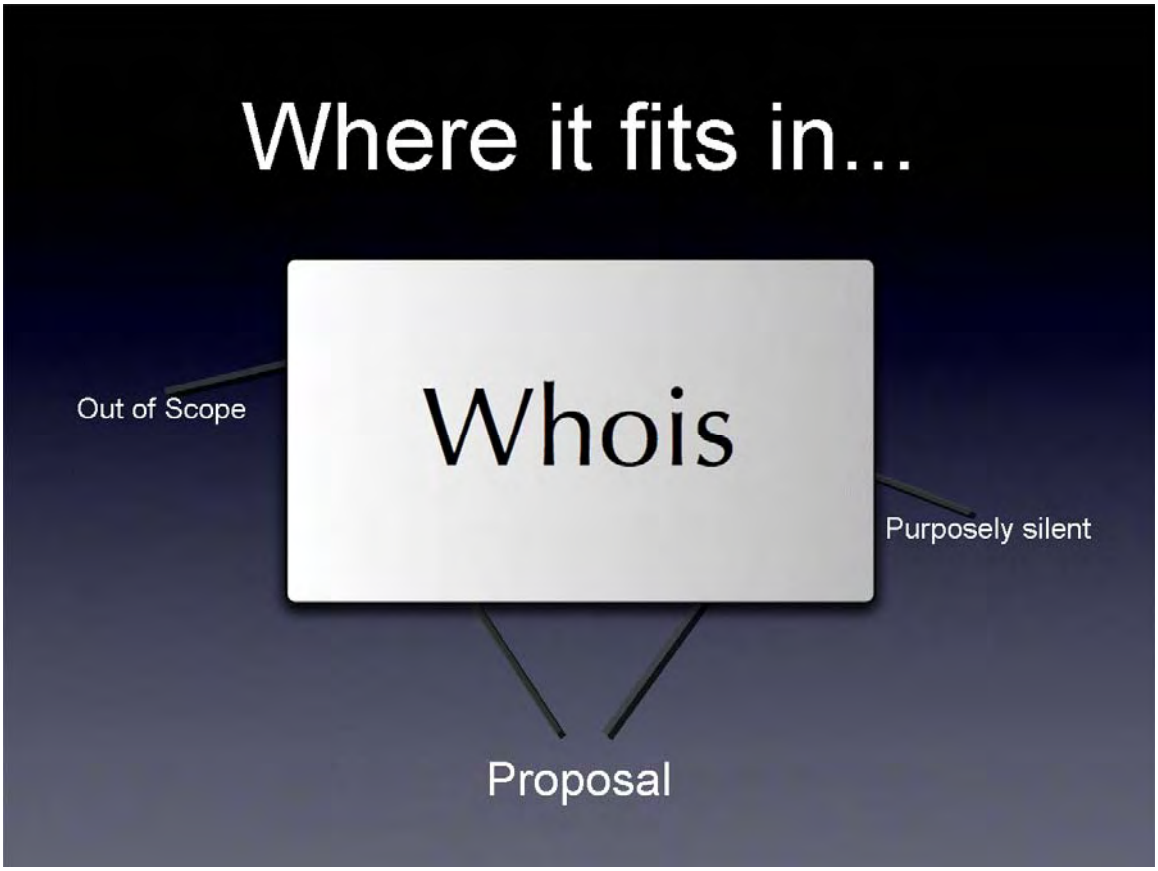
History of the proposal:

- First draft created by independent working group April, 2005 in Mar del Plata, Argentina in response to the lack of progress on Whois issues
- Was widely circulated, discussed and modified with dozens of stakeholders throughout 2005 and into 2006
- 7 different versions produced
- informal input solicited from all constituencies and major stakeholders prior to presentation to Task Force
- received agreement in principle from several key constituencies
- Presented to GNSO Whois Task Force on January 18, 2006
- Became an official work product of the Task Force at that point
- Subject to significant review and revision since that time

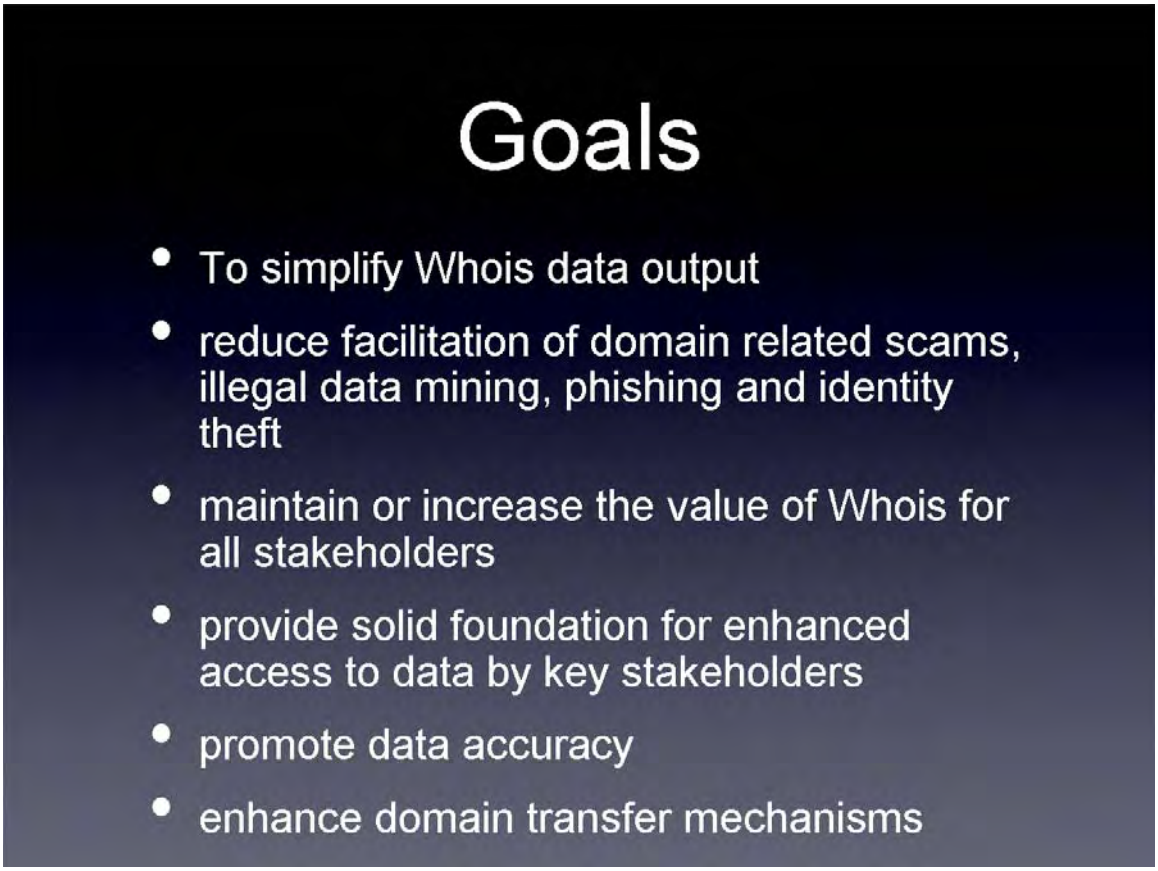
In January of this year, the proposal went from being an informal document. It was presented to the Whois task force as a position statement of the registrar constituency. The registrar constituency had voted that as its position i believe in December of 2005. At that point. So it was out of our hands and into the larger community for finalizing.

Since it became an official work-product of the task force, we have had a lot of discussion about the OPoC proposal, and a lot of further changes. There has been a lot of good progressive, substantive growth in that document.

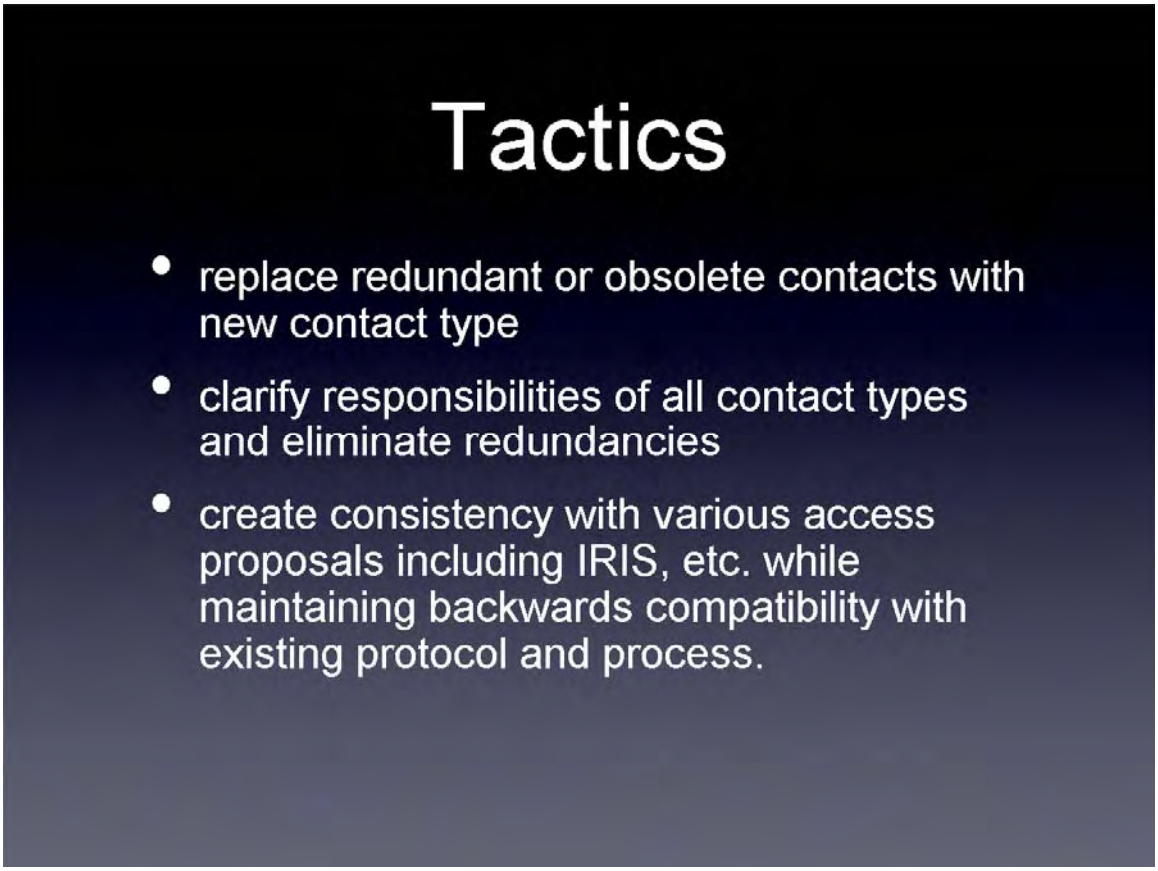
So here's where it fits in:



The operational point of contact doesn't deal with all of the issues that the Whois Task Force is trying to solve for. The OpoC proposal is silent on the issue of access to unpublished data. The proposal deals with the publication and management of data.

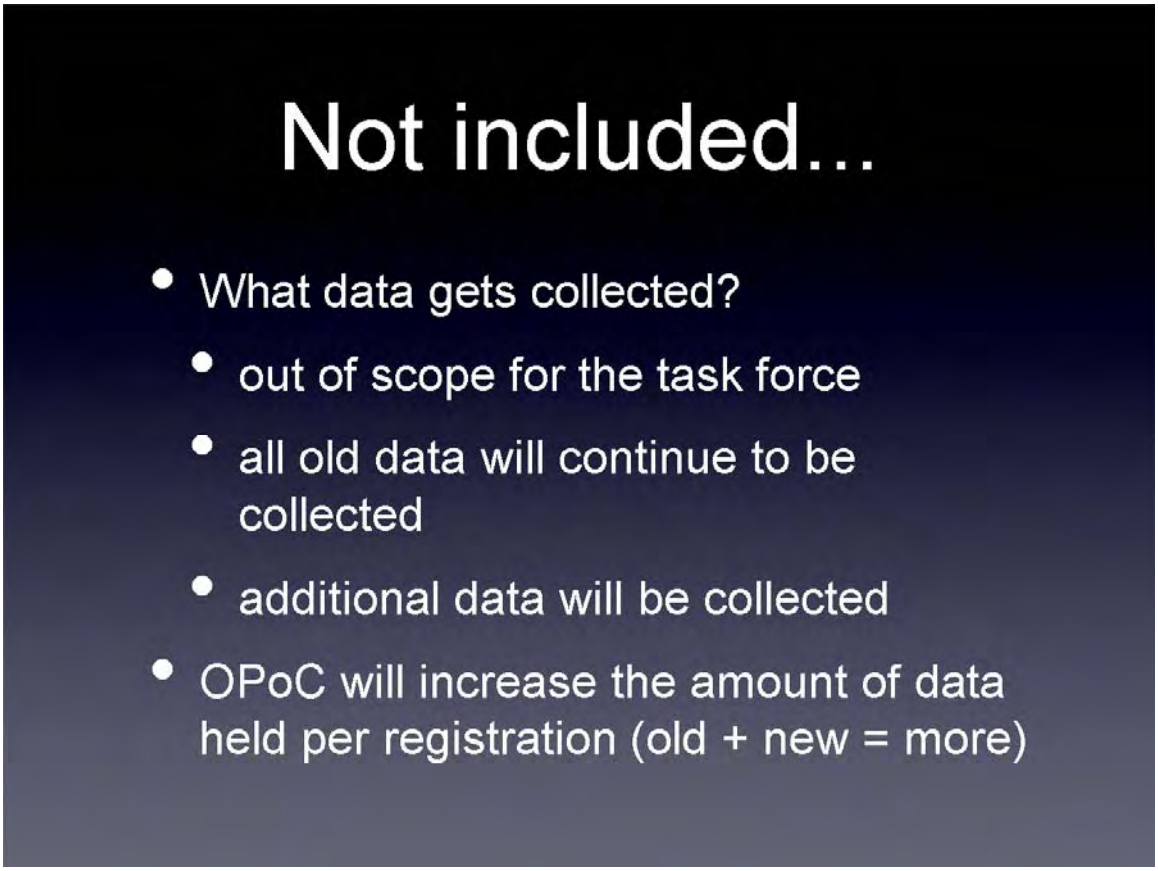


So how were we going to achieve those goals? We first looked at the data that was in there. We realized that the old contacts, the administrative technical and, to a smaller extent, the billing contact had really lost their meaning, not only to the users of the DNS but also to the registrant community.

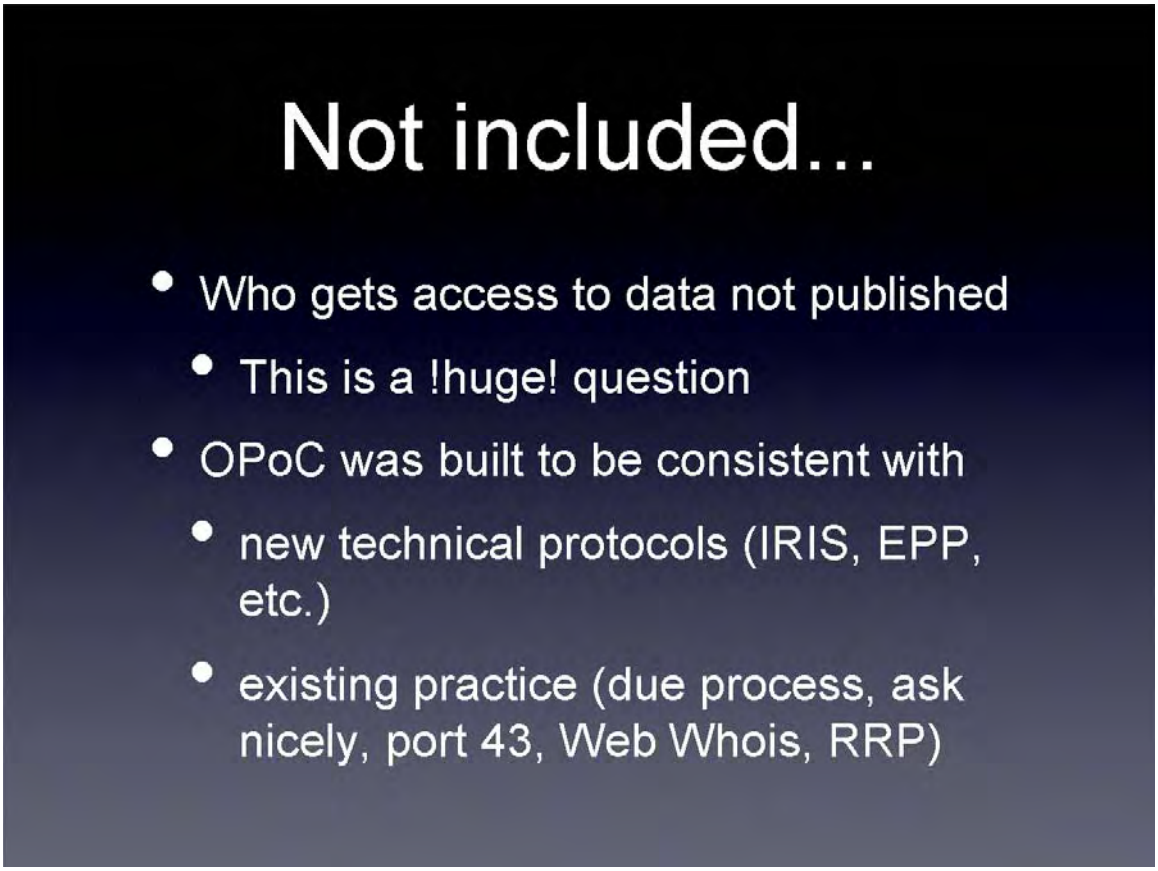


Most of the functions originally envisioned for those different contact types were actually being performed by one or two people related to the registered name holder.

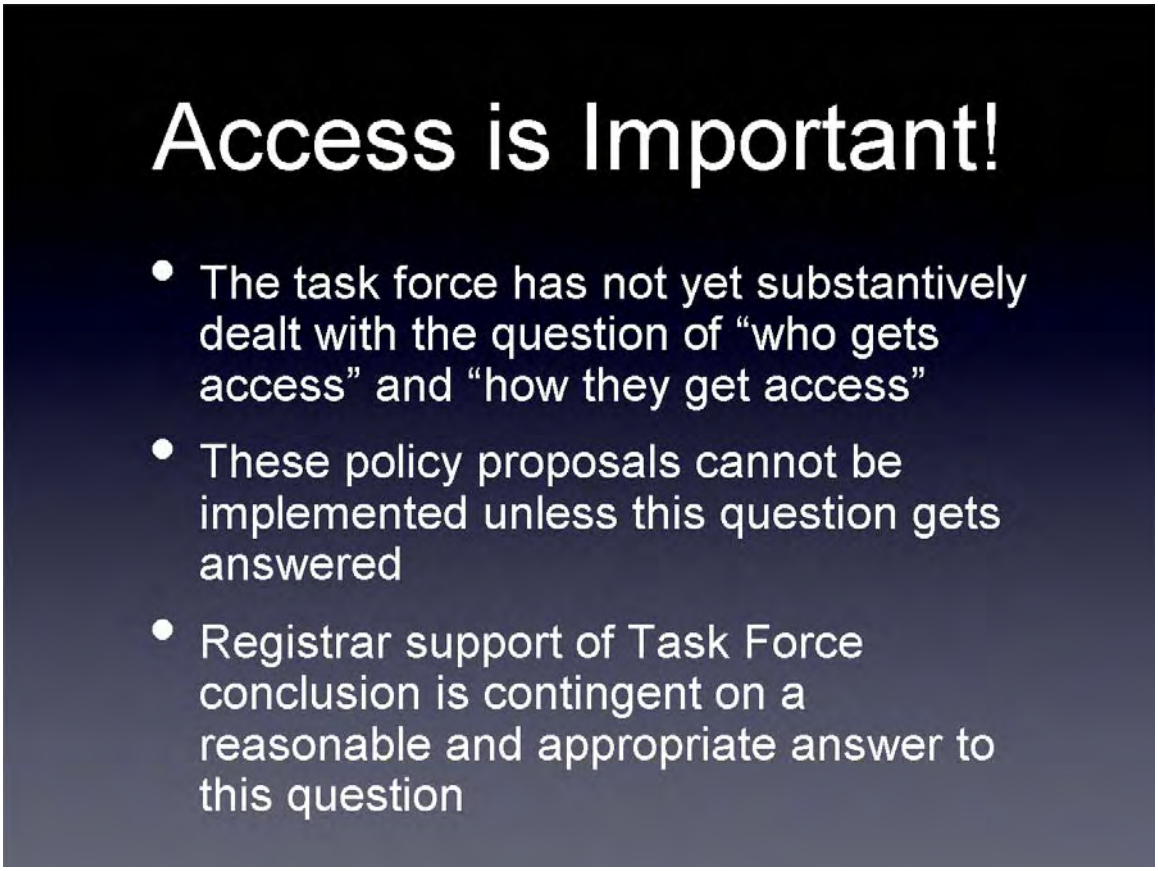
We wanted to clarify those responsibilities. If there were any redundancies, we wanted to eliminate those and to create consistency with existing access proposals, for example, IRIS, while maintaining some semblance of backwards compatibility with the existing mechanisms.

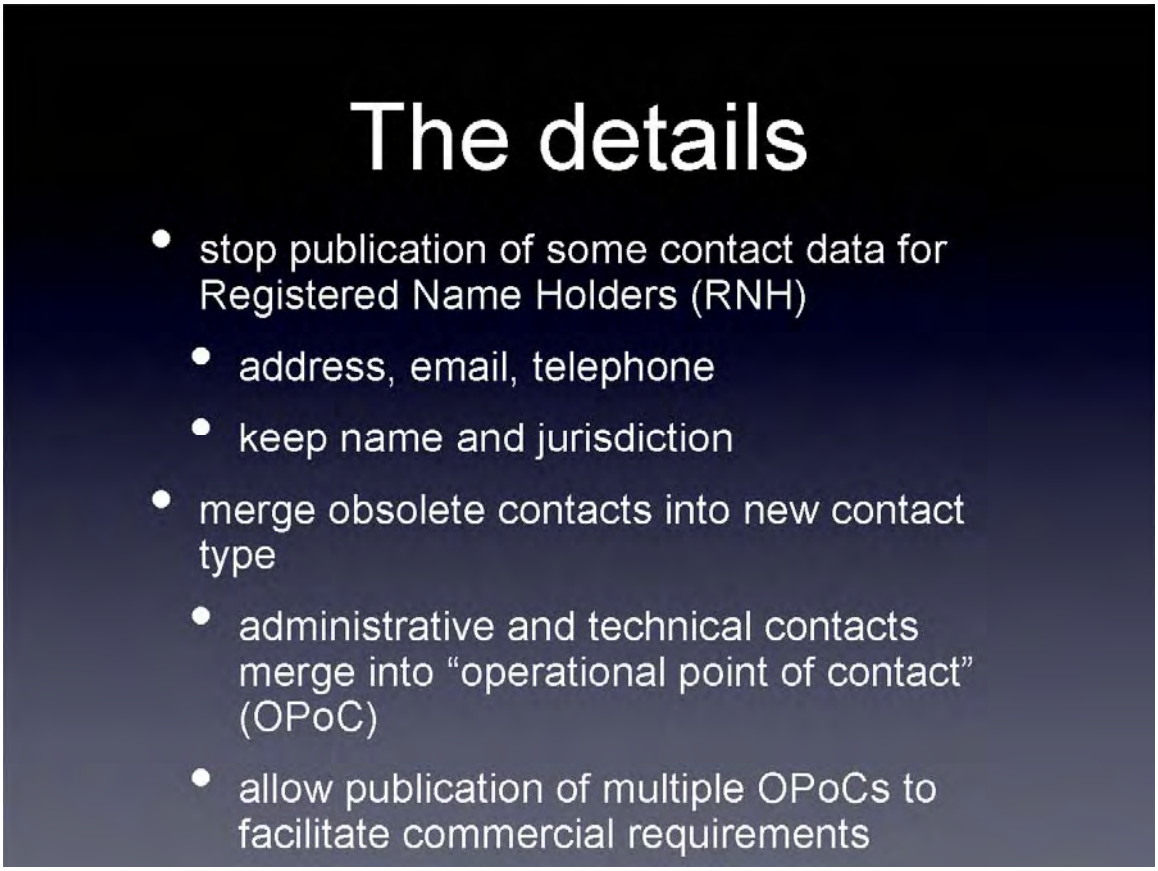


Registrants will still have to provide their telephone number and street address, even though those data points may not appear in the Whois at some point. So the OPoC proposal will actually increase the amount of data collected and stored on registrants.



As Jordyn pointed out, one of the big questions the task force has yet to deal with - but is not dealt with in this proposal - is who gets access to this data. The OPoC proposal was built to be consistent with any provisions that will ultimately made on tiered access. It lives very nicely with the IRIS/EPP protocols and with existing practice, e.g. requesting or getting the data through port 43 or through web-based Whois forms.


Access is Important!
The task force has not yet substantively dealt with the question of "who gets access" and "how they get access"
These policy proposals cannot be implemented unless this question gets answered
Registrar support of Task Force conclusion is contingent on a reasonable and appropriate answer to this question

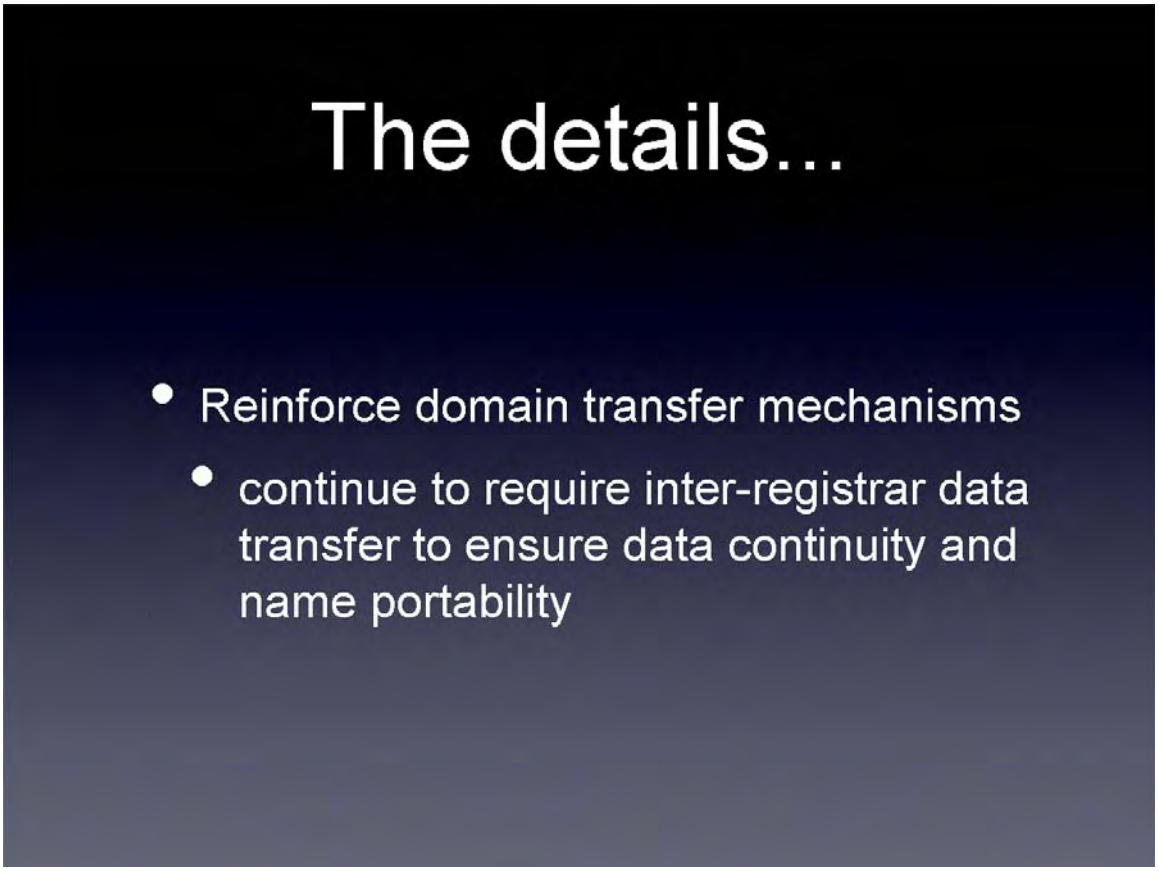


The specific data that would no longer be published via the Whois, would still be collected but not published, would be the address of the registered name holder, the e-mail address, telephone number. The name and the jurisdiction of the registered name holder would still be published.

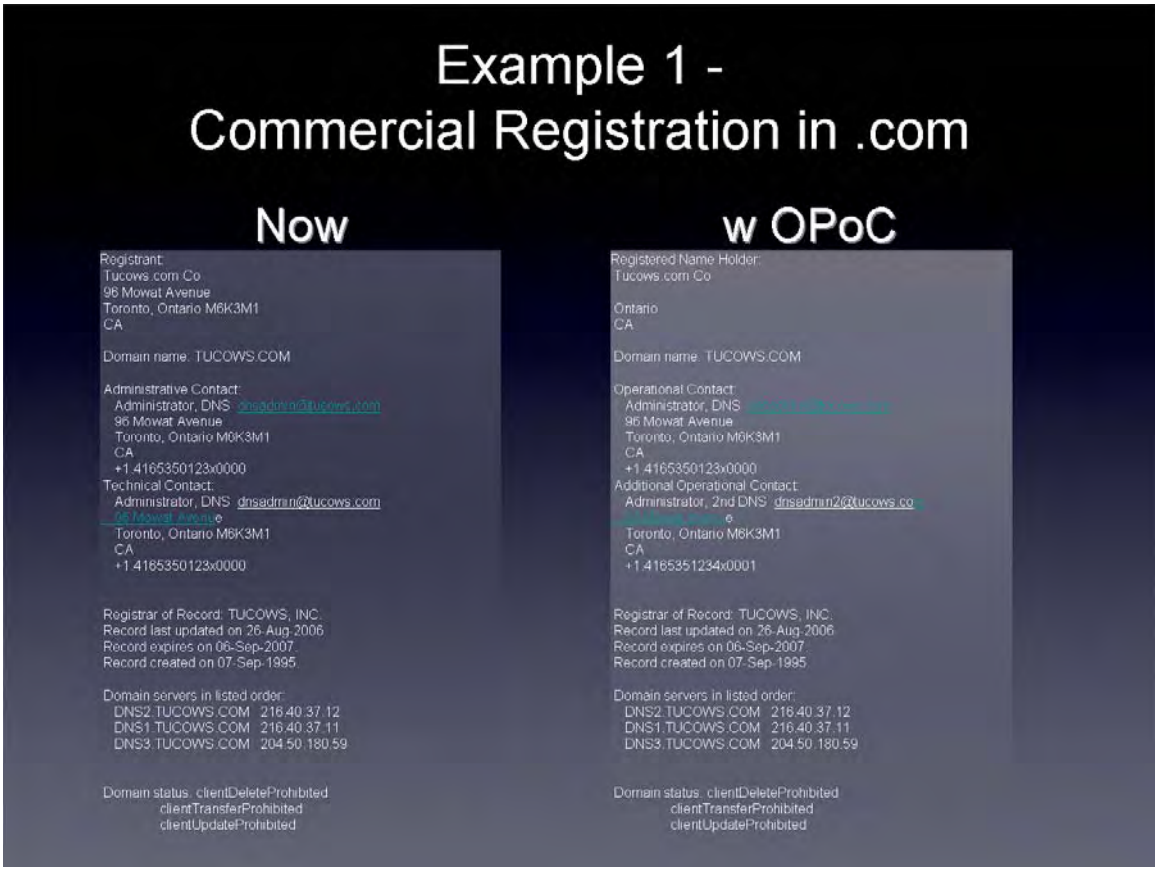
The administrative and technical contacts would merge into a new contact called the operational point of contact.

We would allow registered name holders to specify multiple OPoCs to ensure that the existing commercial requirements could be fulfilled. In a large company, it's not uncommon for companies to appoint different people to manage different aspects of the domain name, and this proposal certainly tries to facilitate that.

Some of you may be familiar with the Whois Data Problem Reporting System. The OPoC proposal makes that more substantial so that specific actions are taken within specific periods of time. We are also looking to create additional correction requirements.

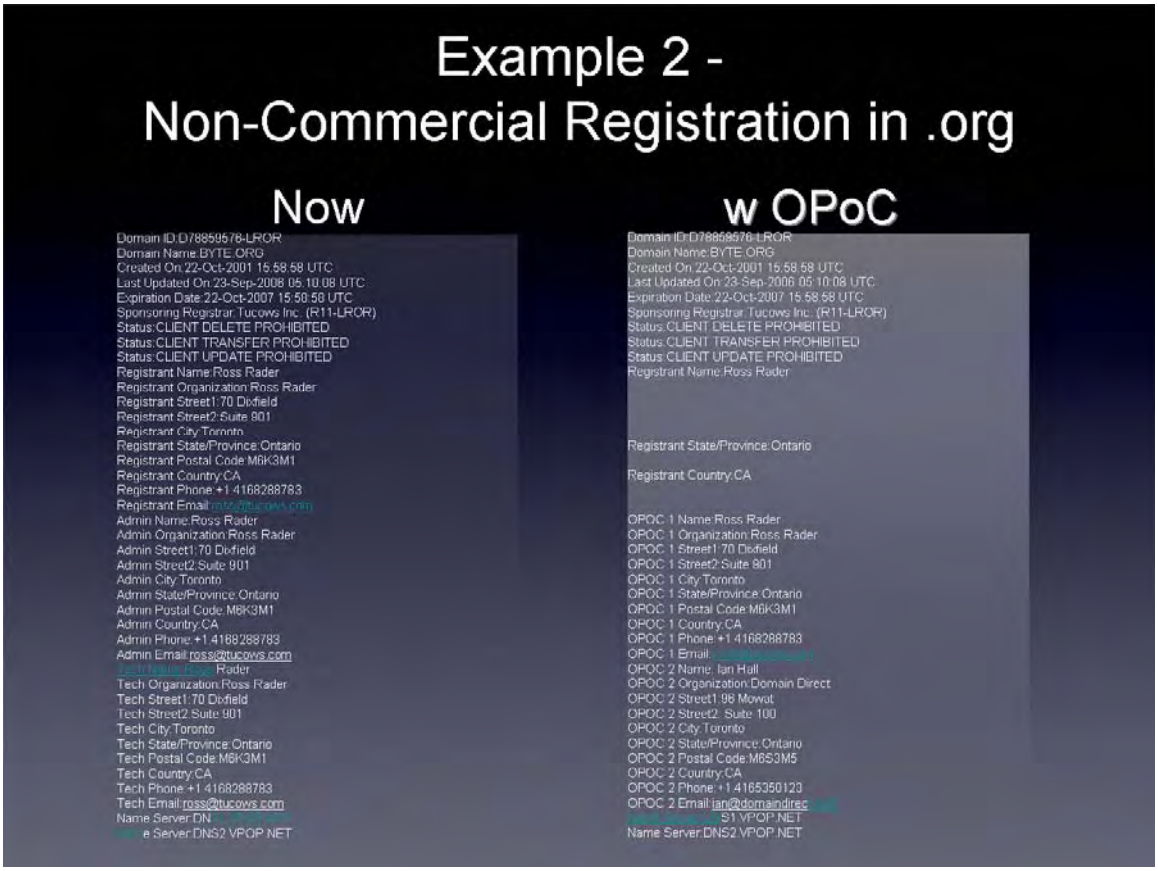


Here is an example of what Whois output might look like under the OPoC proposal:



This example is a registration in com. On the left-hand side of the screen you see what it would look like for Tucows.com. You see the registrant information up top, other pertinent details, domain name, contact information, et cetera. What this would look like under the OPoC proposal is on the right. Very little information would actually be removed in the case of a commercial operation.

I have also created a slightly harder to read example that shows you what a dot org Whois sample might look like:



Again, the street address, telephone number, et cetera, would also be removed. The administrative and technical contacts would be re-displayed as OPoC details. So in terms of the practical impact on the absolute data payload, there are very few changes.

Presentation by David Maher, Whois Task Force member, Registry Constituency

(no powerpoint slides)

I am Senior Vice President of Public Interest Registry, the manager of the registry of dot org. The registry constituency has an independent interest in this.

We publish the data that is provided to us by the registrars. We don't collect any data, but we publish it, and there are two different kinds of registries. One is called thick and the other is called thin. Com and net are thin. Most of the rest of the registries now are thick and publish more data.

We strongly support the propping set forth in the OPoC. There are a few details, but OPoC is a major step in the right direction.

The interest of the Registry Constituency, fundamentally, is that individual registrants of domain names have a reasonable expectation of protection of their personal privacy, and we support that. We don't see the need to give the home address and home phone number of every individual who has ever registered a domain name. Historically, there might have been some reason to do that, but that's really ancient history now.

There is a big difference between data collected and data published. And one of the good things about the OPoC proposal is that it clearly makes that distinction.

Assuming, as we do, that the OPoC proposal gathers sufficient data for law enforcement authorities, the UDRP or for intellectual property interests, we would support a reasonable means, tiered access or whatever it is, to give access to the parties that need it legitimately. The details of how that's done can be worked out. It may not be easy, but that if there is some attempt to reach a consensus, we can do it.

We certainly insist, however, that it is not necessary to publish generally all the data that is collected.

A few very specific questions that the registry constituency has about the OPoC:

There may not be enough data collected under this proposal for some of our sponsored generic top-level domains, like dot coop, dot museum, etc. They have specific needs about their registrants which are quite different from com, net, or

biz, info etc. There might need to be some tweaks in the process to get the information for the sponsored generic top-level domains.

Also, there are some differences between the thick and thin registries that would have to be worked out.

This is significant because the com and net are such large registries and such large collections of data. But this is a detail that can be worked out without great difficulty.

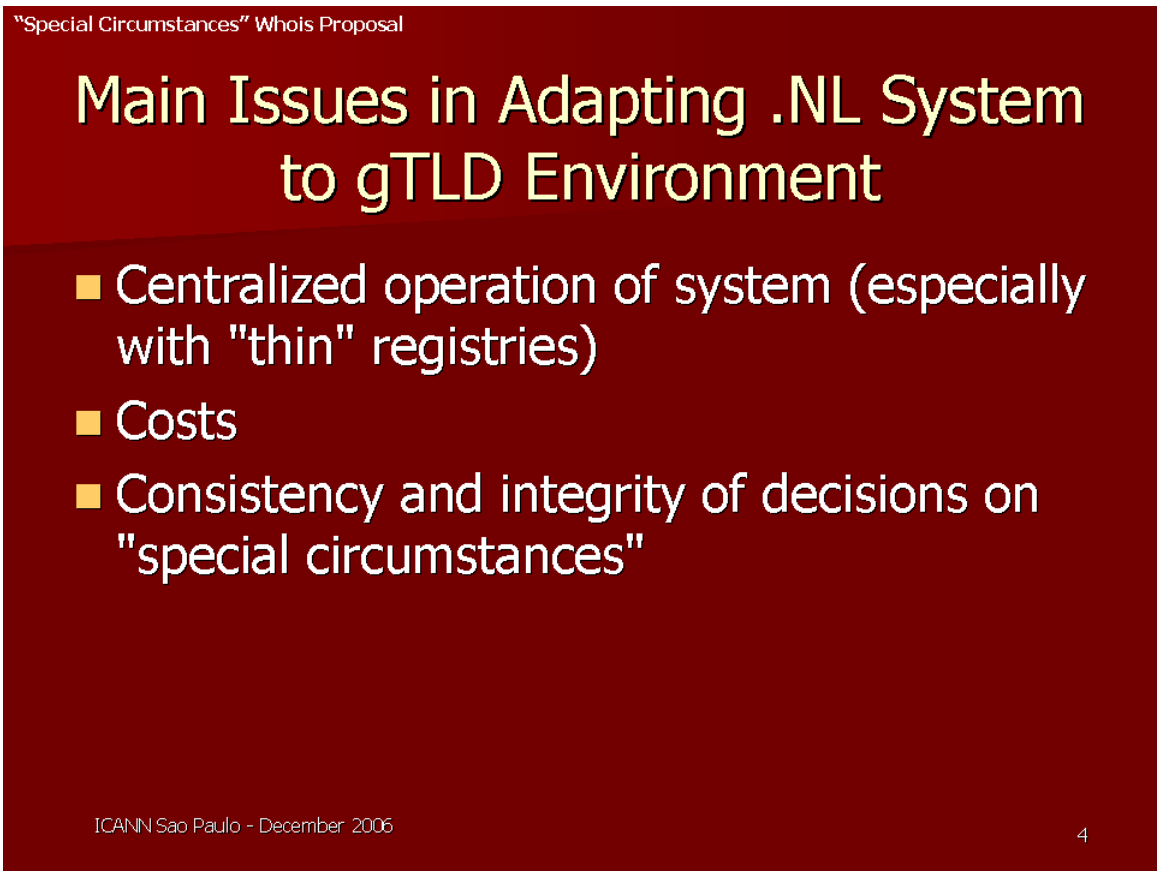
Presentation by Steven Metalitz, Whois Task Force member, Intellectual Property Constituency

Our proposal is modeled on a system that has been in use since 2003 in dot nl, the ccTLD in the Netherlands. It's about the ninth largest ccTLD in the world. There was a presentation about it at the Montreal meeting of ICANN in June 2003.

Like the status quo in the gTLD world, the full range of Whois data, registrant information, administrative contact, technical contact, is publicly available for most registrants. But the dot nl system does suppress from public access some Whois data of some individual registrants who demonstrate a need for special treatment.

So what we are talking about here is the gTLD status quo plus some added privacy protection for individual registrants who show that they need it. This has been in operation for three years in .nl, a country that is subject to the EU data protection rules.

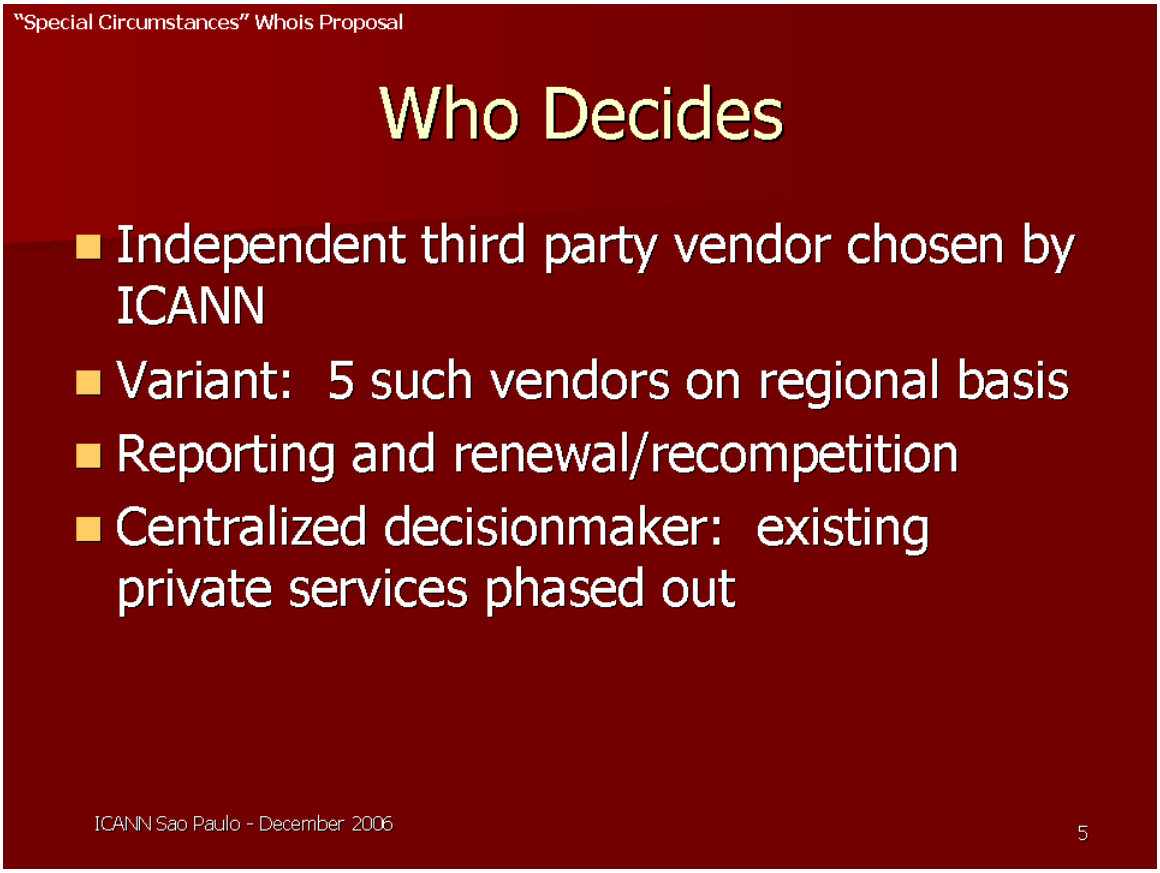
Our proposal based on dot nl is like the OPoC proposal in that it is focused on the issue of publication of data, and leaves to one side the issue of access to data that's not published. It may be a little bit less pressing in our proposal because there will be less data suppressed from publication, but it still is an issue that would need to be resolved.



These issues in adapting .nl are discussed in more detail in the Whois Task Force report.

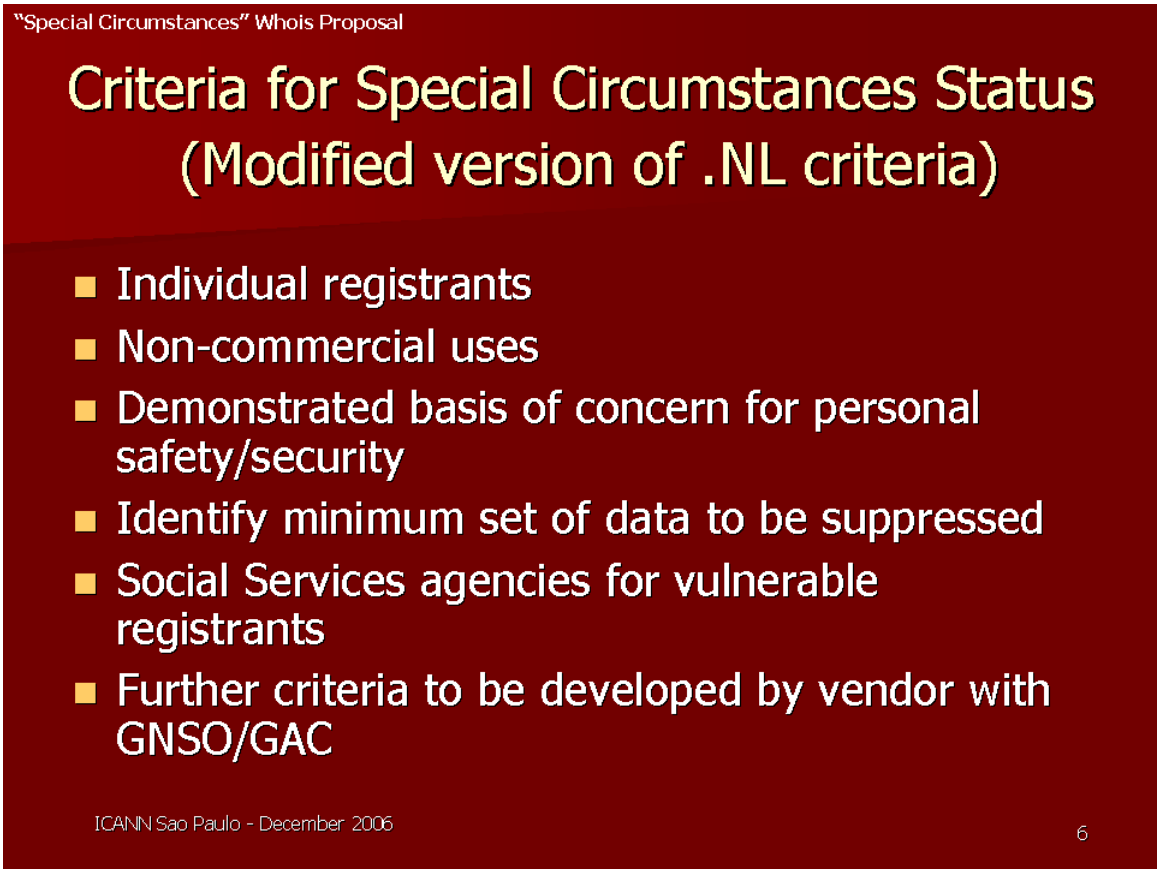
Decisions about what data would be suppressed from public access are made on a centralized basis. That creates some problems in a thin registry setting where it's the registrars who hold virtually all the Whois data that has personally identifiable information in it. So there are issues about cost and how those are allocated.

Then there's a big issue about having consistency and integrity of decisions on whose data should be suppressed from public access. Since all of the data is now held by each of the 800 registrars, that's a significant issue.



Who decides whether a particular registrant's data would be withheld from public access? Our proposal is that an independent third-party vendor be chosen by ICANN, or perhaps five such vendors on a regional basis.

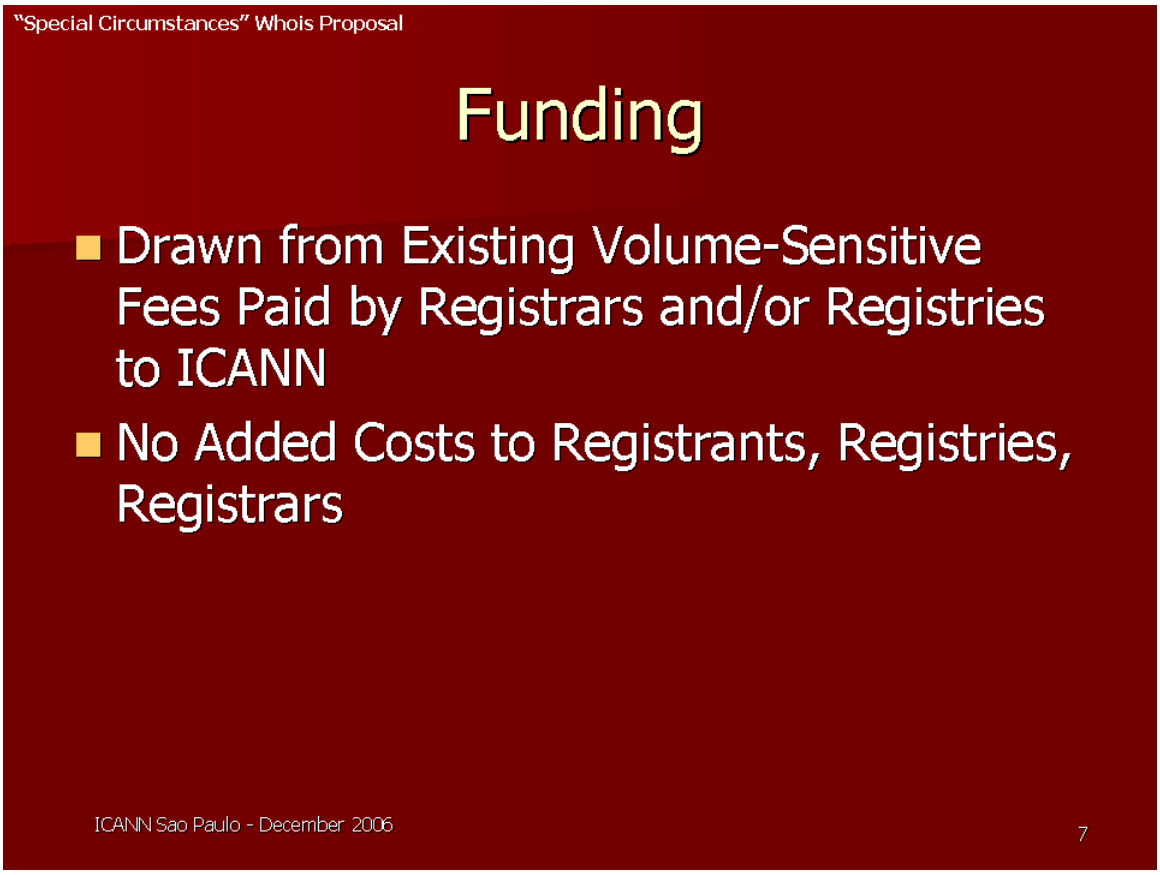
They would have to meet reporting requirements. There would be rules about renewal or re-competition of that contract. But there would be a centralized decision-maker, and the current system in which there are private services that are operated by registrars or by alter egos would be phased out. We would have one decision-maker applying one set of criteria.



I will call your attention to the second point here about noncommercial uses, because a number of people have indicated that this adds a lot of complexity to the proposal that perhaps is not strictly necessary. To demonstrate or to monitor whether the domain name is being used for non-commercial purposes adds a layer of complexity that may not be necessary. That criterion is not in the dot nl criteria. So we'll be interested in people's reactions about whether the non-commercial use criterion is necessary or not, or whether it's more trouble than it's worth.

There would be a provision also for agencies that represent vulnerable registrants, such as a battered women's shelter or something like that, to qualify.

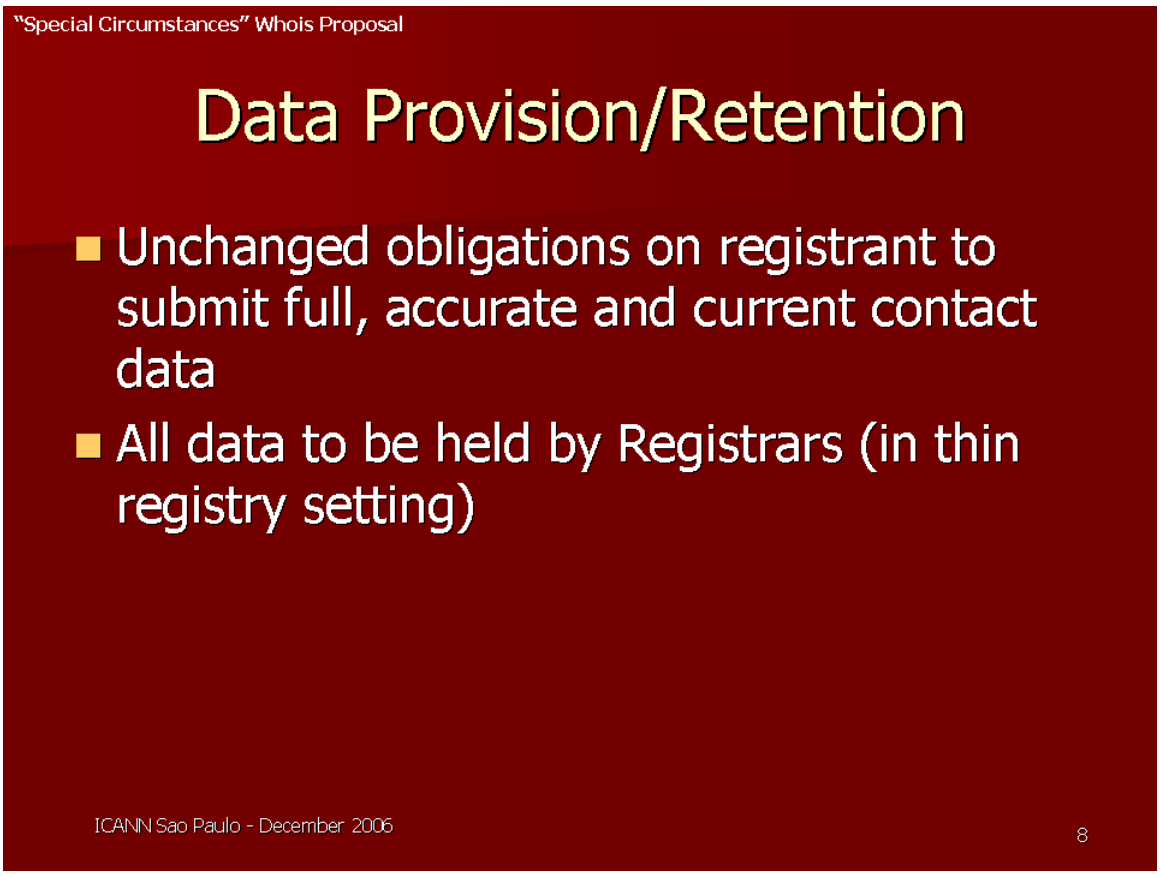
Obviously further criteria need to be developed in order to implement this.



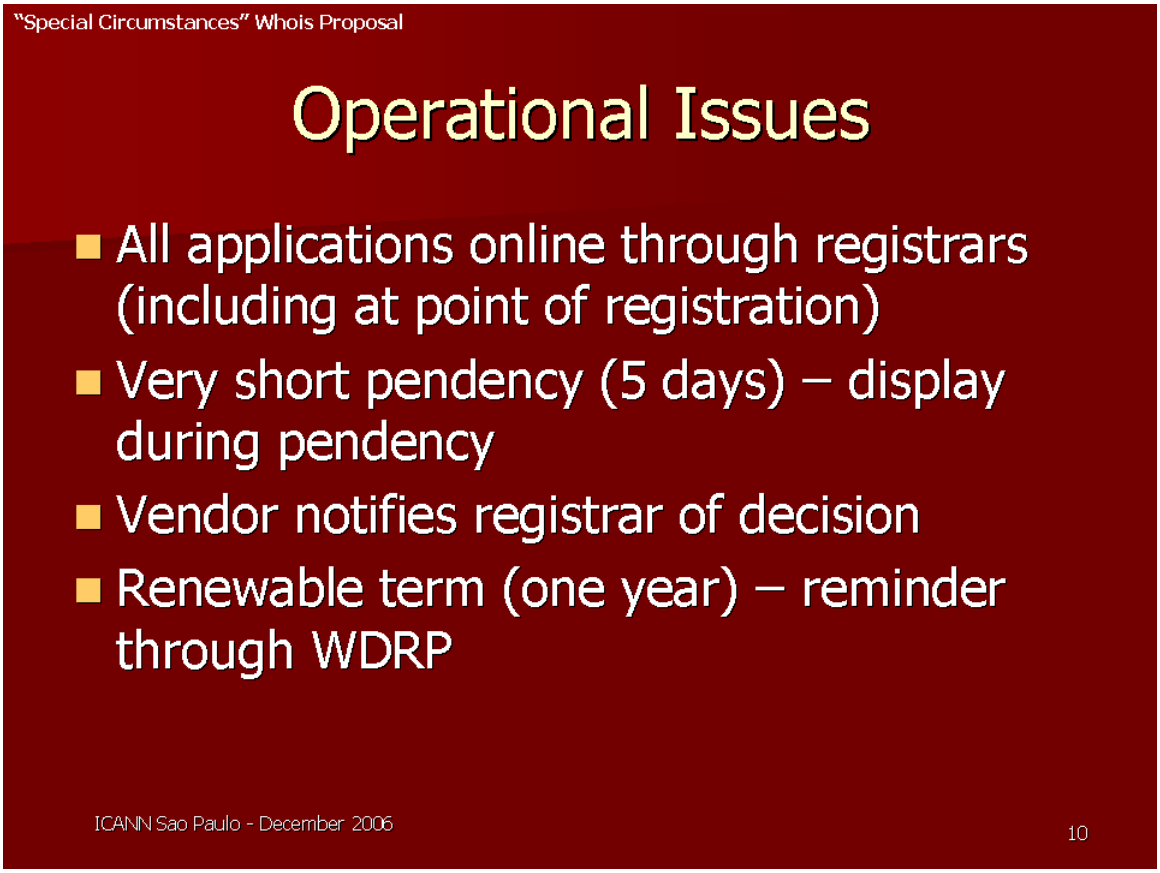
This can be paid for from the existing volume-sensitive fees that are paid by registrars or registries to ICANN. It's going to vary depending on whether it's a thick registry or thin registry situation. The goal should be to do this, if possible, with no added cost to registrants, registries, or registrars.

The status quo is that registrants pay to have some of their information suppressed from public access through private registration services. Some people object to people having to pay for privacy protection, and that argument is at its strongest when you are talking about people who have a demonstrated need for privacy protection.

The change is to the data display for the registrants who demonstrate special circumstances:



A registrant who doesn't demonstrate special circumstances or isn't eligible for it -- for example, a non-individual registrant – so the data that's displayed would be the data that's displayed now. It would be the name and the mailing address of the -- of the registrant. A registrant with special circumstances who shows that certain data needs to be removed, would have the corresponding data for the registrars substituted.



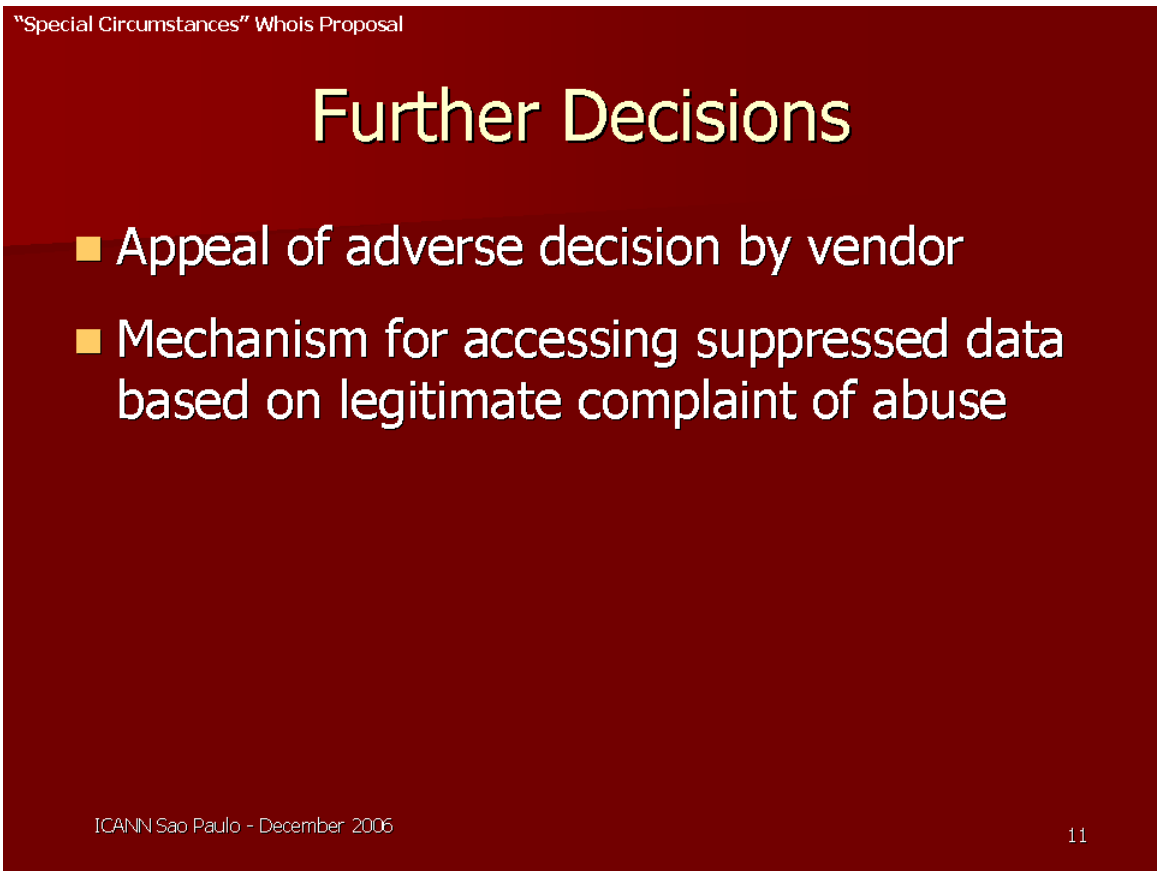
You could have a short pendency period if you have very clear criteria, so that people have a good sense about whether this is appropriate for them.

The vendor notifies the registrar of the decision, and then the registrar acts accordingly, in terms of what data is made available in Whois.

During pendency, the display won't have someone who doesn't qualify have their data inadvertently exposed, so there are some provisions in our proposal on that.

The status would be available for a renewable term. People's circumstances change. We already have a system where the registrars are supposed to remind registrants about their obligation to provide full, accurate Whois data every year (the Whois Data Reminder Process, WDRP). So registrants are reminded that if they want to keep this status, they need to reapply.

There are two issues that we have flagged that need to be addressed:



What is the mechanism for appealing if the vendor says, applying the criteria, that, you're not eligible for the special circumstances proposal.

The other is the point that David and Ross both mentioned, and it applies really to all these proposals; what is the mechanism for accessing this data if there is a legitimate abuse situation? As Jordyn indicated, we didn't reach any consensus or even a great deal of area of agreement in the task force yet, but that is certainly something that would need to be addressed no matter what the proposals were.

Open microphone session

Nils Montan, President of the International Anti-Counterfeiting Coalition

It seems that these two proposals put certain burdens in different directions. Often in law enforcement or in the enforcement of intellectual property rights, speed is an important element, if there's an infringement taking place.

How would your proposal deal with that problem in cases of the law enforcement of criminal counterfeiting activities or the like? You often want to act quickly. You don't want infringing activity to go on without being able to take some kind of action. Every civil law in the world that I'm aware of, including the TRIPS agreement, focuses on the ability of the intellectual property owner to take very timely action.

Under OPoC, would you know if one of my members wrote and said they wanted the address for infringement purposes, how would you know that they were legitimate, what kind of hoops would they have to run through, et cetera?

Ross Rader (in response)

One of the misconceptions about the OPoC proposal is that it will eliminate the potential or the capability for people to contact the registrant. One of the responsibilities of the OPoC is to forward a request to that registrant, so even though my personal home phone number for my personal domain name will no longer be in the Whois, it will be the responsibility of the OPoC to ensure that i get notices in a timely manner from people such as yourself.

The issue of law enforcement access to that data in criminal investigations is still a live issue that the task force hasn't quite dealt with yet. Translation: the OPoC proposal punts on that issue, and further discussion is required.

David Maher (in response)

The registry constituency certainly recognizes the need for speedy access, and we're not talking about five or six days. We're talking about instantaneous access. The tiered access concept is flexible enough to handle that.

You raise the question of: who is a legitimate law enforcement body?

My answer to that is that every registry and every registrar operates under the jurisdiction of some law enforcement body. Dot org is in Virginia. We would probably refer a request from some suspicious would-be law enforcement body to the FBI and ask them to tell us whether it's legitimate.

We have gone even further, to propose that there might be Interpol or some other group that could filter requests. Our proposal is that the law enforcement bodies would have instantaneous access, just as they do today.

My concern with Steve Metalitz's proposal is that it starts from a false premise that privacy is something that you have to request or earn. I think everyone is entitled to privacy. That's why the data should not be published from the beginning, but we can work out some reasonable accommodation for your needs and the needs of law enforcement bodies.

Bruce Tonkin, Melbourne IT

I want to make a few general comments about both of those proposals and where they fit into an overall system.

From the point of view of the overall system for gTLDs is – the system has a characteristic that there is very low verification of registrant data when a domain name is registered, and the only verification that registrars do is verify that registrants can pay. So there's some fraud control and sometimes that involves checking the address against credit card address registries to see whether the payment is fraudulent.

But assuming the payment is correct and goes through, there's no real verification on whether the phone number actually works, whether the e-mail address works, whether the physical address exists. So that's sort of the up-front side of it.

The other side of it is that when we display this information, it is data mined and most organizations that have a lot of information about individuals need to be very wary about how this data is mined or retrieved electronically and then potentially misused. Registrars have introduced their own services for privacy, which are at a small additional cost to the registration fee. Those services have a huge take-up. There's probably 30% of registrations through our company that have been registered with a privacy system of some form. That shows that

people are concerned about their data being openly available to anybody, and are concerned how that data gets used.

The OPoC proposal is an ideal proposal for dealing with this unrestricted data-mining issue. It allows for appropriate data to be displayed that lets a member of the public contact the registrant using that data, and that OPoC is then responsible for forwarding the request on.

I'm also very conscious of the need that because we have this low-cost process and we have this huge volume of registrations - and in fact, every day we probably get an additional million names for various reasons I won't go into - this is a burden for the community that's trying to protect their businesses, whether it's at a consumer protection level or whether it's protecting of business interests. And at that level (protecting business interests), we need a second tier. This tier should be based on the fact that some authentication is done of the person that's requesting the data. And at this tier it's reasonable that they should be able to access more detailed information about the registrant, but that's based on a tiered access. That still allows registrars to put privacy services in front of that, if they wish. But this is a second tier where we're authenticating the party that's accessing that data and that party needs to commit that they will only use the data for legitimate purposes and particularly won't use the data for unsolicited marketing.

Then where I see Steve's proposal coming is at a third tier, that is, where we do a much stronger authentication of the end registrant, which is not the case in the earlier steps. There is some justification for that registrant needing to bury their data very deep. And at that layer, if it passes this special consideration proposal, then in my mind the only way that that data can be retrieved should be via court order. Using an analogy, because we seem to be using law enforcement analogies, essentially at that point they've gone into a witness protection program. Steve's proposal is, in my mind, the equivalent of a witness protection program, so it's obviously needed in a number of special circumstances.

So I see three tiers, the first tier being the OPoC proposal that the registrars have put forward which deals with open public access to Whois; the second tier, which doesn't seem to have been discussed by the task force in any depth, but at least a standardized process for authenticating who it is that's asking for the data and the party that asks for that data needs to commit that they're not going to use it for unsolicited marketing. The second tier is where I see the counterfeiting groups and the intellectual property groups, et cetera getting access. And then the third tier is the witness protection program tier, where someone really doesn't want to be found for whatever reason, and that requires a lot more verification. You'd actually have to fully identify the person, they'd have to have justification,

and then need a very high level, like a court order, to be able to retrieve that data.

Danny Younger (written comment)

We understand that when consensus is both present and ratified by the ICANN board, that those under contract with ICANN must abide by such consensus policies. However, when consensus is clearly not present, as appears to be the case with respect to the current Whois policy, why aren't we releasing registries and registrars to formulate their own independent policies?

Steve Delbianco, Netchoice Coalition, member of the Business Constituency.

My question is directed to Ross, Steve, and David with respect to your programs and your proposals. Setting aside the notion of publication and access, I ask you to address questions about the data collection policies. Would your proposals prevent registrars from imaginative policies that circumvent intent, such as proxy registration? In other words, would they prevent proxy registration?

And the second question is: how would your proposals then, on the back end, beef up ICANN's ability to enforce whatever new policies have been developed, so that registrars have to actually follow the rules in a diligent and time-sensitive manner?

David Maher (in response)

I'd like to read you a piece of news that i just got this afternoon:

Godaddy, which is one of the major registrars in the world, has just received a United States patent, no. 7,130,878, and the abstract of the patent begins: "a system and method of proxy domain name registration permits a would-be domain name registrant anonymity."

We're going to have to live with proxy registrations and anonymity, partly because of local law. You may well have registrars operating in a jurisdiction where anonymity is fostered. Of course there are many jurisdictions where the

reverse is true. There's no answer, I think, to the question of what are we going to do about proxy registrations, other than accept the fact that there will be some.

To me, proxy registrations illustrate the fundamental demand for protection of personal privacy, and we ought to take account of that.

Steve Metalitz (in response)

To answer Steve Delbianco's two questions, the first is that our proposal would phase out the private registration services in favor of a centralized service that applies objective criteria.

Based on the news David has just announced, people who are providing proxy registration services have to worry about whether they're infringing somebody's patent as well, but I won't get into that.

[laughter]

In terms of beefing up enforcement, that's a very good question which neither proposal really addresses. It's out of scope for this task force. Also out of scope is one of the points that Bruce raised, which is; should registrars be doing something more to authenticate the data that they collect at the time of registration as far as registrant contact data That is a topic very much worth discussion, but it is not part the remit of this task force.

Ross Rader (in response)

Yes, Steve (Delbianco), you raise some great questions, but I also think it's equally or perhaps more important for this task force to focus on what is actually within the scope of this task force. So as it relates to data collection or the use of proxy services, et cetera, those are all great discussions. But it's certainly not something that this task force can actually deal with at this point in time.

Steve Delbianco (in response)

There's a risk of simply answering that question by saying "out of scope," since whatever proposal we come up with, we will sooner or later confront this issue of enforcement and proxy registration. So if you truly believe it's out of scope -- and

i respect that opinion -- we ought to have it in scope at such point that a policy has been developed that represents the consensus policy.

Ross Rader (in response)

I would agree. If there is an issue there, I would encourage the business constituency to bring that forward. I would certainly welcome that discussion, whether it be over cocktails or at council.

Rita Rodin (in response)

As a board member, I think proxy registrations and looking for anonymity in connection with domain name registrations is something that, in general, people are talking about. While that specific issue may not be in scope, it is something that has been considered and discussed at the task force level, and will be something that ultimately needs to be discussed as per your last statement.

Jim Reid (Telnic)

I work for Telnic, although I'm speaking here in a personal capacity. I'm actually struggling with this at the moment, trying to formulate Telnic's Whois policy. One of the concerns we have is that, broadly speaking, a Whois publication of personal individual data is in contravention of the UK and EU data protection law. So unless the user gives explicit consent, their data cannot be published through Whois.

Somehow we have to formulate a policy which complies with the ICANN guidelines, but is also compatible with UK and EU law. This is a very difficult problem to solve, and I fully support any efforts that this task force can do to try and square that particular circle.

Further than that, for those who have got legitimate reasons for access to registrant data, and such as with intellectual property disputes or law enforcement purposes, I don't think Whois should be the first port of call. There should be a lightweight mechanism where people with a legitimate right to use the data can get to that data fairly quickly without having to go to the expense of a court order.

Although having said that, the advice I'm getting from the UK lawyers for Telnic is our ‘is don't disclose unless someone has a court order’. And we tell people, "come back and let the court sort it out, so that Telnic doesn't make any value judgments about who has got a legitimate right to access that data or not.

Finally, I would like to say something about tiered access. It’s also got some potential, and some drawbacks, too. Taking into account data protection measures specifically in Western Europe, I could only disclose data to somebody if they will comply with EU data protection law. So if I have to pass this data to someone, say, in the US, they must either have a contract with Telnic or abide by safe harbor provisions or the EU model clauses that govern personal data transfers. That would have to be incorporated somehow into any kind of tiered access arrangements.

But this will become very, very complicated because ultimately that will become a problem because of different jurisdictions and different rules for data protection. Thank you.

Jordyn Buchanan (in response)

I'll note that one of the policies that the Whois Task Force has already adopted at least partially addresses one of your concerns, which is that in some cases, there may be a conflict between the Whois requirements and various laws. The policy that's also been ratified by the board and is now a consensus policy instructs the staff to create a procedure to resolve where there's a conflict between national law and contractual requirements ICANN imposes with regard to Whois. Kurt Pritz is going to give a presentation on that procedure later.. So hopefully you'll get some more insight into that particular component of your concerns.

Jay Westerdal, Domaintools.com

I've done the Whois thing for quite a long time. I have a Whois portal, and one of the most common things I hear from the people that have private registrations is that they don't want their e-mail address in Whois because it gets spammed by robots. Beyond that, they don't really consider domain Whois privacy much of a service beyond that.

As far as the address where the person physically resides, you don't know where you're going to be serving a subpoena or some kind of legal document to this

person that may be infringing on your rights, and having that available is helpful when you're going to a court.

So I think that has to be taken into account that there is a physical address associated with the domain name and a jurisdiction where you should be suing this person that's infringing on your rights. You may not want to tip the person off by going through the privacy service. You may want to serve them directly before they have a chance to do something. As you go through the proxy service, the information will get relayed to them.

The other thing I see is that law enforcement actually comes to us quite often and they don't have the infrastructure or the capability to do historical Whois information, and unless it's able to be collected, they cannot go back in time and track down where the bad person started and where someone else that's caught up in the process may not have actually done anything.

Kieren McCarthy, journalist (written comment)

Are people not getting a little bit carried away when they talk about court orders for simple domain name ownership information? If it is that important to provide anonymity, people can follow the age-old system of starting a company and gaining anonymity and legal protection by providing those company's details in Whois. What exactly are the examples that we are so worried about where the police shouldn't have access to Whois?

Amadeu Abril i Abril

Two different set of questions. The first one is just a short question for Steve Metalitz, whether he has an educated guess about how much it would cost per domain, a system like the one he's proposing.

The second one is the trans-border issues. Doing that at an international level may be easier than doing that even at a regional level. As soon as you have some verifiers outside your country, or different languages, you have the language problem, but you also have a legal problem if you're exporting the data before taking the decision. So you are still stuck with the problems.

And, unfortunate as it might be, on one side, you have this. On the other side, you have data protection agencies in Europe that are quite radical in their view. They say that we don't need to provide the Whois. They say that IP address is a

personal data that shouldn't be published and things like that, which is just extreme on the other side.

Second is, I am not working for .cat anymore, but one of the remaining issues i still have to solve is the question of Whois for .cat. We need to do something to comply with the repeal law. We would love doing something that's coherent with what other TLDs do instead of creating more confusion. So we expect that the task force has a clear recommendation about the mechanism quite soon.

And regarding the interests of personal anonymity or that, all I know is .cat started, and nothing happened. The very day that open registration started, five minutes afterwards, the Whois was belly up because of the massive demands from all sorts of companies from all over the world. That's a very small, marginal TLD in the whole picture. So apparently some people that had no idea of what we were doing, they only know that a new Whois machine is there, go for it, and then we will decide what we will do with the data.

Steve Metalitz (in response)

No, I don't have a per-domain-name cost. Obviously, it depends on the volume of registrations or applications. We may learn and have some data from .nl that has been doing this for the last three years.

Second, I don't see that there is a problem of exporting the data if you are applying for special circumstances, because that would obviously be done with your explicit consent. It would be disclosed to you, for example, that a third-party vendor was located in Germany and you were a registrant in France - or the third-party vendor was located in Canada and you were a registrant in a European country. So I don't think there's really an export problem there.

I don't know why the .cat Whois went belly up. But I do know that for many of the smaller sponsored TLDs, there's not a lot of Whois traffic, certainly from the intellectual property world and from law enforcement. It depends on what people are doing in those domains.

But I think the statistics for .name - I haven't looked at .cat - show that there's a relatively low volume of Whois requests. I think most of this -- we have been focusing this on -- predominantly on the larger top-level domains, gTLDs. But, if there's a need for special treatment for some smaller ones, that --

Amadeu Abril i Abril (in response)

Let me provide the answer on that. The regular use is very low and the problems are nonexistent. On the first day, there were marketing companies that were going toward that data. We know those that addressed us the day to say 'oh, what happened, we cannot access anymore'. So we have restricted some IP addresses and we have restricted the number of queries you can do per minute to five per minute under port 43. And the ones addressing are marketing companies saying, "why are you restricting this?"

Steve Metalitz (in response)

Dot .nl does that, too, and we don't have a problem with that.

Wendy Seltzer, ALAC

Finally I have been able to participate in the work of this task force, although not as a voting member. What we're hearing in these two proposals doesn't represent the full range of privacy considerations that have been made. The other end point from "there shall be virtually no privacy" is "there should be very strong privacy options."

I have said many times as a personal and civil liberties viewpoint that there should be absolute anonymity possible in domain name registrations, that you shouldn't be required to register with physical identity in order to have access to this tool of speech. And so already the OPoC represents a compromise far from that, at least to give people privacy options.

And my recommendation that people be permitted to put domain names into suspension rather than revealing personal information was another attempt to give people alternatives that satisfy those who think domain names are going to be abused and those who think that their personal information is going to be abused if it's associated with a domain name.

So I want to encourage people to think that there are lots of different interests in not having your name and address and telephone number and e-mail address associated with the domain name, not all of them nefarious.

Margie Milam, MarkMonitor

We're a registrar and we're also a brand protection company. So we have a different perspective, because our clients are mostly corporations trying to protect their intellectual property. They also engage us in services to combat phishing. So some of the concerns that we have on these proposals is the perception that there's going to be less information available to fight situations such as cyber-squatting or phishing.

One of the concerns that we have with OPoC is the concern that when you lay OPoC with the proxy services, it'll be very difficult to get information to find out who's behind bad acts such as cyber-squatting or phishing.

One of the suggestions we have for the task force would be to set up standards. If you are going to adopt something like an OPoC, to say when information would have to be disclosed or provided to the registrant - some sort of clarification on what the responsibilities are if they are an agent for service of process for UDRP or something like that.

In looking at the two proposals, it looks to us that the special circumstances model is a little bit better from an IP perspective, because there's less change. Status quo's essentially the same, although there is a mechanism to address privacy concerns.

At least initially, from our perspective, the special circumstances model looks like it can accomplish both needs to address the privacy issue as well as being able to have information for law enforcement, for service providers like MarkMonitor or other companies to be able to provide the information to governments and to corporations that are concerned about protecting their rights.

Ross Rader (in response)

The suggestion that the task force would write some guidance as to how a registrant would react to various types of services is not a new suggestion. One of the things I've struggled with that is understanding exactly what that would mean. I shied away from supporting that because every time I hear that, it sounds like the suggestion is that we should give registrants legal advice. Certainly, when I get those types of notices myself, I take them to my lawyer. What form would that take to really satisfy the requirement you're describing?

Margie Milam (in response)

I'm sort of mixing up concepts here. With proxy services at the moment there are no real rules that apply to them. So if you're sending a cease and desist letter to a proxy service, you don't really know when it's going to go to the actual party behind the domain name. If it's a UDRP complaint, again, you've got the same issue.

The Whois information is also used for things like transfer requests. As registrars, we have to confirm that we have authority to transfer a name in or out. It slows the whole process of transfers and, you know, registrar business if you don't know that the information is actually going to the party that needs to respond.

So there needs to be a lot of thought on if proxy is going to exist with OPoC and special circumstances or some other model, that there needs to be some at least clear rules on the types of things that are typical with the domain name, UDRPs, a transfer request, your WDPRS, all of that, that needs to be thought through.

Ross Rader (in response)

So the complexity comes from the environment, then, is what you're describing. So it's an issue with proxy services more than it's an issue with the recommendations that we're putting forward. But with the marriage of those two, it's creating tertiary complexities that you're worried about.

Margie Milam (in response)

Right. I know you've walked through the three different types of contacts that exist now. That is useful from a protection standpoint, because we do a lot of correlation to find out who's actually behind a phishing attack or an infringement attack. And it is useful to find out whether someone is a bad actor versus just a normal registrant.

Marilyn Cade, GNSO Councillor, member of Whois Task Force, Business Constituency

I'm speaking as an individual stakeholder, but I want to note that I am a member of the task force. I'm not, however, directly speaking about the two products or the two approaches that the task force is addressing. Instead, i think it's important to remind all of us from whence we came.

I was the chair of the first task force that did an extensive study and then went on to make some recommendations related to Whois. Since we've all been working together, we have recently, in Luxembourg, then Vancouver and then in Marrakech, had the opportunity to sit in some workshops that have been very balanced and have brought forward the views of a number of different parties and interests to talk about in the issues related to changes and Whois.

One of the tensions I see for us is to keep in mind that balance must be achieved and that there are a number of interests. There are interests of law enforcement, of consumer protection authorities, of trademark authorities, of common, everyday users who use Whois to find out what web site their children are visiting. I spent a good deal of my life working in the area of protecting children and then helping to create groups that protect kids online and Whois is a basic tool used in those environments. The information has an important role to play.

I have heard over the time I have been working in this space concerns about data mining of e-mail addresses or telephone numbers. The Whois task force that I co-chaired proposed that we look at things like moving Whois access to a web-based access, moving to a white list approach to access to bulk access to data and to port 43. I think we ought to be looking hard at those kinds of steps and seeing what improvements they make. I do agree that when there is a legitimate need for privacy that there needs to be an approach. The special circumstances approach that Steve Metalitz has mentioned I think has merit and could be explored further.

But I note that that is a special circumstances environment. By moving to web-based Whois and using it to do a verification check, we can certainly begin to limit any misuse of the data for purpose of spam, et cetera.

I will say also about the issue of Whois data, I voluntarily register a domain name. I voluntarily hold myself out to communicate to the public via a web site. I think the public has a right to know who I am. I think that there are mechanisms for people who need anonymity to be able to use a web site or to find other mechanisms by which they can communicate in an anonymous manner. But I do believe that we need to maintain some balance.

If we don't have appropriate consent at this point, we certainly have notice from the registrars that we need to move to a stronger form of mandatory consent for registrants. That may be another step that we should take in order to make sure that the registrant is fully informed.

Bob Hutchinson (identified self later as with Dynamic Ventures)

I would like to relate an experience I had about the last meeting we had on Whois, which I tried to trace back a phishing attack which I got through e-mail, which was ‘come tell us about your Paypal, update your Paypal’. I walked that back through the registry and found that the entry was registered to an individual in London. And then I googled the name that was on the registry. There were articles about this person being a cyber criminal. There was no place to report this information or shut this web site down. So I would like you to address how that should be done for people on the internet. In other words the function of Whois is really there to protect the public and it's not doing the job. These kinds of attacks should be shut down in hours after they're on, not months or years.

Person unknown (in response)

ICANN is not a government. When criminal activity occurs, there's one and only one jurisdiction for the activity to be prosecuted.

Bob Hutchinson (in response)

But my point is that Whois perhaps should be connecting you to the proper legal authority for shutting down that web site, as opposed to giving me the information about who it is who registered that web site, 'cause I can't do anything about that.In other words, the system, the Whois system is broken. It's not the way you would set up law enforcement. For example, a crime occurs here. I don't have to have your name or whoever's the criminal. Don't have to have an identity of that person. All I have to do is report it to the proper authorities and say, "that's the person." I don't even know their name.

Ross Rader (in response)

The first thing that i would like to respond to is the notion that Whois can help you solve crimes. If you are aware of a crime, you should report the crime. Whois can help you get in touch with people that can provide you with more information about who may be associated with various resources, for instance, who may own a domain name or the people who are associated with the domain name. It can also tell you where those domain names are hosted. And in some cases, it will also tell you the identity of the company that's providing the hosting. There's a lot of information there. There's also different types of Whois. But I'm uncomfortable or unclear about whether- are you requesting that the Whois be reformed to become a better tool for law enforcement? Or that its current uses be made more usable?

Bob Hutchinson (in response)

I don't believe that the registrars should become the act of doing the enforcement. But they're the logical authority to provide the public that connection to what is the legal cybercrime-fighting unit for that domain name. And i don't think that's asking too much.

Ross Rader (in response)

So just as a note, that happens today. There's a very strong coordination between the registrar community, the service provider community, the legal community, i.e., law enforcement, and the network operator community. Issues are being dealt with on a very regular and concerted basis. The fact that this issue has dragged on within the ICANN community for now six or seven years does not mean that progress hasn't been made within the community. I would be certainly happy to share more details with anybody that was interested in finding out a little bit more about what the registration community is actually doing to make sure that they're part of the solution, not part of the problem.

Steve Metalitz (in response)

I would agree that ICANN is not the law enforcement agency and we can talk offline about where you (Bob Hutchinson) might take that information. But one thing you will find when you talk to law enforcement is that they rely on people like you, who do some of this spade work, to find out what you can about who is responsible for the attack. They depend on that, and phishing, in particular, the role of law enforcement is quite different that it may be in other crimes because of the necessity to respond very quickly. So i think the more information that is available through Whois and other sources, the more people like you will be able to help law enforcement in cracking down on this. I hear what Ross is saying that there are a lot of things being done. But the bottom line is as you've said it, I'm not sure the trend is in the right direction in terms of access to the information that's needed to try to keep the internet safe.

Jordyn Buchanan (in response)

There are situations in which actually having information from Whois doesn't actually help you solve your problem. It helps you get information. So it may be that there's further thinking that should be done on how do we coordinate responses to problems more effectively, especially when it's a problem that's threatening the security or the stability of the internet.

Mawaki Chango, GNSO Councillor, Non Commercial User Constituency:

One thing that slightly bothers me when we are discussing Whois and I hear about the law enforcement argument is that we seem to imply that in an ideal state of worlds, the government agencies act in the best interests of people. Unfortunately, that's not the case everywhere. Not all the countries are like Sweden or France or Germany or the US. So we need to balance the pros and the cons by advocating for a public display of that information. There are places where the simple display of the name is -- can be a source of threats for some people's life. There are places where people are still struggling for their rights to speech. So I understand those Wendy was referring to who advocate for strong privacy. But I also understand the need for compromising.

We shouldn't only be thinking of the possibility of law enforcement while ignoring the threats to people in some other places. And also, i would like to point out yahoo! currently offers to keep information private. It's like if a couple of other

registrars followed the same explicitly, we will have to make a policy to forbid registrars to offer that service. So I don't think that's really the way to go.

In fact, I would like to think that I'm supportive to law enforcement agencies. But when law enforcement agencies act, we recognize them specifically as acting to enforce law. So if for a law enforcement agency to be able to do their job we need to put the data up there for everyone to be able to access them, then there's no difference between the privilege, if I may say so, of a law enforcement agency and every other people, including the wrong-doers they are trying to protect us from.

Avri Doria, GNSO Councillor, member of the Whois Task Force

I'm only going to speak on two points, looking at security, and looking at the notion of legitimate, because those have come up several times.

In terms of security, we talk about constantly going back to ICANN's principles. When we look at security, many of the speakers, when they are talking about security of the Internet, they're talking about catching the bad guys, putting somebody in jail, stopping somebody from doing something. There's also the notion of security for the users of the Internet. That security demands that they be able to operate with privacy, that the security of the individual, the many individuals of the net, is, indeed, protected.

The OPoC proposal has gone too far in allowing too much information, specifically, the name and nation and state- the jurisdiction, in other words, how the law is going to get you. That was already put in as a compromise, and one needs to live with it as a compromise in terms of at least telling the law enforcement where they have to go.

We then talked about who is legitimate when we talked about a tiered notion. How do we determine who is legitimate to have this more information in the tiered process? Again, people up there have said, "ICANN is not a government." It's governments that decide what is legitimate, what is the law. So the only way we have of saying that someone has legitimate access to information is for them to come with an instrument from the law that says they have legitimate access, specifically, a warrant. That's what warrants are. They indicate that someone has legitimate access to data that is normally private.

So at first I was thinking ‘no’. I disapproved of the tiered notion. But I realize I do actually approve of some notion of tiered. All information is private. You get more information when you have a warrant saying you get it.

Kristina Rosette, GNSO Councillor, member of Intellectual Property Constituency

I am speaking as an individual but I an IPC representatives to the GNSO Council. I am trying to get a sense as to what realistically would be the eligible universe as of today of persons who would qualify under that proposal. I don't know if we have got any statistics or you can make an educated guess or we can extrapolate based on nl but i wanted to get a better idea are we talking 10,000 people, are we talking 25,000, is it 5?

Steve Metalitz (in response)

We have some statistics from nl. I don't know whether you can extrapolate. The issue here is what are the criteria. If the criteria are spelled out clearly that it only applies to individual registrants, that they have to show a concrete threat to their personal safety or security, and there's even some more detail in some of the documents that are referred to in the proposal. That gives you the picture of a category for which there would not be that many people eligible, and that makes it a manageable process. At the same time, it recognizes there are some people that qualify and need the special circumstances treatment. It also helps somewhat on the side of how to get access to that information, because if it's a relatively small universe, then perhaps there are ways that don't require so much of an apparatus to decide who has access to it.

Kristina Rosette, GNSO Councillor, member of Intellectual Property Constituency

With regard to OPoC, just a point of clarification. It did not seem to me that there was anything in the proposal itself that would delineate or categorize what categories of entities or who could be the OPoC. I wanted to confirm that that is the case, and if that's true, has there been any discussion about that? And if so, how has that come out so far?

Ross Rader (in response)

The short answer would be no, there isn't anything in there. Help me understand the question a little bit better. Why we should have that discussion?

Kristina Rosette (in response)

There are certain categories of persons that as counsel to IP owners, I would be less worried if most OPoC, for example, were the registrar, than I would be if, for example, most OPoC were the registrant's next-door neighbor. So i was trying to get a sense as to what extent there had been any discussion about should we delineate about who these people can or cannot be and how that process would work.

Ross Rader (in response)

That's the first time I have heard that question. Historically speaking, the administrative, technical and billing contacts, or the registrants, for that matter, have not been specific persons or entities. It could be your ISP, web-hosting company, telephone company, your next-door neighbor.

In terms of raising the bar as to who would qualify to be a contact on a domain registration, we could talk about it. I don't know how we could implement that without some sort of licensing mechanism, but it's an interesting perspective.

Jordyn Buchanan (in response)

Perhaps there is some notion of OPoC accreditation. We have discussed in the task force the notion that the registrant could be their own OPoC. So there is a notion that if it's an individual in particular, theoretically they could just continue to list themselves, as some people do, for administrative and technical contacts today.

Robin Gross, IP Justice, GNSO Councillor, member of the Non Commercial User

I wanted to pick up on this point about security, and the need for security with the Whois database. Avri talked about the security rights of Internet users, not just of the intellectual property holders but the users in the community. This year, the US Federal Trade Commission has announced that now in the US, online data mining is the number one crime. Privacy experts, in particular, EPIC, have testified that it is the Whois database that is one of the most significant contributors to this problem.

We need to pay some attention to the security interests of ordinary, everyday Internet users who register domain names, and not just the large intellectual property rights holders. They have legal mechanisms at their disposal if someone is violating their rights. It's called due process of law. I really haven't heard any explanation for why legal due process should be circumvented in this case.

We hear ‘gosh, it's a hassle to go into court and to convince a judge that we need someone's personal information’. But it's supposed to be a hassle. And it’s not that much of a hassle. You can get that information in a day. So this idea that we need instantaneous access to everyone's personal information that has ever registered a web site, it's just completely absurd.

When I look at this special circumstances proposal, I am quite frankly shocked by it. We're talking about some enormous barriers to privacy here. If you just look at the eligibility criteria, it's open only to individual registrants, for non-commercial purposes, and they have to demonstrate that they have a reasonable basis. These are all lawyer words meant to be stumbling blocks, by the way. That this access would jeopardize a concrete and real interest in their personal safety or security that cannot be protected other than by suppressing that public access.

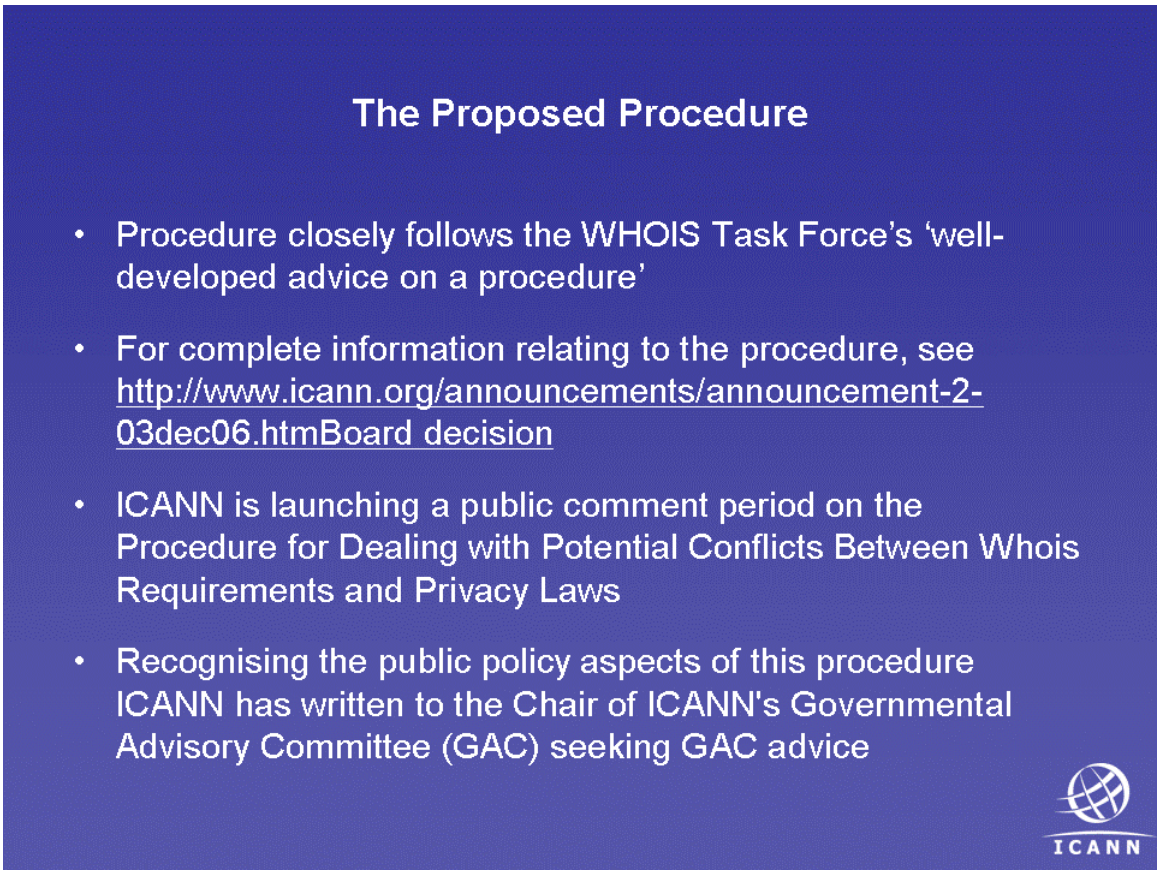
Wow! That is an enormous burden for individuals to have to prove before they can have access to their privacy rights. I don't think it's appropriate for ICANN to be trying to be building in barriers to an individual privacy like we see in this proposal.

We decided this issue already. We voted on this issue at the Wellington meeting. So the idea that those who lost that vote can now put forth another proposal and we get to re-open the debate, it's not acceptable. I'm sorry.

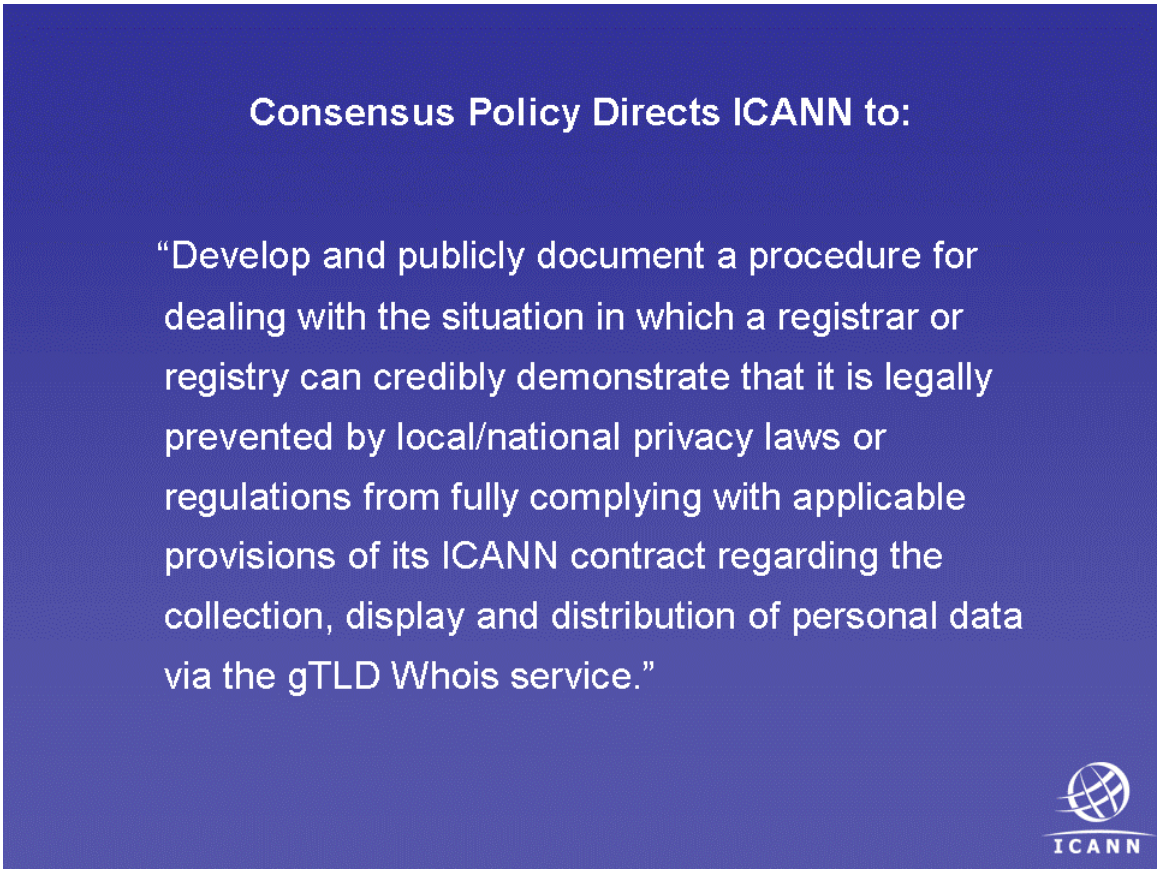
Section 2 – Draft procedure on potential conflicts of Whois requirements and privacy laws

Presentation by Kurt Pritz, ICANN

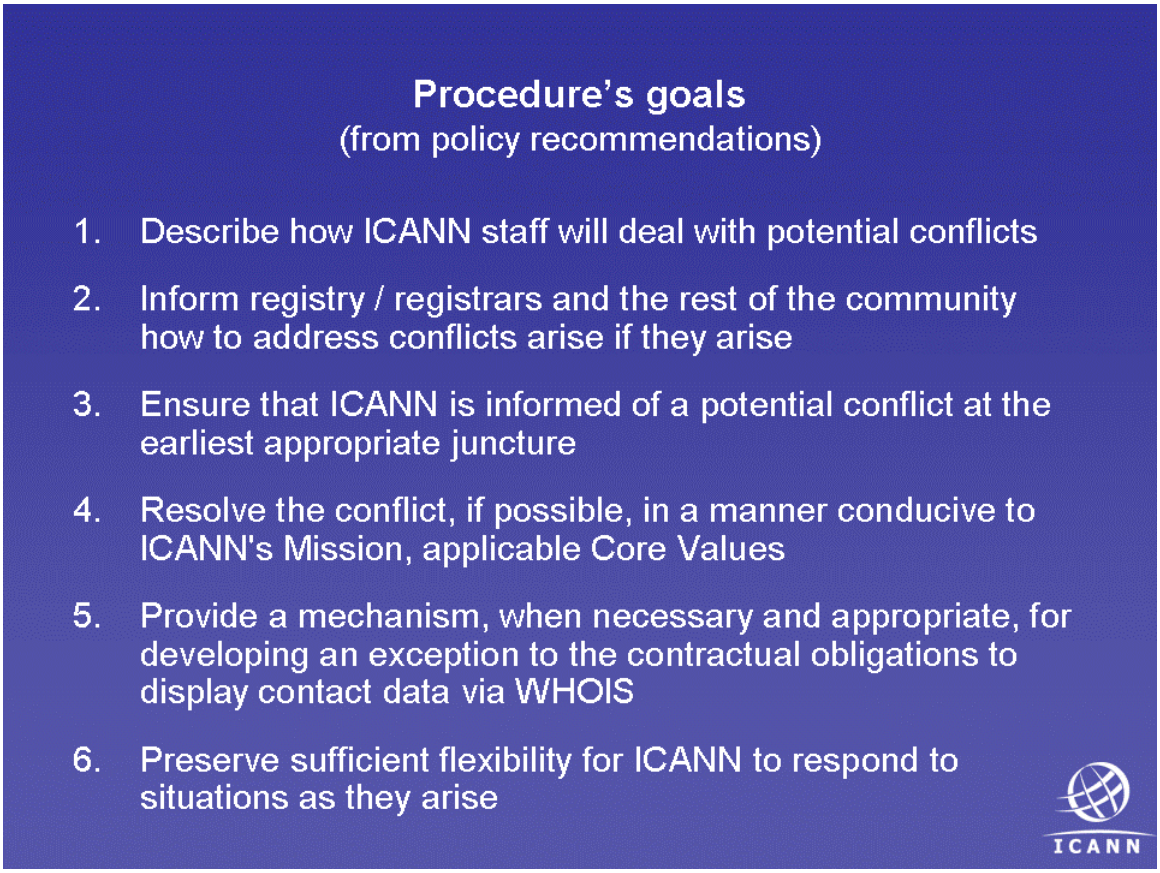
This procedure, which requires some interpretation, is available for public comment until January 15th, 2007. We have also specifically written to Mohamed Sharil Tarmizi, Chairman of the Governmental Advisory Committee and asked him to work with the gac in order to provide advice on the policy.



This is the direct advice we received from the GNSO that was in the final report. We followed it to develop the procedure:



The procedure has several goals. The first two are from staff, and then the last four are actually in the policy recommendations:



There are six phases of the policy:

Phase I: Notification of Whois Proceeding

Registry/Registrar receives notification of a Whois proceeding and provides ICANN staff with essential information

Phase II: Consultation

If appropriate, ICANN staff will contact the national agency

If proposed changes result in non-compliance with contractual Whois requirements, ICANN staff will refer to the Board

Phase III: Referral To Board

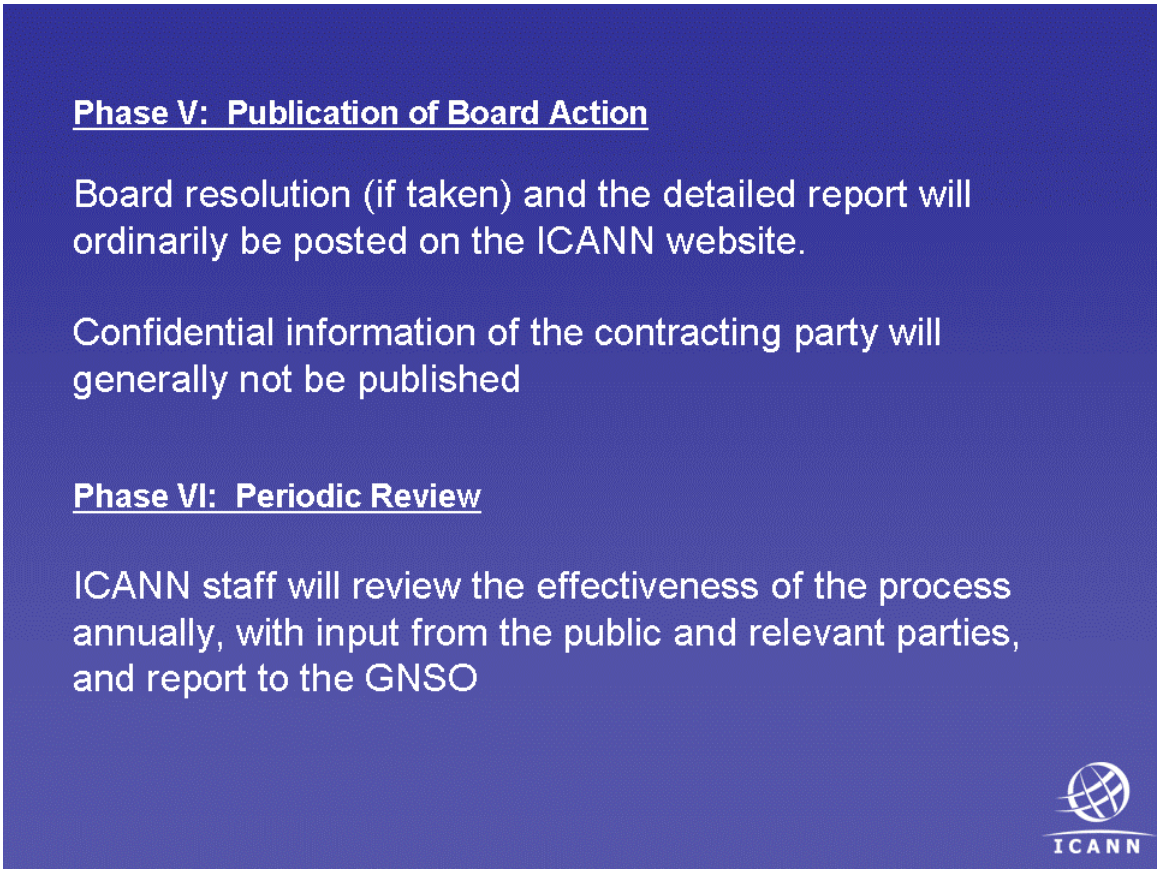
Staff may refrain from taking enforcement action against the registrar/registry for non-compliance.

Staff may prepare a public detailed report and recom-mendation and submit it to the ICANN Board for a decision.

Phase IV: Resolution By Board

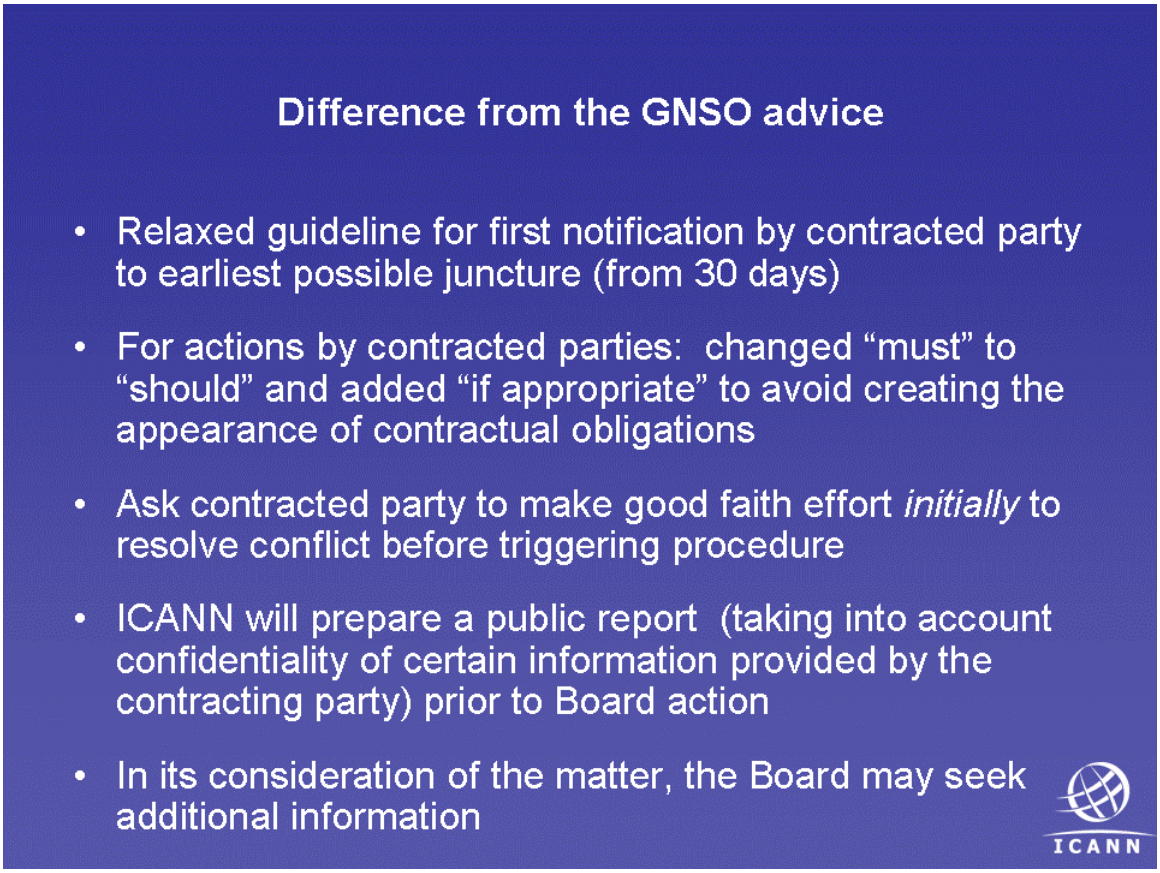
The Board may consider and take appropriate action as soon as possible:

1) Approve/reject/modify report recommendations
2) Seek additional information
3) Schedule a public comment period
4) Refer to the GNSO for review and comment



The final step in this procedure is that ICANN will regularly review the effectiveness of this process. There are a lot of uncertainties going into this process. Will there be one request? Will there be a hundred? What are the sorts of requests? What will the threshold of requests be? So we take this advice from the Council, but there would have to be regular and, I think, rapid reviews and recommendations to the council for potential adjustments.

When the consensus policy was read and the accompanying advice, there were some clarifications made to the procedure in order to facilitate the management of it:



In the consensus policy it is called out that ICANN will make a report to the Board and publish it to the contracting party. We think in the interest of transparency that the reporting should be public, taking into account the need for confidentiality for certain considerations. And in the actions the board can take, we have added the board can temporize.

Marilyn Cade

I have two questions. One is, to date, what number of complaints and contacts does ICANN receive from governments about exceptions of this nature?

Kurt Pritz (in response)

I don't know. I'm not aware of them. I'll find out.

Marilyn Cade

If you are not receiving complaints and contacts, and I would assume you are not because they are not receiving much publicity, either, you are going to go

through a public comment process. The GAC will have time to comment on this. We are thinking this will be formal and launched in the March time frame?

Kurt Pritz (in response)

I think that GAC advice might come in Lisbon if it doesn't come here.

Marilyn Cade

So the good news is that because you are announcing it, it will raise this to the awareness of governments. Did I understand that (reports will be made) on a regular basis on how many complaints that you are getting and what the general nature of the concerns are that have been raised.

Kurt Pritz (in response)

Yes, that's correct. We think that's important because of the great deal of uncertainty going into it.

Marilyn Cade

My comment, then, would be based on the fact that ICANN has not received a great number of complaints up to now and that we just put a consensus policy in place, we need to allow sufficient time to test and see how many complaints we get and what kind of problems that we encounter before we start making a lot of changes in Whois policy.

Sharil Tarmizi, Government of Malaysia, Chair of the Governmental Advisory Committee

Just to manage some expectations, I would like to thank you for the letter which we just got today. Thank you for the formal notification. It presents a lot of

complex issues for considerations for the government. So we will endeavors to see what we can do in this limited time. But I can certainly promise you, Kurt, you are not going to have one at this meeting. Lisbon, maybe. But we'll see.

Jordyn Buchanan

It's still 6:59, and i declare this meeting closed. Thank you, everyone.

[applause]