PART II: Methodology and Outreach

Appendix B:

Methodology: How the WHOIS Review Team Conducted its Work

Appointed in September 2010, the WHOIS Review Team engaged in a year's effort to conduct its review. The Review Team divided its work into four broad review and evaluation steps:

1. To Assess ICANN's WHOIS Policy requirements as set out in the Affirmation;
2. To Determine ICANN's current WHOIS Policy as published and implemented;
3. To Evaluate the effectiveness of ICANN's WHOIS Policy by methods including a compliance review; and
4. To Measure ICANN's WHOIS Policy relative to the specific goals established by the Affirmation in 2009, via a gap analysis.

Each step involved Review Team research, consultation, data collection, public comment, review of responses and incorporation of appropriate changes.

1. *To assess ICANN's WHOIS Policy requirements as set out in the Affirmation,* the Review Team worked through the wording of the Affirmation of Commitments signed by ICANN and the US Department of Commerce, and the goals and standards that it sets. Specifically, Affirmation section 9.3.1, states enforcement of WHOIS policy is “subject to applicable law,” and implementation of the WHOIS policy must meet “legitimate needs of law enforcement and promotes consumer trust.”

Key terms within this section, the Review Team determined, are broad and subject to multiple interpretations, including: applicable law, law enforcement and consumer trust. To clearly define these terms, the Review Team members conducted research, consulted with experts and questioned Affirmation drafters and signatories.

The Review Team set out its working definitions of “applicable law,” “law enforcement' and “consumer” for public comment on March 4, 2011 http://www.icann.org/en/announcements/announcement-04mar11-en.htm. It held public sessions in San Francisco with Advisory Committees and Supporting Organizations to discuss these definitions, and the groups they represent. The result of this investigation, and the definitions adopted by the Review Team for purposes of its work, are found in *Chapter 2: The WHOIS Review Team, Scope of Work & Key Definitions*.

2. *To determine ICANN's current WHOIS Policy as published and implemented*, the Review Team researched and pieced together ICANN's WHOIS policy from publicly-available documents, including the contracts of Registries and Registrars posted on the ICANN website and the GNSO consensus policies and procedures, as adopted by the GNSO and ICANN Board, and posted on the ICANN website. ICANN Policy staff assisted in this process, as did members of the ICANN Community.

The Review Team published key questions regarding WHOIS policy in its public comment of June 9, 2011, http://www.icann.org/en/public-comment/whoisrt-discussion-paper-09jun11-en.htm. Extensive discussion took place at the ICANN meeting in Singapore with Supporting Organizations and Advisory Committees, including at the Public Forum on June 22, 2011, and also at a special meeting with representatives of the Registries and Registrars, the two parties specifically bound under ICANN contracts to collect, maintain and provide WHOIS data.

Full discussion of this issue is set out in *Chapter 3: The Complex History of WHOIS Policy.*

3. *To Evaluate the effectiveness of ICANN's WHOIS Policy by methods including a compliance review,* the Review Team reviewed ICANN WHOIS Policy compliance efforts closely. The Review Team met in lengthy meetings with ICANN Compliance staff to fully understand ICANN compliance activities, time-frames, reporting and results.

In its June 2011 Discussion Paper, the Review Team requested public comment on the expectations of stakeholders regarding compliance, the effectiveness of ICANN compliance efforts, and whether parties subject to the compliance efforts feel the work is being carried out in a fair and balanced manner.

These questions led to robust discussions with numerous parties in at ICANN meeting in Singapore, including:

- Public Forum, 6/22/2011
- Intellectual Property Constituency (GNSO), by teleconference, at its request, prior to the Singapore meeting,
- Security & Stability Advisory Committee (SSAC), 6/21/2011

- Noncommercial Users Constituency (GNSO), 6/21/2011
- Commercial Stakeholder Group (GNSO), 6/21/2011
- Registries Stakeholder Group (GNSO), 6/21/2011
- At-Large Advisory Committee (ALAC), 6/21/2011
- Joint meeting with Registrar and Registry representatives (GNSO), 6/22/2011
- Government Advisory Committee (GAC), 6/22/2011

Based on this research, and public comments, Review Team members wrote additional questions for ICANN's Compliance team, and followed-up with a detailed compliance review assessment at the Marina del Rey offices.

Full discussion of this Compliance Review is set out in *Chapter 4: Implementation of WHOIS policy – ICANN's Compliance Efforts.*

4. The fourth task was *To Measure ICANN's WHOIS Policy relative to the specific goals established by the Affirmation in 2009, via a gap analysis.* This step required incorporating sections of all prior Review Team work, including its research of ICANN Policy, review of ICANN Compliance, and assessment of the definitions of key terms in the Affirmation to review whether "subject to applicable laws," ICANN is implementing its WHOIS policy in a manner that protects the "legitimate needs of law enforcement and promotes consumer trust."

This Review Team evaluation included additional methods of outreach:

- A Review Team questionnaire for Law Enforcement circulated by Sharon Lemon, Law Enforcement Representative, and Peter Nettlefold, Designated Nominee of Heather Dryden - Chair of the GAC, to law enforcement and government agencies, and
- A Review Team-commissioned survey of Internet users and domain name registrants (consumers) on their expectations regarding WHOIS data and its access conducted by a professional survey organization.

In addition, the Review Team raised with the community a number of sensitive issues regarding the tension between two values within the Affirmation of Commitments: privacy of registrant data and public access to it. The Discussion Paper requested country code TLDs (ccTLDs) to share information regarding if they have responded to domestic laws and whether they have modified their ccTLD WHOIS policies.

It also requested input on the use of privacy/proxy services and “their impact on the accuracy and availability” of WHOIS data. http://www.icann.org/en/announcements/announcement-09jun11-en.htm (translations available).

This important research, assessment and analysis work is found in two chapters with the Report: *Chapter 6: Understanding the Needs of Stakeholders* and *Chapter 7: Gap Analysis* as well as numerous recommendations and appendices.

Finally, in its *Chapter 8: Recommendations,* the Review Team sets out the result of its extensive evaluation and presents its conclusions. These Recommendations are designed to guide future work within ICANN, and the ICANN Board is required to take action on them.

Summary of Review Team Outreach and Committee Work

The Review Team devoted thousands of hours to its work. It met widely with members of the ICANN Community and those in government and law enforcement bodies outside of ICANN. The Team met bi-weekly by phone, conducted extensive two-day planning meetings in January and September 2011 and held full day team meetings at each ICANN meetings in San Francisco, Singapore and Dakar.

In response to requests for public comment, the Review Team received dozens of written comments and hundreds of oral comments at its Public Forums and meetings with advisory committees and supporting organizations. The Review Team appreciates these valuable and thoughtful contributions, and offers its deep appreciation to everyone who participated in its processes.

Appendix C:

The WHOIS Review Team's Law Enforcement Survey

This Review Team questionnaire for Law Enforcement was circulated by WHOIS Review Team members Sharon Lemon, Review Team Law Enforcement Representative, and Peter Nettlefold, Designated Nominee of Heather Dryden - Chair of the GAC, to international law enforcement and government agencies. By prior agreement with the respondents, the results of the survey will be published in full but without the names of the responding individuals and organizations.

1. Do you feel this definition is suitable in the context of this Review?
Yes, but...
Yes this definition is suitable.
Yes
YES
No
No
Yes
YES

2. If not, do you have any suggestions/changes or additions?
...keep in mind that there are many private initiatives by private entities that are doing a lot of great work in countering abusive behaviour on the internet. These organisations also make use of public WHOIS data.
It should include references to the competence in criminal investigation activities, otherwise even CERT´s could be considered as LEA, and I don´t think ICANN will agree.
If anything I thing this is overwide and would cover just about everyone involved with Government or working in the public sector. I think this could be restricted to those bodies with Law Enforcement powers or regulatory functions. If it is as wide as this how will ICANN possibly be able to check the credentials of all government bodies.

3. Does WHOIS policy and its implementation meet your needs? **a. If so, are any aspects of the WHOIS service more important than others?**
The registration date in the domain WHOIS is a very useful information: "Fresh" domains are more suspicious than long established ones. Network WHOIS provides leads to physical infrastructure and is therefore, from a technical point of view, more important than domain-WHOIS.
In some parts yes. Serbian MoI and We think MoIs in many countries around the world have a problem with accuracy of data, some of register data are incomplete, many of them give an opportunity for anonymous registrations, some of them are not updated/data are old as example if some service is sold to other person etc.

Yes it does, email accounts and registrar details are quite useful because they lead to payment details and connection logs.
b. If not, what issues or problems have you encountered with WHOIS?
Criminals use fake-WHOIS or proxy/privacy-registration (with STILL fake data behind) which makes determination of the competent jurisdiction difficult.
Whois does not provide the exact physical location of a computer nor does it guarantee that the information provided on entities/persons is correct.
It doesn’t fully meet our needs. The main problems are whois privacy (when there are no results in whois) and fake data (when details of the owner of resourse/IP range/AS appear to be fake).
Some remarks: sometimes there is an information in registering data not about an end user but about a company by means of which the domain name was registered; and publication of fictitious data.
Lower level & free domain name and website access creates the opportunity for anonymous creation of websites with fictitious email and address details. Advertising revenue has created a situation where anyone can host anything for a given amount of time before checks are made and very often no checks are done until LEA intervention.
4. How important is WHOIS for law enforcement activities? Are there alternative data sources that you could use?
WHOIS is very important. It provides first leads. If accurate, jurisdiction can be determined and criminals may be found – if inaccurate, Domain can be revoked (violation of T&C).
WHOIS is very important because We think that the most valuable information’s could be found there. Alternative data sources could be forums and other services that have some kind of registers like national services etc.
Important for finding location of devices, identifying subjects. Others sources can be used, but the don’t fully offer the same results if we had a proper functioning WHOIS
Whois is, of course, of a great importance. Sometimes we can use additional sources but also based on whois info.
It is considered vital in cybercrime investigation due to the fact that there is no other way to obtain data about the legitimate owner of a domain or IP range.
WHOIS is very often used in our work. There is an alternative data source – www.centralops.net
"WHOIS" is an important first step in the enquiry chain but cannot be relied on, often the contact details are dated and non-responsive on a 24/7 basis.
5. What changes to WHOIS would you recommend to better meet the needs of law enforcement? Please provide reasons.
Verification of registrant or at least “plausibility-check” of entered WHOIS-data can lead to better quality of data and might prevent fraudulent domain registrations.

We think that accuracy of data is important, some of register data are incomplete, many of them give an opportunity for anonymous registrations, some of them are not updated/data are old as example if some service is sold to other person etc. We need exact data of registrants, more information about administrative contact witch are updated and correct (as example checking of those contacts to see are they real or fictive). The real reason is that We losing a lot of time to establish who is behind some services on the Internet. That would help to prevent anonimity of cyber criminals etc.

Guarantee that a full ID or company (Chamber of Commerce) check had taken place before WHOIS info is entered into database. That the above information will be checked on accuracy regularly. That the exact physical location of server(s) (IP-based, AS-number) is stored in the relevant WHOIS (or RIPE/ARIN…etc.) database, possibly including GPS-coordinates. That if incorrect information is provided, that IP/Domain/AS will be revoked. This only to enforce the entry of correct data.

The main change it should be introduced is an effective check policy, in order to guaranty that the information provided is real and updated. If not user can still use any data to fill in the registration forms.

a) By legislation down level responsibility. b) by-monthly record updates from it and administrators. c) Immediate upward facing suspension for creating or permitting anonymous or false information for site ownership and responsibility.

6. In your view, how well is ICANN performing against these requirements? Please provide reasons.

ICANN just recently started to “de-accredit” registrars for non-compliance (before, there have only been cases of de-accreditation for non-payment of charges).

I am not very familiar with this topic

They appear not to be aware of LEA’s (and thus legitimate internet users) needs.

7. Do you have specific examples of effective ICANN policies or implementation activities, or suggestions of how ICANN could improve its performance?

ICANN should be able and willing to enforce its policies. WHOIS policy seemed long to be just a recommendation whose non-compliance didn’t have consequences for registrars.

If it is possible, it should be a good idea to start digital certificates as a requirement when someone tries to register a domain or IP range.

8. How can ICANN balance privacy concerns with its commitment to having accurate and complete WHOIS data publicly accessible without restriction?

Forbid private-registrations for commercial websites (commercial by content or by TLD – “.com” should be commercial by definition?!) or just allow private registration for private homepages. Define policy about usage of privacy/proxy-services – where it should be allowed (eg freedom of speech) and where not (commercial use). If someone wants/needs to remain anonymous, does he/she really need to register internet-resources or can they also publish content in other ways?

Some data could be given in a form that is available to wider public but it must have solution that involve some kind of protected database available only to restricted number of people who are authorised to have more details that are not available to regular users (data could be given as some protected link witch could be seen able only to people with authorization and maybe they could establish database with protected access with user name and passwords). Access should be given upon requests. It is important for the users to be aware of the scams that could be committed when clone Internet sites appears on the Internet as example in cases of phishing etc. If they are aware of this differences between real sites they use and falsh once they could give that information to police.
Publicly accessible could data could show less info as LEA accessible data. This would help to keep up with local privacy issues. The problem will pop-up that foreign LEA's won't be able to see all data without permission of the "hosting" LEA.
Being stricter when somebody tries to register a domain or an IP Range. They should check that the data provided is real and corresponds to the legitimate user. Developing an effective inspection system. Obviously these inspection mechanisms should be accompanied by penalties, fines, or punishments in order to be effective. In Spain the Ministry of Industry has developed a very strict regulation about this aspects and it is working very good with .es domains.
I think this is difficult if not impossible to achieve, especially in relation to the EU and the EU privacy regulations and laws. We need to draw a distinction between privacy and anonymity which is why LE are not against proxy registration per se but that the accurate details of registrants needs to be obtainable by Law Enforcement swiftly and globally without the need to return to the International letter of Request route which is too cumbersome and slow to be effective. ICANN needs to implement a policy which, while respecting individuals rights to privacy allows authorised Law Enforcement (as per definition above) access to the data for the investigation and prevention of crime. Special attention needs to be paid to the "accurate and complete" part of the statement ensuring registrants details are correct. This relies upon ICANN and the TLDs (both cc and gtlds) to implement know your customer policies. A swift removal of infrastructure from any shown to have not supplied correct data is crucial to the effectiveness of the system. If there are no consequences to registering with false data, people will continue to do so.
We think that it is really important to keep in mind the right of the Internet users to receive reliable data about the owners and registrants of the domain names providing services for them. Privacy protection should not infringe upon the right to receive accurate and complete WHOIS data.
a) Information given to all registrants that administration information must be available to the public when a site is for unrestricted public access. b) Third party registered data controllers could be used for private or vulnerable sites (i.e. Schools, Financial Institutions etc.) c) Set levels of information similar to Companies House so that more detailed information requires at least a reason and some level of identification, email, incoming IP etc.

9. Are you aware of any efforts by country code Top Level Domain operators within your jurisdiction to find a balance with regards to WHOIS between potentially conflicting legal requirements for data protection, privacy and data disclosure?

In our jurisdiction, all data that has to be published needs to be defined by laws/bylaws. Email-addresses have been removed from the public WHOIS to counter spamming.
No, I am not.
NL WHOIS is mainly closed for public now, only LEA is allowed access to full data. Works, but with the concern mentioned under 8.
.ES domains from Spain have an excellent system that has been approved by the Data Protection Agency. The information provided includes Name, address, and 4 different ways to contact the owner. It is regularly checked by the Ministry and if data is not updated a fine is issued.
Not within the UK to my knowledge.
NO
10. What is the importance of WHOIS data being publicly available without restriction?
Providing contact address for issues with the relevant internet-resource. Indicating possible jurisdiction. “Know your businesspartner”: Possibility to check on registrant of domainname.
ICANN should rise awareness of governments in countries that are main sources of proxy services. Round checking should be one of solutions as well.
Legitimate companies could use this data to improved their services to the public.
It is the single database in the world that can provide information about IP&domains owners. Those details are very useful because lead you to corporation that is in possession of the information that is relevant to the different cases. If WHOIS data was not public, it would be impossible to identify these corporations, so the investigation could not be carried out.
It’s in direct proportion to the importance of Internet in modern world.
To the general public, knowledge that it is available is sufficient but knowing that LEAs can access detailed accurate information readily and immediately is more important.
11. How should ICANN address concerns about the use of privacy/proxy services and their impact on the accuracy of the WHOIS data?
Provide accreditation for privacy/proxy-services similar to registrar accreditation.
We think that this is a great problem because it could conceal traces and give an opportunity for anonymity and abuse of this services by criminals
See 5.
They should developed a strict regulation about the privacy services these companies can provide with, and when they are forced to disclosure that information
If a person goes onto the street wearing a face mask that person is likely to be detained for some purpose. Access to some buildings will be restricted for example banks. Then equally restrictions on access to and distributing information for or pertaining to the public or individuals are justified to protect the public interest.
12. What is your view on the use of privacy and proxy services by registrants?
It’s a tool to remain anonymous which may be useful and justified in certain limited cases. Nowadays it’s mostly used by people who run illicit or “immoral” business and

fear repression by law enforcement or private “cruisaders”.
No
See 3.
It turns the LEA job extremely difficult because most of these privacy companies are based in foreign countries, so it becomes quite hard to gather information about the real owners of the domains. Even somebody manages to contact them they rarely provide details about their customers. So, in fact, is like deleting the WHOIS databases
See previous.
From the point of view of LEA the use of proxy services embarrasses the investigation.
a) Generally suspicious however they can serve to protect from some intrusive protocols. b) Reasons for use of proxy servers should be recorded when registering and later use without updating the Whois profile should result in punative reaction.
13. Are there any other relevant issues that the review team should be aware of? Please provide details.
This cannot be just more rhetoric and another talking shop but demands some action from the Internet community to protect their own space. Law Enforcement have been lobbying for change to the governance procedures for several years now and to my view absolutely nothing has so far changed. ISPs, Registrars appear to take the short term, fiscally rewarding routes at all times whilst ignoring the long term threat to the stability and international nature of the Internet posed by growing criminality affecting economies and business. Even small changes and steps towards a more transparent and creditable WHOIS system would be welcome. I welcome ICANN’s dialogue with Law Enforcement but t really does need to lead to something tangible, and soon.
Not relevant to this questionnaire.

Appendix D:
Consumer Study (User Insight)

A subcommittee was formed to address the questions enumerated in chapter 6. The initiative, led by Lynn Goodendorf, engaged a third party service provider tasked with obtaining information sufficient to provide the answers.

UserInsight, the third party selected by our subcommittee and retained by ICANN, conducted a study performed in two phases; a qualitative phase was conducted to help formulate and construct questions for a second quantitative phase.

Phase One: Qualitative Phase

The primary purpose of the qualitative phase was to inform the creation of a quantitative survey. An additional goal of this phase was to determine similarities across countries as well as distinct differences resulting from unique cultures and perspectives.

User Insight selected 20 individuals now living in the U.S. whose home countries represented 8 of the 10 countries targeted for the follow on quantitative surveys:

- Argentina,
- Australia
- Brazil,
- China,
- France,
- South Africa,
- Spain and
- United States

This small focus group of 20 users included:

- 8 Males and 12 Females
- A balanced representation of ages that ranged from age 18 to 56.
- All were Internet users and expressed confidence in making purchases online
- 9 of the 20 owned a domain name
- 12 of the 20 had concerns about websites they have visited in the past

After completing a 15-item questionnaire the participants were paired based on levels of Internet use experience. Each team contained a participant with a low level of Internet experience and the second with a higher level of experience. Each pair were interviewed and filmed while they answered questions and performed tasks on an Internet connected computer.

These tasks included:

- Review and feedback regarding a known fraudulent website that appeared credible;
- Observations of the individuals attempting to locate domain name registrant information and feedback for that exercise;
- 11 of the 20 individuals owned a domain name and were asked to look up their own information and provide their feedback.

Although the initial phase of the study was not intended to provide statistical data, qualitative feedback from the participants may indicate that "consumer trust" is a multi-layered concept. Visual aesthetics of a website and ease of navigation to find information was a key influence on perceived credibility. Specific observations included:

- Older "style" websites were seen as less trustworthy; possibly not maintained.
- Legitimate WHOIS result pages by various registries and registrars were misinterpreted as not valid because the format, font and presentation looked like computer script.
- Legitimate WHOIS result pages often had prominent and conspicuous advertisements that distracted from the actual WHOIS results.

Phase Two: Quantitative Phase

The global online study, the second phase of UserInsight's work, involved the administration of a 17 item multiple choice format survey questionnaire to Internet users in diverse geographic regions. The online survey involved 1,217 respondents from 10 countries distributed as follows:

- Australia, China and India from the Asia Pacific region;
- France, Germany, Spain and South Africa from Europe and Africa;
- Argentina, Brazil and the U.S. from the Americas region.

The surveys began September 30th and concluded October 14th, 2011. 553 males and 664 females from 18 to over 60 years of age were included in this study.

277, or approximately 23% of those surveyed, owned domain names. Most of the domain names owned by those surveyed were for personal use, with the remaining, approximately 40%, for commercial use. A significant percentage of those owning domain names claimed to collect personal information, or facilitate financial transactions, through their website.

The survey focused on the two key areas: website trust and awareness of WHOIS. Towards the end of the survey, the user was asked to locate "the website owner of www.thecocacolacompany.com".

Thick WHOIS information for www.thecocacolacompany.com is available from the registrar CSC Corporate Domains, Inc. Other WHOIS services, as for example Internic's WHOIS, will only return thin WHOIS data. Consequently, the name and address of the owner of the domain name in question would be available from a WHOIS service only to those who managed to locate the CSC Corporate Domains, Inc. WHOIS webpage. And, the address published on the website for general contact purposes is different from the address of the Domain Name Administrator listed in the WHOIS registrant information, permitting a way to distinguish if a participant actually found the WHOIS registrant data or not.

The results of the survey revealed that most located the correct name and address of the owner of the www.thecocacolacompany.com domain name but they were not aware of WHOIS and they used other methods such as search engines and user forums to locate the contact information for the website the WHOIS data. Interestingly, similar themes emerged from this phase of the study, summarized in chapter 6.

UserInsight provided some comments and recommendations at the conclusion of the study. Items of particular note were:

- Consider the overall strategy of having domain providers (registries and registrars) maintaining and promoting WHOIS look-up service

- Consider conducting future research to better understand:
  - Why some users do not trust the information found;
  - The impact of incomplete records on consumer trust;
  - The impact of single vs. double byte characters for some International users.

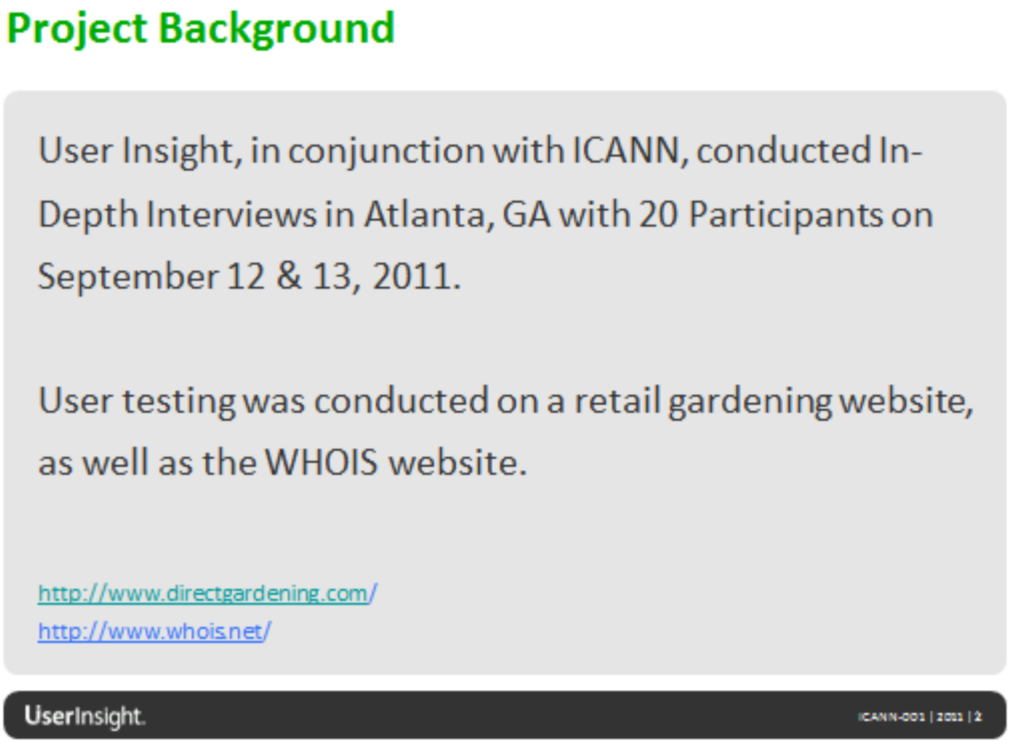
Qualitative Results

UserInsight.

ICANN

WHOIS Consumer Trust Research

In-Depth Interviews - September 12 & 13, 2011



Project Background

User Insight, in conjunction with ICANN, conducted In-Depth Interviews in Atlanta, GA with 20 Participants on September 12 & 13, 2011.

User testing was conducted on a retail gardening website, as well as the WHOIS website.

http://www.directgardening.com/
http://www.whois.net/

UserInsight. ICANN-001 | 2011 | 2

Project Goals

- Utilize in-depth interviews to understand consumers’ perceptions, concerns, and overall trust for websites
- Determine awareness and understanding of WHOIS
- Evaluate the effectiveness of WHOIS policy and its implementation as it relates to promoting consumer trust
- Determine similarities across countries as well as distinct differences as result of unique cultures and perspectives
- Gather feedback on Users’ experience of finding WHOIS, their understanding of the content provided, and how they utilize the information
- Utilize feedback to inform the creation of a quantitative survey

User Profiles

20 Total Users

8 Males

12 Females

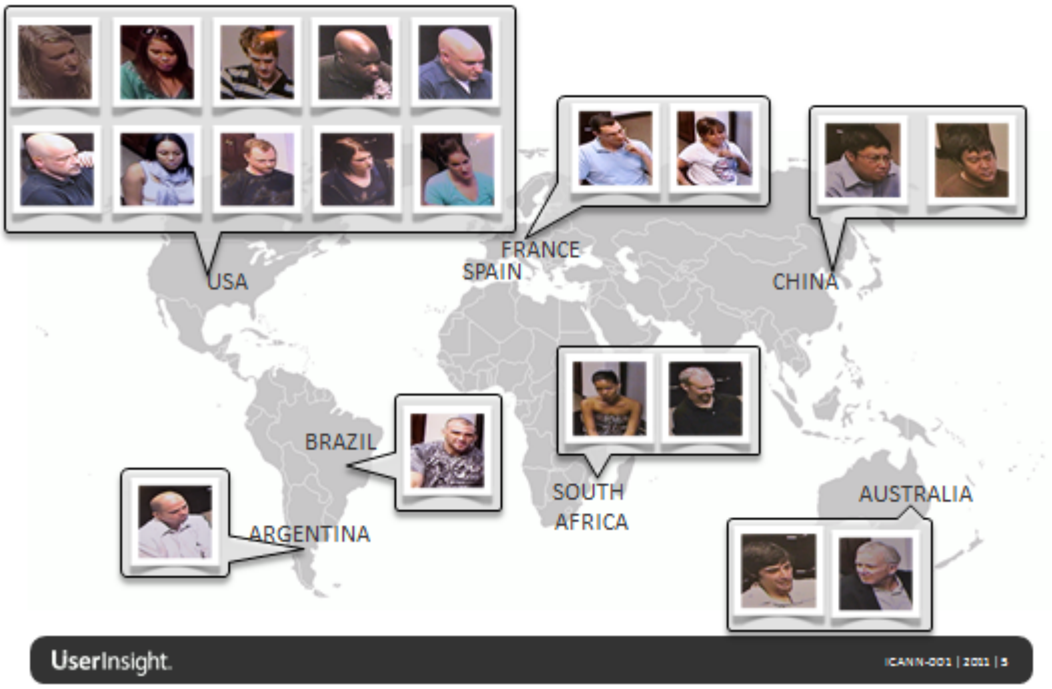
3 Users 18-24 years	2 Users 35-39 years
4 Users 25-29 years	7 Users 40-49 years
2 Users 30-34 years	2 User 50-56 years

11 out of 20 do not own a website domain

All use the Internet and are comfortable making purchases online

12 out of 20 have concerns about websites they have visited in the past

Countries Represented



Discussion Guide

Part 1: Background & Context

□Create a conducive environment where respondents willingly cooperate on a task and share their thoughts, insights, and impressions with one another and the moderator.

Part 2: Internet Security and Sharing Personal Information

- □ Respondents complete an individual questionnaire covering the following topics:
  - Internet security
  - Sharing specific personal information
  - Knowledge of resources, including national and international organizations that help make the Internet safer
  - Participation in social media
  - Website domain ownership.
- □ Respondents discuss answers in dyad to help set the stage for a series of tasks over the next 60 minutes.

Part 3: Attempt to Resolve Unfulfilled Order

- □ Respondents work to resolve an unfulfilled Internet order for nursery plants.

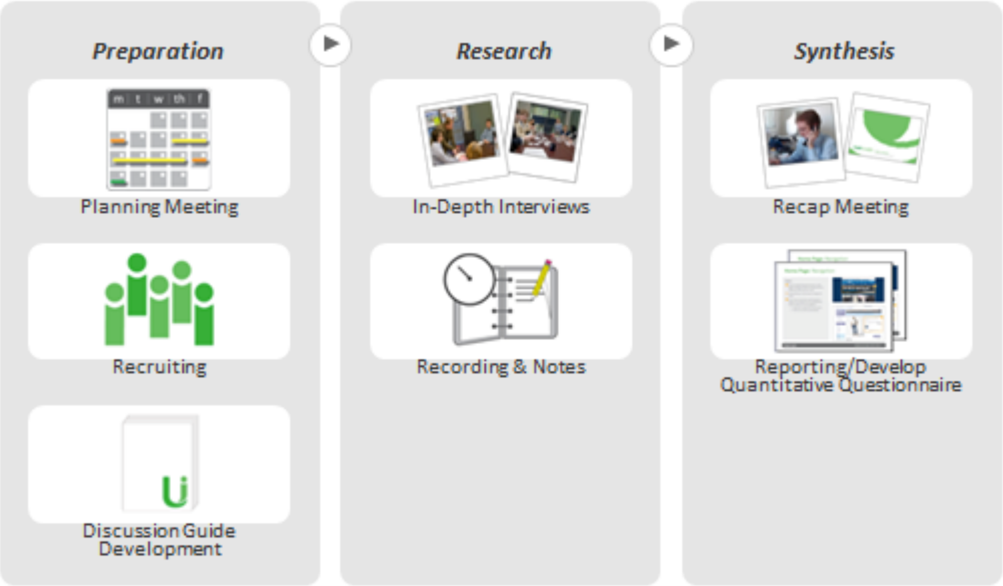
Part 4: Uncover Owner of Website

- □ Respondents work together to find as much information about the owner of the Internet site and who registered this particular business domain.

Part 5: Respondents use WHOIS to Find the Owner of Website

- □ Respondents work together to find the WHOIS website and use the website as a resource to find the owner of the website.

Project Lifecycle



Preparation

Planning Meeting

Recruiting

Discussion Guide Development

Research

In-Depth Interviews

Recording & Notes

Synthesis

Recap Meeting

Reporting/Develop Quantitative Questionnaire

Major Findings: Website Trust

- Users' trust in a website is enhanced when they find familiar logos and signage when visiting e-commerce sites (i.e., VeriSign, BBB, etc.)
- Websites that exhibit user-centered design encourage trust, particularly simple navigation, easy to find information, contact details, and overall aesthetics
- Users prefer website addresses ending in .com, believing they are more trustworthy
  - When asked about .net, Users assume the registrant was not able to get the .com address and expect the site to be inferior
- Users do not think that country code top-level domains are more trustworthy than .com

Major Findings: WHOIS Awareness

- Overall, awareness of WHOIS is low. When asked to find a website domain owner, most Users do not think to utilize the WHOIS site
- Some Users recognize the name "WHOIS," but are not aware of what service or value WHOIS provides
- Current domain owners use the most familiar domain register provider to search for a domain owner rather than the WHOIS website (i.e., GoDaddy, Network Solutions)
- Those who no longer maintain a website do not feel they need their own personal website because social media websites allow them to share information easily

Major Findings: Domain Provider Findability

- Users without domain names and who are unfamiliar with WHOIS use a variety of strategies to find domain owners
- By utilizing Google (Maps, Search), Facebook and User-generated reviews about the websites (Forums), Users are able to track down information they find credible and actionable
- Current domain owners are successful in finding the domain owner through their preferred domain register provider.

Major Findings: WHOIS Usability Issues

- Users do not understand the information they find on domain owners and how to use this information due to confusing terminology and formatting
- They overlook pertinent domain owner information because it is underneath Ads for Available and Premium domains

UserInsight

Cultural Differences

Cultural Differences: Australia & China

🇦🇺 “We have to order online all the time in Australia. We have the same ‘rights’ as America; you’ ll find a lot of our regulatory issues are the same in Australia as US, we adopt US policies”

🇨🇳 “No problem to put in personal information, I am comfortable with sharing information online. There are no secrets on the Internet”

🇨🇳 “I don’ t know who to talk to in China. My brother won’ t even do bank transactions online, it’ s not safe”

🇨🇳 “There’ s no way to ‘police’ Internet usage”

🇨🇳 “You don’ t have to go far; It’ s better to shop in person - you don’ t have to go online”

🇨🇳 “Also, shipping is problem [shopping online]. It’ s about education - in rural areas, there’ s no tracking system”

Cultural Differences: Argentina & Brazil

- **Trust:**

🇧🇷🇦🇷 “ think being from Argentina and Brazil we don't trust a lot (Argentina & Brazil)”

🇧🇷 had to trust and let my guard down a little in my neighborhood coming to the US”

🇦🇷 noticed that Americans are more trustworthy. I would be more skeptical in Argentina”

- **Purchasing:**

🇧🇷 “We get ripped off easily when buying things; I approach transactions with concern”

□ 🇧🇷 “I feel comfortable buying products online in Brazil and having them delivered, if I lived in razil”

□ 🇦🇷 “In Argentina, it depends. Maybe if someone already gave me a good experience with the ebsite. But I would be at home if it was delivered; it’ s not like here in the US”

Cultural Differences: France & Spain

- **Purchasing:**

🇪🇸 *'t' s no good to buy online in Spain because you have to wait so long"*

🇪🇸 *"My sibling lives in Spain; One doesn' t buy anything online"*

□ *"The French place a high value in personal relationships, prefer to shop in person, not*
🇫🇷 *nline"*

□ *"I try not to have any automatic charges unless I know how much it' s going to be"*

🇫🇷 *Buying music from an Argentinian website, I was nervous until someone told me word of mouth to make me feel comfortable"*

🇪🇸

Cultural Differences: South Africa

- **Better Business Bureau:**
  - “South Africa has a similar group - the return policies here (US) exceed the return policies South Africa”
- **Reviews:**
  - “It is not easy to get reviews in South Africa; In the US, people review more”
- **Bandwidth & Security:**
  - “We don’t have free wireless in South Africa, bandwidth is difficult”
  - □ I have South African customers and they are paranoid because the level of security in South Africa is bad”

Cultural Differences: South Africa (Cont)

- **Obtaining a domain:**
  - “Here you can have a domain name in five minutes but South Africa is highly controlled and it is difficult to get or even change a domain”
- **Purchasing & Tracking:**
  - “Buying in South Africa is final with certain companies”
  - □ “I do not fear too much - I do buy things in South Africa because sending things from this country (US) is a pain with customs, it’s better to use a South African site when I buy a gift for my mum”
  - □ “Tracking purchases is important, otherwise it will be taken if you can’t track it”
  - If you want to send something to Africa it’s best to get it to you and then send it yourself and track it; if you leave anything outside your house in South Africa it would be stolen, so you should get a signature”

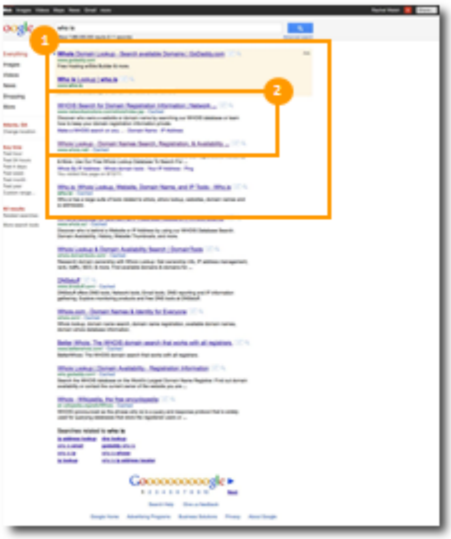
UserInsight | **Detailed Findings**

Google Search for WHOIS

Users:

1. who do not own their own domain name, utilize search engines to look up information about WHOIS
   - Users find a number of site links to click on:
     - www.godaddy.com
     - www.who.is
     - www.networksolutions
     - www.whois.net

2. are unclear about which link to choose based on the search results

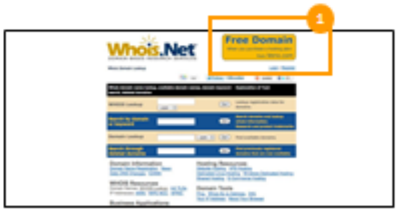


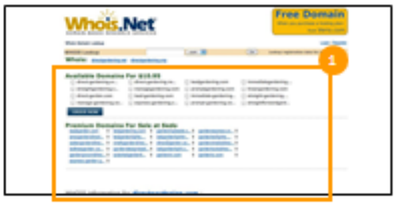
WHOIS.net

Users:

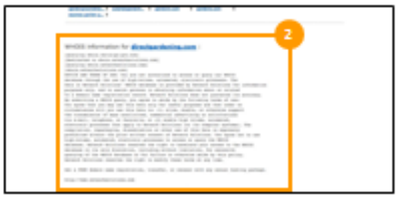
1. are confused by advertising and messaging on WHOIS.net search and results pages

2. overlook content below the fold
   - Users struggle to find helpful information and do not understand what the content is telling them to do (go to Network Solutions and perform a domain owner search)
   - Users do not think to copy and paste the link at the bottom of the text to get to the Network Solutions website





Whois.Net
Free Domain
1
Available Domains For $10.95
Premium Domains For Sale at Sedo



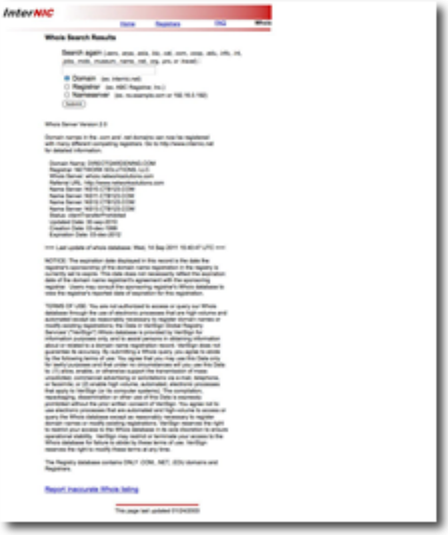
WHOIS Results

Users:

① struggle with the terminology on the domain registrant information page

- Users mistake "Registrar" as the website owner, in this case, thinking Network Solutions owns the website

○ No specific corresponding call out



InterNIC

Home Registrars FAQ Whois

Whois Search Results

Search again (.aero, .arpa, .asia, .biz, .cat, .com, .coop, .edu, .info, .int, .jobs, .mobi, .museum, .name, .net, .org, .pro, or .travel) :

● Domain (ex. internic.net)
○ Registrar (ex. ABC Registrar, Inc.)
○ Nameserver (ex. ns.example.com or 192.16.0.192)
Submit

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

Domain Name: DIRECTGARDENING.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: [illegible]
Name Server: [illegible]
Name Server: [illegible]
Name Server: [illegible]
Status: clientTransferProhibited
Updated Date: [illegible]
Creation Date: [illegible]
Expiration Date: [illegible]

>>> Last update of whois database: Wed, 14 Sep 2011 15:40:47 UTC <<<

NOTICE: [illegible]

TERMS OF USE: [illegible]

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Report inaccurate Whois listing

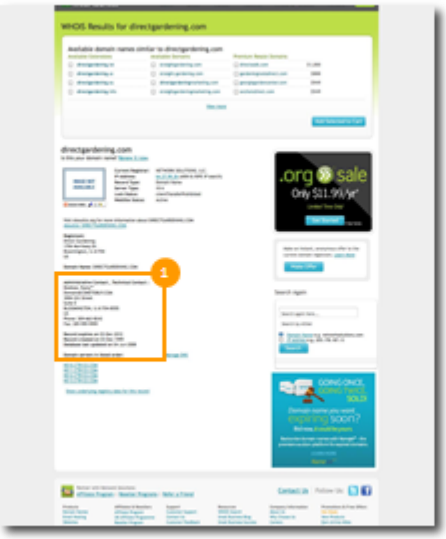
This page last updated [illegible]

Results on Network Solutions

Users:

❶ appreciate level of detail of the content on this page (e.g., the registrant's name)

- This format and presentation is the most successful



WHOIS Results for directgardening.com

Available domain names similar to directgardening.com

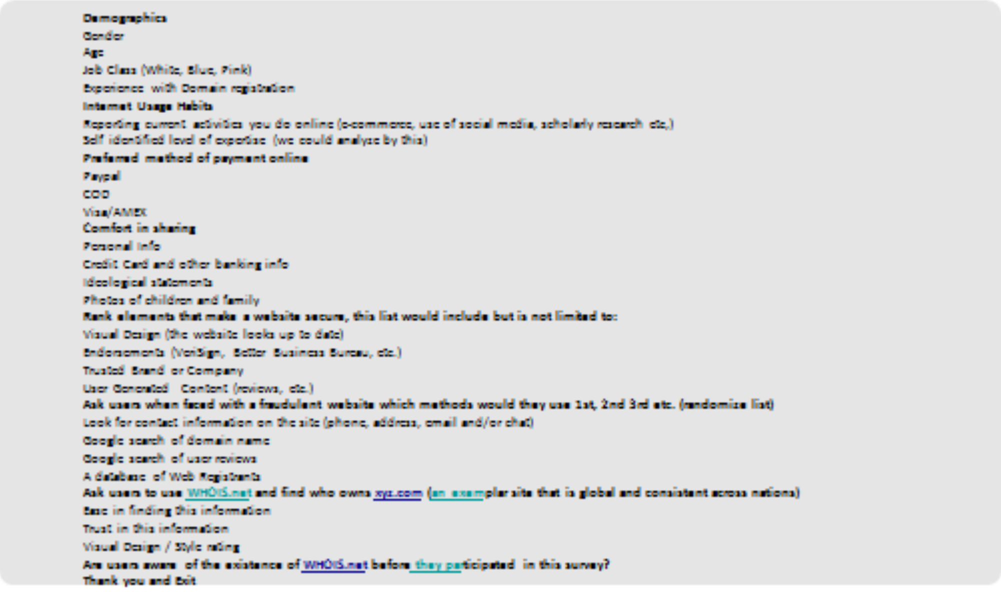
directgardening.com

1
.org sale
Only $11.99/yr*
Search again
GOING ONCE, GOING TWICE, SOLD!
Domain name you want expiring soon?

UserInsight.

Next Steps

Quantitative Survey



Demographics
Gender
Age
Job Class (White, Blue, Pink)
Experience with Domain registration
Internet Usage Habits
Reporting current activities you do online (e-commerce, use of social media, scholarly research etc,)
Self identified level of expertise (we could analyse by this)
Preferred method of payment online
Paypal
COD
Visa/AMEX
Comfort in sharing
Personal Info
Credit Card and other banking info
Ideological statements
Photos of children and family
Rank elements that make a website secure, this list would include but is not limited to:
Visual Design (the website looks up to date)
Endorsements (VeriSign, Better Business Bureau, etc.)
Trusted Brand or Company
User Generated Content (reviews, etc.)
Ask users when faced with a fraudulent website which methods would they use 1st, 2nd 3rd etc. (randomize list)
Look for contact information on the site (phone, address, email and/or chat)
Google search of domain name
Google search of user reviews
A database of Web Registrants
Ask users to use WHOIS.net and find who owns xyz.com (an examplar site that is global and consistent across nations)
Ease in finding this information
Trust in this information
Visual Design / Style rating
Are users aware of the existance of WHOIS.net before they participated in this survey?
Thank you and Exit

UserInsight.

50 Glenlake Parkway, Suite 150
Atlanta, Georgia 30328
www.userinsight.com

T 770 391 1099
866 755 8188

Quantitative Results

UserInsight

ICANN

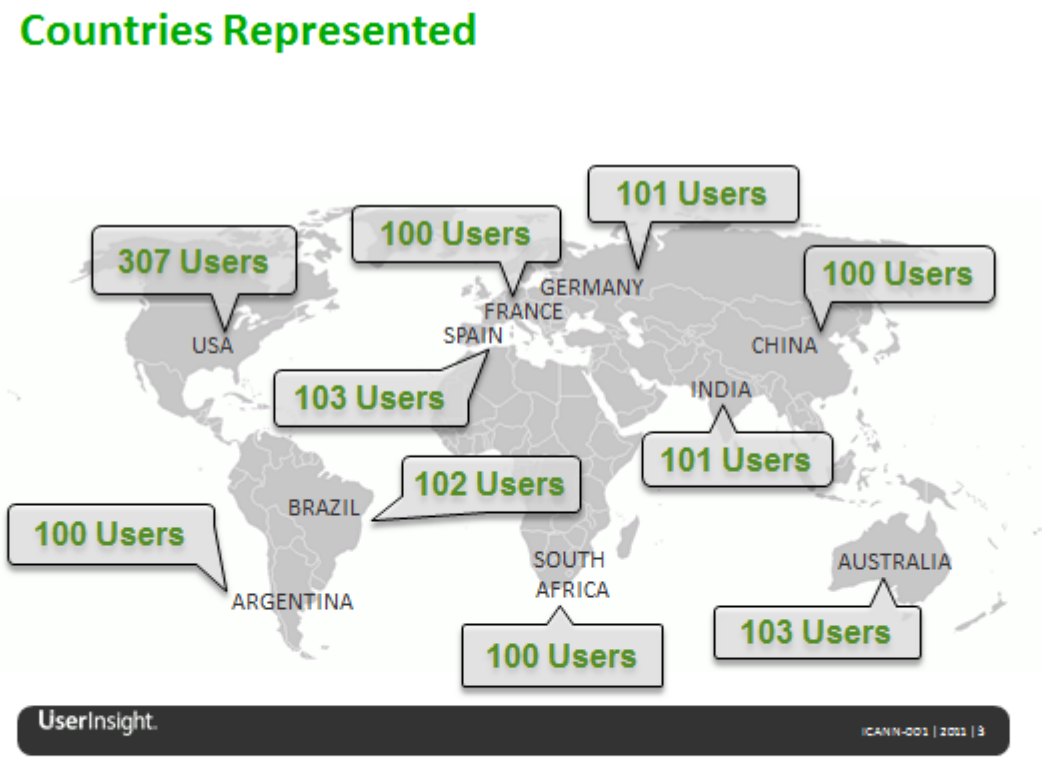
WHOIS Consumer Trust Research

Online Survey Results

Project Background

User Insight, in conjunction with ICANN, conducted an Online Survey with 1,217 respondents from 10 countries distributed across the Asia Pacific region, the Americas, Europe and Africa from September 30th to October 14th, 2011.

The Online Survey was conducted to validate the findings from the In-Depth Interviews held in Atlanta, GA on September 12th and 13th, 2011.



Countries Represented

UserInsight

User Profiles

1,217 Total Users

553 Males

664 Females

468 Users 18-29 years

342 Users 30-39 years

244 Users 40-49 years

115 Users 50-59 years

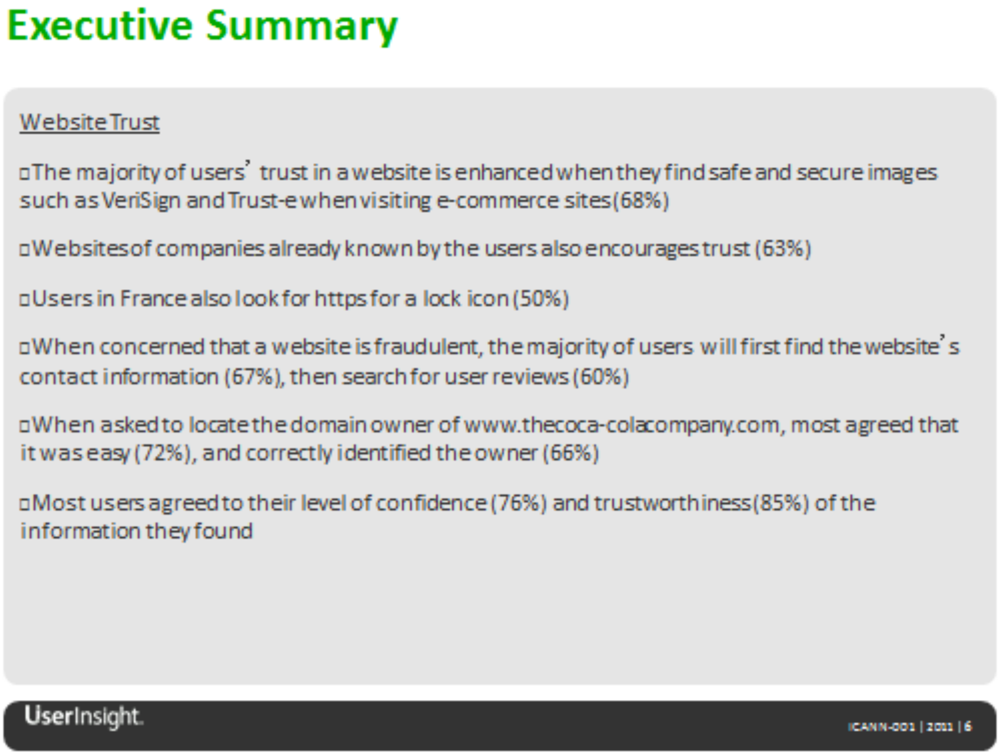
48 Users 60 or Older

Mix of Employment Industry

940 out of 1,217 do not own a website domain

UserInsight

Executive Summary



Executive Summary

Website Trust

□The majority of users' trust in a website is enhanced when they find safe and secure images such as VeriSign and Trust-e when visiting e-commerce sites (68%)

□Websites of companies already known by the users also encourages trust (63%)

□Users in France also look for https for a lock icon (50%)

□When concerned that a website is fraudulent, the majority of users will first find the website's contact information (67%), then search for user reviews (60%)

□When asked to locate the domain owner of www.thecoca-colacompany.com, most agreed that it was easy (72%), and correctly identified the owner (66%)

□Most users agreed to their level of confidence (76%) and trustworthiness (85%) of the information they found

Executive Summary (Cont.)

WHOIS Awareness

□Overall, awareness of WHOIS is low (24%). When asked to find a website domain owner

□Most users did not think to utilize the WHOIS look-up service (77%)

□Most users do not currently own and maintain a personally registered website domain (79%), of the users that do, the majority use it for personal use (60%)

□Of the users that do own a registered domain, only half (50%) were aware of the WHOIS look-up service prior to the survey

□The majority of International users collect personal information or have financial transaction services through their website (54%), however, most National users with a website domain do not (57%)

UserInsight

Online Survey Results

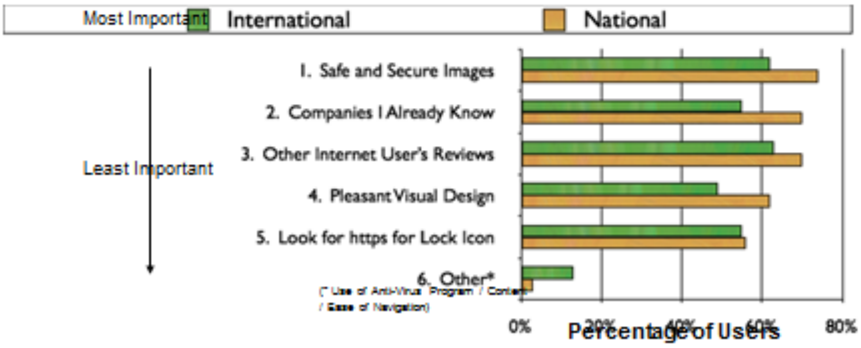
UserInsight

International vs. National

Website Trustability: Most Important Elements

- When determining if a website is trustworthy, 62% of International and 74% of National users rank "Safe and Secure Images" as the most important element.
- "Companies I Already Know" is also of importance, with 55% of International and 70% of National users ranking the element a 1 or 2.

TOP 2 BOX

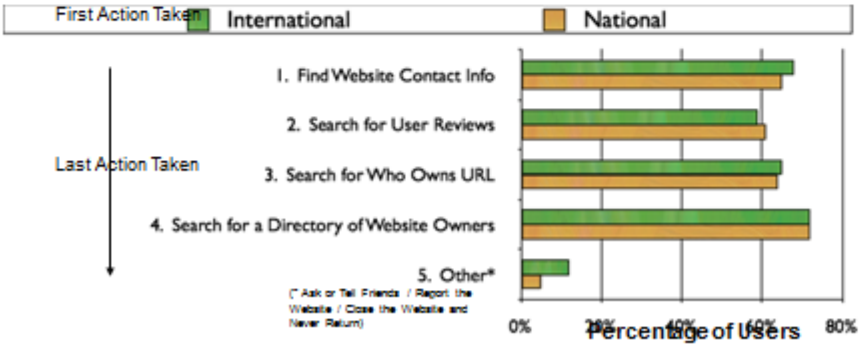


Q10. Please rate the importance of the following elements when determining if a website is trustworthy.

Website Fraudulence: Order of Action Taken

- If concerned that a website is fraudulent, 68% of International and 65% of National users would "Find Website Contact Information" first.
- "Search for User Reviews" is the second step users would take (59% of International and 61% of National).

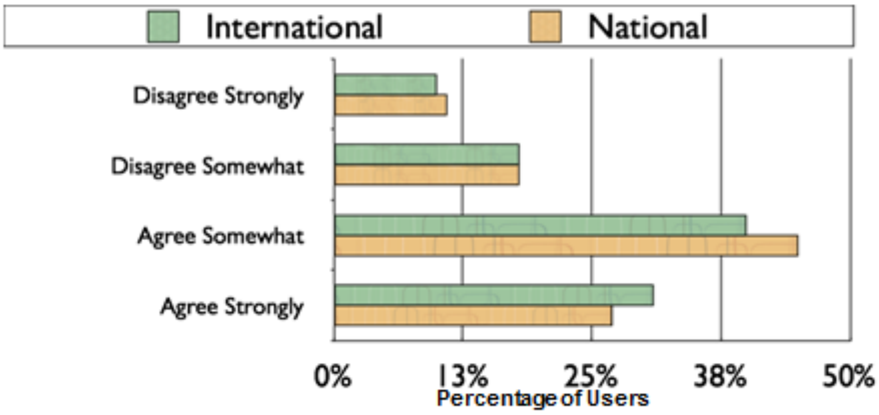
TOP 2 BOX



Q11. If you were concerned that a website was fraudulent or questionable, which of the following would you do first.

Domain Owner Findability: Most agree to the ease of finding the website owner.

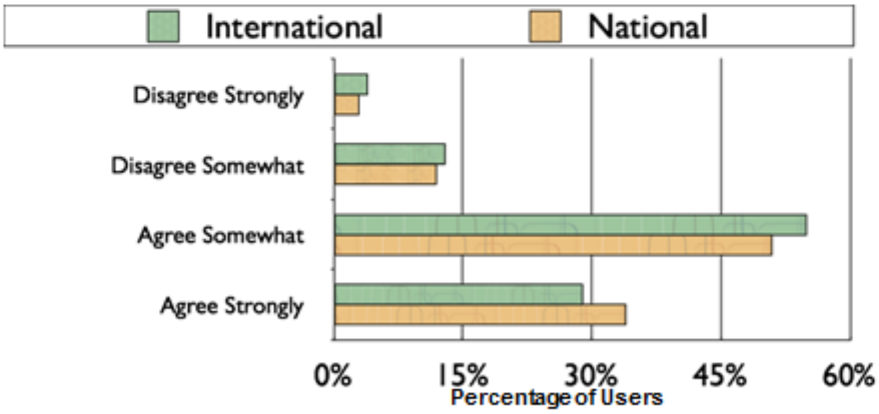
- When asked about the ease of locating the website owner of www.thecoca-colacompany.com, 71% of International users and 72% of National users agree somewhat/strongly that the process was easy.



Q12. I was able to easily find the information on the website owner of www.thecoca-colacompany.com.

Domain Owner Findability: Most agree that they trust the information found on the website owner.

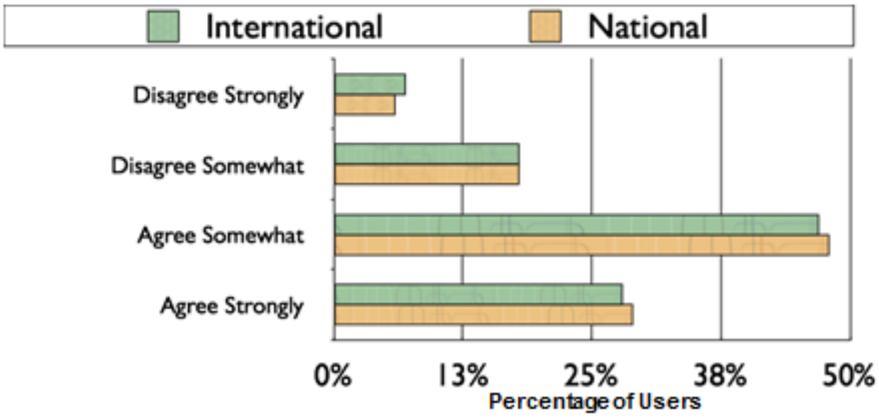
- When asked it they trust the information found on the website owner of www.thecoca-colacompany.com, 84% of International users and 85% of National users agree that the information is trustworthy.



Q13. I trust the information that I found.

Domain Owner Findability: Most agree that they feel confident they found the website owner.

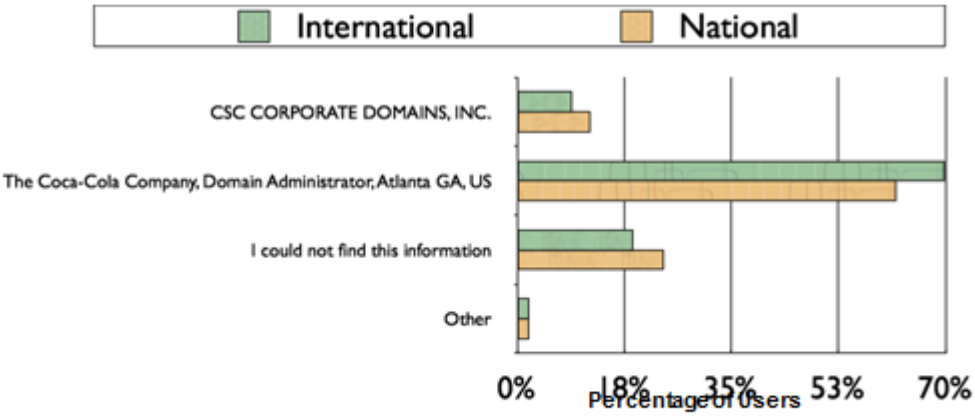
- When asked if they feel confident that they found the information they were looking for, 75% of International users and 77% of National users are confident.



Q14. I am very confident that I found what I was looking for.

Domain Owner Findability: Most correctly identified the website owner.

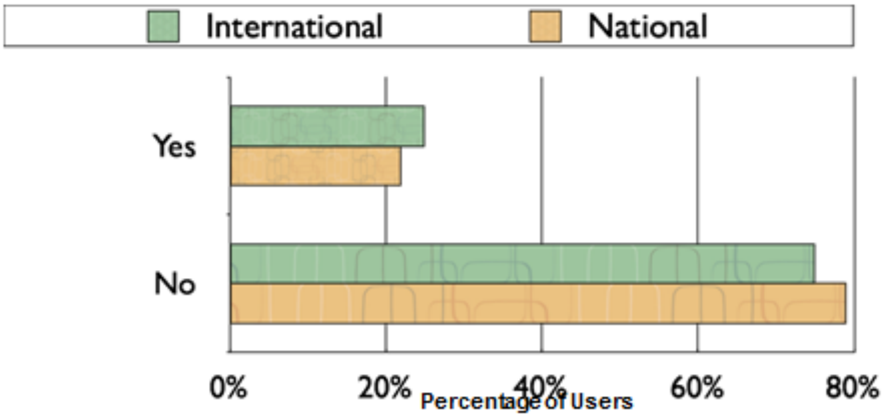
- 70% of International users and 62% of National users correctly identified The Coca-Cola Company, Domain Administrator, Atlanta GA, US as owning the website.
- While 70% of the users correctly identified the website owner, % could not find the information.



Q15. Based on the task you undertook today, who did register the website www.thecoca-colacompany.com?

WHOIS Usage: Most do not use a WHOIS look-up service when locating the website owner.

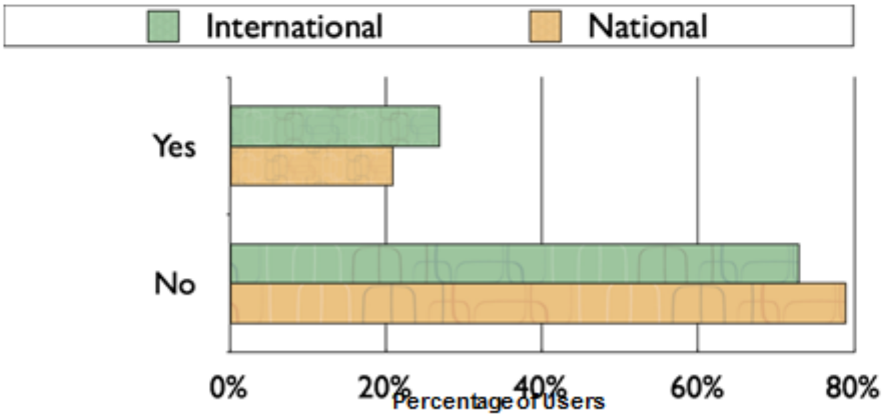
- 75% of International users and 79% of National users indicated not using or being unaware of using a WHOIS look-up service to locate the website owner of www.thecoca-colacompany.com.



Q16. Did you use a WHOIS look-up service to find this information?

WHOIS Awareness: Most were not aware of the WHOIS look-up service.

- 73% of International users and 79% of National users were not aware of the WHOIS look-up service before taking the survey.



Q17. Last question, before participating in our survey today, were you aware of the WHOIS look-up service?

Recommendations

Recommendations

- Consider overall strategy of having domain providers maintaining and promoting WHOIS look-up service
  - Consider that WHOIS.com is the most visible web presence (first Google result)

- Consider endorsement (like VeriSign, Trust-e) of websites that conform to the ICANN policy.

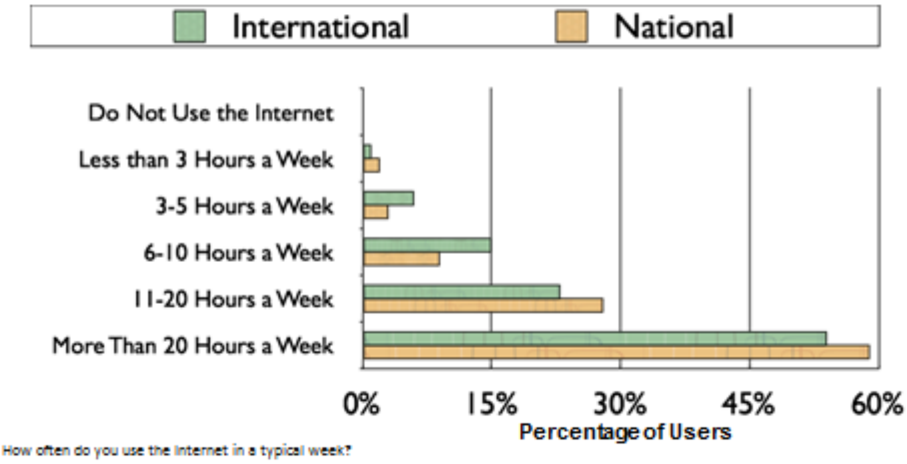
- Consider conducting future research to better understand;
  - Why some users do not trust the information found
  - The impact of incomplete records on consumer trust
  - The impact of single vs. double byte characters for some International users

UserInsight

Appendix

Internet Usage: Most use the Internet 20 hours a week or more.

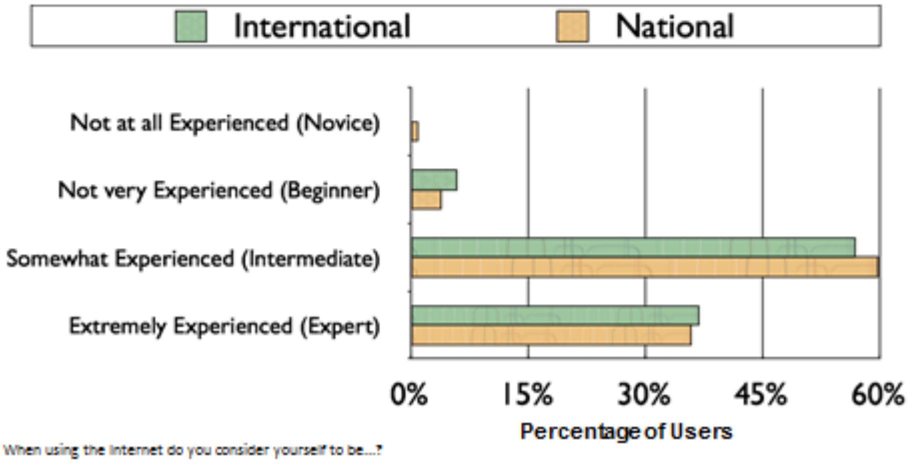
- When using the Internet 54% of International users and 59% of National users use the Internet more than 20 hours a week, followed by 23% of International users and 28% of National users that use the Internet 11 to 20 hours a week.



Q4. How often do you use the Internet in a typical week?

Internet Usage: Most consider themselves somewhat experienced using the Internet.

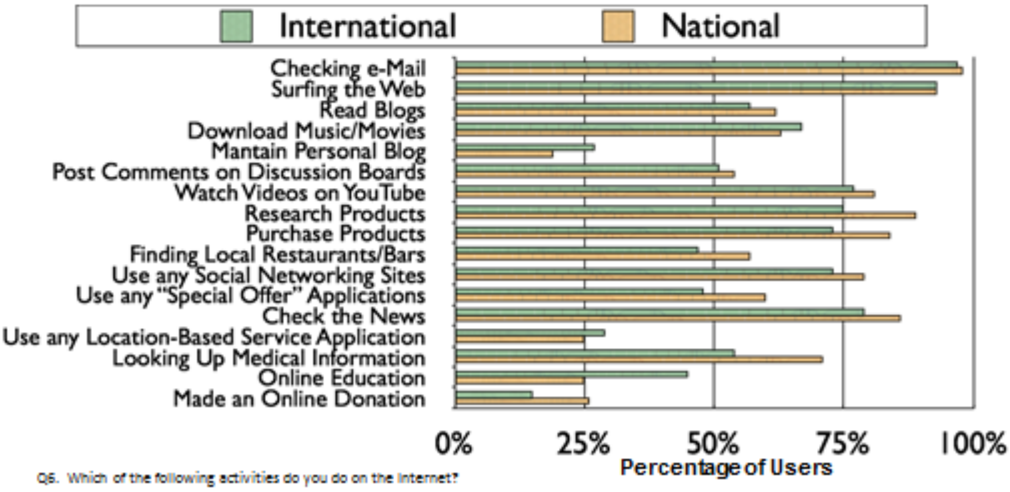
- When using the Internet 57% of International users and 60% of National users consider themselves to be somewhat experienced (intermediates), followed by 37% of International users and 36% of National users that consider themselves to be extremely experienced (experts).



Q3. When using the Internet do you consider yourself to be…?

Internet Usage: Most use the Internet primarily for checking e-Mail and surfing the Web.

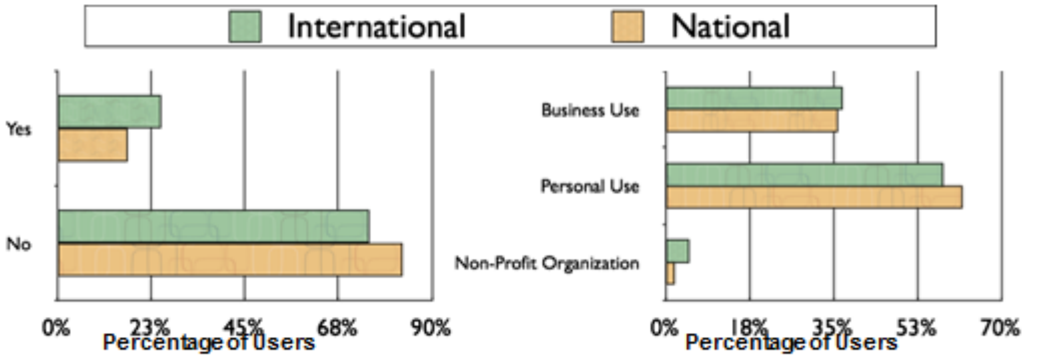
- When using the Internet 97% of International users and 98% of National users use the Internet for the purpose of Checking e-Mail, followed by 93% of International and National users that use the Internet for Surfing the Web.



Q6. Which of the following activities do you do on the Internet?

Website Domain: Most do not own and maintain a personally registered website domain.

- 25% of International users and 17% of National users own and maintain a personally registered website domain.
- Of the users that do own a domain 58% of International users and 62% of national users have it for personal use.

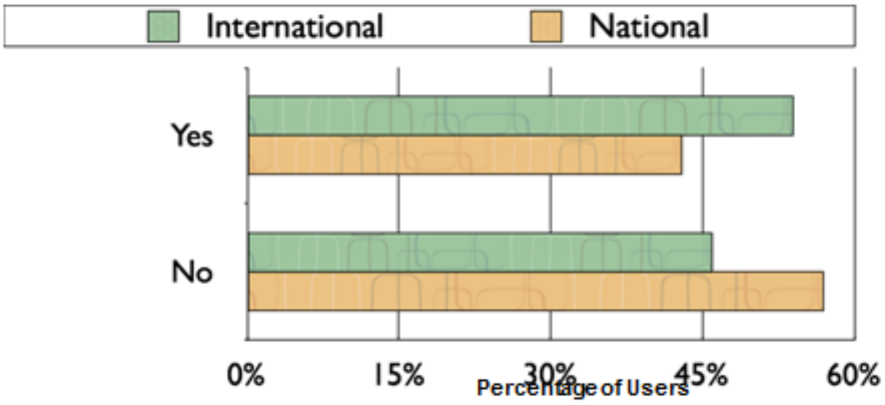


Q7. Do you own and maintain a website domain which you personally registered?

Q8. Which of the following best describes the purpose of your website?

Website Domain: Collecting personal information or having financial features through their personal website is divided.

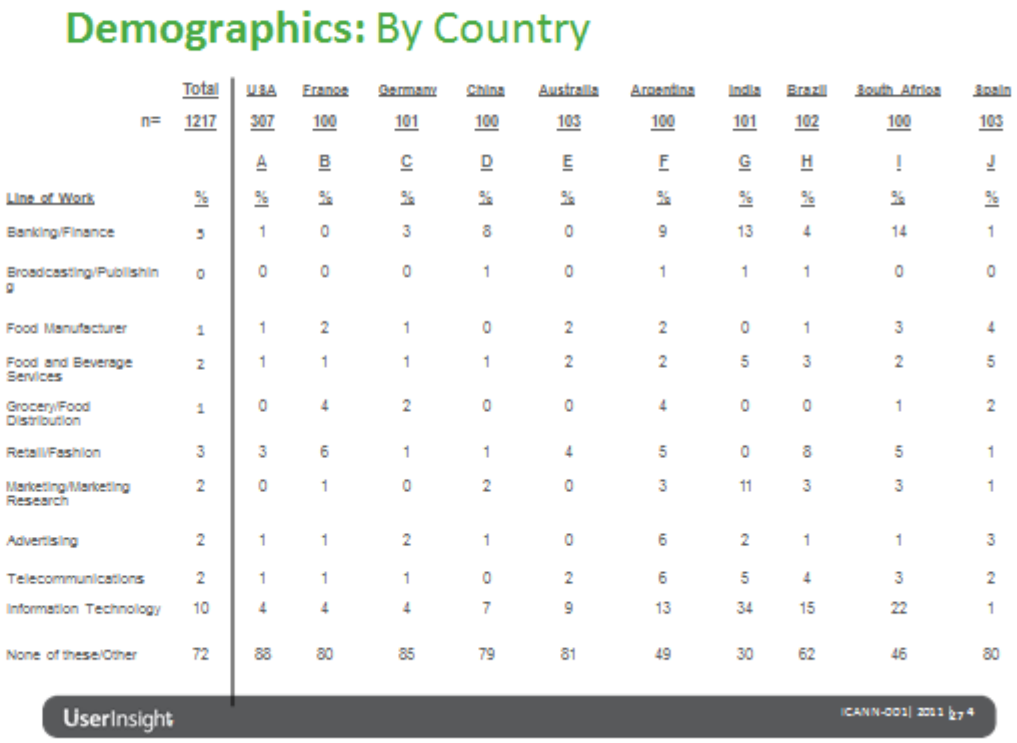
- Of the respondents that do own a domain, 54% of International users indicate they do collect personal information or have financial transaction features through their website, however, 57% of National users indicate they do not collect personal information or have financial transaction features through their website.



Q9. Do you collect any personal information or have financial transaction features through your website?

Demographics: By Country

	Total	USA	France	Germany	China	Australia	Argentina	India	Brazil	South Africa	Spain
n=	1217	307	100	101	100	103	100	101	102	100	103
		A	B	C	D	E	F	G	H	I	J
Age	%	%	%	%	%	%	%	%	%	%	%
18-29	38	30	28	25	31	25	62	68	63	49	20
30-39	28	27	33	34	54	23	19	23	27	25	17
40-49	20	21	21	31	12	21	9	6	9	10	56
50-59	9	12	16	9	2	20	9	3	1	10	6
60 or Older	4	8	2	2	1	10	1	0	0	6	0
Gender											
Male	45	30	46	50	51	51	51	55	51	50	50
Female	55	70	54	50	49	49	49	45	49	50	50



Demographics: By Country

	Total	USA	France	Germany	China	Australia	Argentina	India	Brazil	South Africa	Spain
n=	1217	307	100	101	100	103	100	101	102	100	103
		A	B	C	D	E	F	G	H	I	J
Line of Work	%	%	%	%	%	%	%	%	%	%	%
Banking/Finance	5	1	0	3	8	0	9	13	4	14	1
Broadcasting/Publishing	0	0	0	0	1	0	1	1	1	0	0
Food Manufacturer	1	1	2	1	0	2	2	0	1	3	4
Food and Beverage Services	2	1	1	1	1	2	2	5	3	2	5
Grocery/Food Distribution	1	0	4	2	0	0	4	0	0	1	2
Retail/Fashion	3	3	6	1	1	4	5	0	8	5	1
Marketing/Marketing Research	2	0	1	0	2	0	3	11	3	3	1
Advertising	2	1	1	2	1	0	6	2	1	1	3
Telecommunications	2	1	1	1	0	2	6	5	4	3	2
Information Technology	10	4	4	4	7	9	13	34	15	22	1
None of these/Other	72	88	80	85	79	81	49	30	62	46	80

Appendix E:

Public comments: Received and Submitted

The WHOIS Review Team issued 2 calls for public comment during the course of its year-long review and in preparation for this final report. This appendix sets out the full text of the public comment requests and a summary of written comments received by the Review Team. The full individual comments can be found on the ICANN Public Comment webpages.

Call for Public Comment on the WHOIS Policy Review Team's Activities & Definitions (4 March 2011)

4 March – 17 April 2011

The WHOIS Policy Review Team was launched in October 2010 in line with the Affirmation of Commitments (AoC) provisions, section 9.3.1, which stipulates that: "ICANN additionally commits to enforcing its existing policy relating to WHOIS, subject to applicable laws. Such existing policy requires that ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information. One year from the effective date of this document and then no less frequently than every three years thereafter, ICANN will organize a review of WHOIS policy and its implementation to assess the extent to which WHOIS policy is effective and its implementation meets the legitimate needs of law enforcement and promotes consumer trust."http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm
The WHOIS policy Review Team (WHOIS RT) is composed of ten SO/AC representatives, two independent experts, one Law Enforcement representative, the ICANN President and CEO (Selector)'s designated nominee and the Chair of the GAC (Selector)'s designated nominee. For full reference, please consult:http://www.icann.org/en/reviews/affirmation/composition-4-en.htm.

The WHOIS Review Team held its first formal face-to-face meeting in London, January 2011, and agreed a scope of work, road map, action plan and outreach plan. We submit these materials to the Community for review, input and comment.

Further, on the substantive issues, the WHOIS Review Team's first tasks have been to define key terms from its 9.3.1 section of Affirmation of Commitments scope.

The WHOIS Review Team would welcome public comment on the following issues:

1. Scope of Work and Roadmap
   https://community.icann.org/display/whoisreview/Scope+and+Roadmap+of+the+WHOIS+RT
2. Outreach Plan
   https://community.icann.org/display/whoisreview/Outreach+plan
3. Action Plan
   https://community.icann.org/display/whoisreview/Action+plan

4. List of Key Definitions

1. Law Enforcement:
   "Law Enforcement shall be considered to be an entity authorized by a government and whose responsibilities include the maintenance, co-ordination, or enforcement of laws, multi-national treaty or government-imposed legal obligations."
2. Applicable Laws:
   "Includes any and all local and national laws that regulate and/or control the collection, use, access, and disclosure of personally identifiable information. It may also include other relevant legal obligations, including U.N. Universal Declaration of Human Rights and the U.N. Guidelines for the Regulation of Computerized Personal Data Files.

3. Producers and Maintainers of WHOIS Data:

A. Producers: The individuals or organizations supplying contact data for inclusion into WHOIS data.

B. Maintainers: The WHOIS Review Team proposes to subdivide this category in to:

- Data Controllers: Individuals or organizations that define the data to be collected, require its release, and govern its use. May or may not be directly involved in these functions.

- Data Processors: Individuals or organizations engaged in the collection, storage, and release of data, according to the terms defined by the Data Controller. They do -not- determine the nature or use of the data that they collect or maintain.

4. Consumer:

   What is a "consumer"?

   There is no single universally agreed definition of ‘consumer’, and legal definitions in different jurisdictions vary widely. Some are narrow and limited to ‘natural persons’, while others are broader and include various types of organisations.

   The WHOIS review team has been considering a broad interpretation of the term ‘consumer’, as this would allow a broad range of perspectives to be considered by the review team. This appears to be consistent with the intention of the drafters of the AoC.

   In the global sense, "consumer" may mean:

- *All Internet users including natural persons, commercial and non-commercial entities, government and academic entities*.

And specifically within the context of this review, a "consumer" w.r.t. WHOIS data and WHOIS Service may mean:

- *Any consumer that acts as a Producer of WHOIS data (see above), Maintainer of WHOIS data andprovider of WHOIS Service (e.g. Registrars), or User of WHOIS data (e.g. – individuals, commercial or non-commercial entities who legitimately query the WHOIS data*).

Feedback request from community

Community feedback is desired on the WHOIS Review Team's approach to this definition. Is it too broad or too restrictive? In either case, how should it be changed?

The WHOIS Review Team also welcomes general comments on the above issues, and any other issues which you would like us to consider at this early stage in our work.

The ICANN San Francisco meeting takes place during our comment period and we will be reaching out to the Community. The WHOIS Review Team will hold a public session on Wednesday 16 March 2011 at 11 am – 12 noon in the Elizabethan A-C meeting room: http://svsf40.icann.org/node/22173. We hold a full day face-to-face meeting on Sunday, 13 March which is public and silent observers are welcome to join us: http://svsf40.icann.org/node/21983. Finally, we will be meeting with Supporting Organizations and Advisory Committees in San Francisco and Singapore ICANN meetings (and to arrange a meeting please contact Alice Jansen, alice.jansen@icann.org).
To find minutes of our meetings as well as documents and work in progress, please check our public community wiki at:
https://community.icann.org/display/whoisreview/WHOIS+Policy+Review+Team
Thank you for taking the time to consider these issues and documents. Your participation is essential to the success of the review, and your comments will be carefully considered.
This public comment box will remain open for 45 days consistent with ICANN practices and will close on 17 April 2011.

The WHOIS Review Team
Emily Taylor, Chair
Kathy Kleiman, Vice-Chair

Summary of Comments Received

Summary of Public Comments on the WHOIS Policy Review Team’s Activities & Definitions

This document provides an overview of the public comments[1] received in response to the request for input, issued by the WHOIS Policy Review Teams, which features the scope of work and roadmap, action plan, outreach plan and working definitions. The comments’ summaries are grouped per topic referenced and listed in order of submission. Responses without such references are summarized under "General Comments". The summary does in no way substitute for the original contributions, which should be consulted for complete information. The number of comments submitted on this paper tallies up to 18. The comments are hyperlinked below for easy access and available at: http://icann.org/en/public-comment/#whois-rt

Contributions provided by:

At-Large Advisory Committee	ALAC	Markus Hanauska	MH
Business Constituency	BC	Messaging Anti-Abuse Working Group I II	MAAWG
Coalition against Unsolicited Commercial Email	CAUCE	Othello	OTH
European Communities Trademark Association + Marques	ECTA+M	Registrar Stakeholder Group	RrSG
Intellectual Property Constituency	IPC	Registries Stakeholder Group	RySG
International Working Group on Data Protection in Telecommunications	IWGDPT	Ronald F. Guilemette I & II	RG
Jeff Chan	JC	Volodya	VOL
Lexinta	LEX	.nz Domain Name Commission	DNC

RECOMMENDATION/CONCLUSION	SUMMARY OF COMMENTS
General Comments	**OTH**: See http://forum.icann.org/lists/whois-rt/msg00000.html for details on domain transfers issues in both thin and thick registries. The methods available to registrars for obtaining registrant data are unsatisfactory. The only resource available to facilitate transfers is WHOIS, with an insufficient level of data access. **MH**: WHOIS data is increasingly less valuable due to fake address entries and proxy services. A central registry of domain owners might be useful but does not need to be public. If WHOIS is abolished, the decentralized database of today would still exist, just no longer public. Questions of local law are at stake (e.g. criminal

[1] The public comment period ran from 4 March 2011 to 17 April 2011.

	investigations). Registrars could offer a way to contact domain owners without revealing data. By making all WHOIS data private, the quality will improve more than any ICANN attempt to enforce current policies. The majority of domain owners are neither spammers nor criminals, they wish to protect their privacy. Many more would refrain from using fake data If assured that data will be protected and only revealed to a third party when unavoidable. **VOL**: Restricting WHOIS access to LEA[2] would make matters worse. After hiding the data, the problem would remain but nobody would know about it. An alternative would be to keep the data as public as possible and encourage the use of proxy/privacy services which can be mandated to forward the communication to the real WHOIS holder when non-spam comes in. **MAAWG**: It should be possible to obtain registration information in a standard form and with a consistent set of parameters, as for thick registries. ICANN should require transition of all registries to a thick WHOIS. MAAWG opposes allowing only LEA access to WHOIS. Many issues are outside the scope of LEA and dealt with by security and systems administration professionals. WHOIS is critical for a safe Internet for end users. WHOIS must be as robust and highly available as the DNS and certain data-points must be available to security-related assessment systems. This should be considered a minimum and ICANN must enforce compliance with the rules. Overuse of proxy services impairs security systems' assessment of incoming data. The WHOIS DPRS should be available to the public under reasonable and nondiscriminatory conditions. ICANN should report quarterly on WDRPS reports received, related registrars and follow-up actions. Technological improvement is needed and MAAWG hopes this will be taken into account (e.g ARIN proposal). **CAUCE**: WHOIS is a critical anti-abuse resource and needs to be a true production service offering with consistent formatting in contrast to current practice under thin registries. WHOIS is a community resource and access to it cannot be restricted to LEA without endangering security, stability and trust. WHOIS data must be meaningful but is too often fraudulent. Anonymity options should be eliminated, in particular for corporations. The current WDPRS system should be improved with provisions for bulk reporting of multiple domain names sharing the same inaccuracies and registrar. ICANN should make WDPRS reports public. **JC**: Any reform of WHOIS should consider the likelihood of implementation. An anti-fraud requirement would be that domains have working email addresses to use in the event of abuse. Domains failing this should be at risk of suspension. Proposals to require postal addresses, with non-deliverability of a letter considered proof of breach, are absurd.

[2] LEA: Law Enforcement Agencies.

	DNC: Broad definitions ensure an adequate scope of the review. In many cases WHOIS access and information meet the needs of LEA and, if not, their needs should be accommodated rather than changing WHOIS to meet them. The review scope should state that it does not impact or reflect WHOIS policies relating to the ccTLD community. **ECTA+M:** The WHOIS RT should bear in mind the role WIPO plays. ECTA+M support the AoC statement: *such existing policy […] administrative contact information*- see http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm. Attempts to narrow the scope will have detrimental effect; WHOIS is vital in combating internet abuse. ECTA+M support the maintenance and improvement of WHOIS. Abolition is counter to the AoC and would lead to an increase of abusive activity. **RG**: The RT and Internet community are struggling with questions about the intended uses of domain name WHOIS service and how the service can be made to fulfill its intended uses. There is no charter that codifies the formally anticipated and accepted uses of WHOIS. Such a charter should be produced and the RT could acknowledge this as a goal. Absent this context, the *Law Enforcement* definition would be superfluous. Constituencies may have divergent views on availability and some may favor exclusive access, but LEA should not be the sole authorized users of WHOIS. WHOIS is a source of information for network abuse researchers seeking correlations or patterns, which is an authorized and intended use of WHOIS. The accuracy of the current WHOIS is abysmal and ICANN has neither means nor interest in doing anything about it. Solving the problem is neither prohibitively complex nor costly even though ICANN and registrars attempt to make it appear so. Name, snail-mail address, phone number and email address are generally available in the WHOIS records, but there is no practical way to validate all. Cost-efficient and automated mechanisms for validating phone numbers (Sedo) should be implemented and costs could be passed on to registrants. Automated validation should be required to complete a registration and performed routinely as an integral part of the registration process. ICANN is in breach of its AoC commitments to implement measures to maintain *accurate and complete WHOIS information* and in breach of its agreement with DoC. This needs to be rectified as soon as possible. There appears to be financial incentives for both ICANN and registrars not to consider content of WHOIS records closely. ICANN should require all registries to make available a WHOIS server that would be open to all with unlimited access and provide the same data currently provided by the thin top-layer WHOIS server for the .COM and .NET., in particular the registration data/time and the current name servers. The RT should consider formally defining registration date/time and requiring a new data field for all WHOIS records (recent registration {payment}, date/time). Anti-spam, anti-malware and anti-crime research would be greatly benefited by an irreversible triple-DES hash of what might be called the payer ID. **IPC**: WHOIS policy is among the most important matters addressed by ICANN in its stewardship of the DNS.

	ICANN's current policy and implementation are not effective in delivering the *timely, unrestricted and public access to accurate and complete WHOIS information* required by the AoC. A reliable WHOIS database is critical in building public trust in the DNS, e-commerce and Internet. Robust guarantees of WHOIS accessibility and broad definitions of the operative terms in the AOC are essential. There is nothing in the AOC that suggests the existing policy—of open access to WHOIS data that is collected and provided consistent with applicable law—should be restricted merely to conform with a narrow definition of the legitimate needs of law enforcement and the promotion of consumer trust. **ALAC**: ALAC welcomes this timely exercise especially given the imminent gTLD program. ICANN's implementation of its WHOIS policy framework is based on the RAA obligations and enforcement mechanisms. ALAC is concerned about ICANN's handling of its obligations to the community for contract compliance and remains underwhelmed by ICANN's inadequate enforcement regime. The RT needs to provide answers on whether the principles espoused by the WHOIS construct in the context of the DNS remain relevant. If relevant, the RT should provide guidance as to whether the mechanisms remain fit to purpose. The content of the WHOIS data set, quality and accessibility are the main concerns. Controversy swirls around the understanding of *timely, restricted and public access to accurate complete WHOIS information* as the basis for mechanisms and processes. Some contend that the WHOIS obligations impinge on registrants' right to privacy and threaten free speech, while some argue that privacy means anonymity and others believe in restricted/mediated access, advocating privacy services and unfettered access to registrant data. ICANN is obliged to ensure the collection of the full dataset as required, to ensure the validity of the contents and to enforce the contract obligations. The "know your customer and provider" rule is necessary to combat fraudulent activities and must be a rule for all transactions with economic implications. Balance must be struck between these contentions and ALAC offers guidelines to forge a workable one – see contribution: http://forum.icann.org/lists/whois-rt/msg00012.html. Transparency and accountability demands that registrars remain contractually obliged to collect data to be publicly available and ICANN must hold registrars accountable to this requirement and demand that registrars validate WHOIS data. The right to know should be balanced by a right to know who wants to know. **BC**: The BC supports ICANN's effort to review WHOIS policy and advises the RT to focus on: 1) Measures to ensure *timely, unrestricted and public access to accurate and complete WHOIS information*; 2) Penalties for those who fail to provide access to or abuse the above; 3) Development of policy to address abusive registrations that attempt to evade legal process and law enforcement through use of proxy and privacy services. Policy development should be informed by studies now under consideration in GNSO Council (see http://gnso.icann.org/issues/whois/gnso-whois-pp-abuse-studies-report-05oct10-en.pdf and http://gnso.icann.org/issues/whois/whois-pp-relay-reveal-studies-report-11feb11-en.pdf; 4) Strict enforcement that would require thick WHOIS for all gTLD registries.

	RySG: The WHOIS RT is a key component to meet the specific commitments made under the AoC and RySG therefore supports the work of the WHOIS RT. The RysG recognizes the care and thought that has gone into the definitions. Due to existing workloads, RySG expects to provide further feedback shortly. **RrSG**: The expression *Consumer Trust* is a cause for concern and defining it will be challenging. The RT should adopt a temporary working definition that allows the group to move forward in its mission while continually working to create a more permanent definition eventually derived through a consensus process. **IWGDPT**: The IWGDPT draws the RT's attention to a common position adopted on *Privacy and Data Protection Aspects of the Registration of Domain Names on the Internet*. See: www.datenschutz-berlin.de/attachments/222/dns_en.pdf. While some of the issues have been addressed through the creation of the .name gTLD and more privacy-friendly policies of some registrars, issues in the paper remain valid i.e.: 1) lack of purpose, definition and limitation for WHOIS data (including unlimited port 43 accessibility); 2) insufficient protection against secondary uses (including bulk downloads for offering value-added service and for sending spam); 3) Lack of transparency for registrants about how their data will be processed by registrars and registries.
Law Enforcement – Definition *Law Enforcement shall be considered to be an entity authorized by a government and whose responsibilities include the maintenance, co-ordination, or enforcement of laws, multi-national treaty or government-imposed legal obligations*	**VOL:** The term "law enforcement" is defined without making the scope clear: traffic wardens or NSA? The term "government" also needs to be defined. **CAUCE:** The definition does not distinguish between sworn law enforcement officials and other entities with the mentioned obligations. Law enforcement officers should be narrowly defined as individuals: *1) who have been sworn or commissioned as a law enforcement officer by a government agency of competent authority; 2) who are charged with upholding the general criminal laws of an applicable jurisdiction, including having power to arrest; 3) typically have received specialized peace officer training* (see submission for examples); *4) who normally receive tangible official signs of their role such as police uniform or official credentials.* Adjusting this definition does not mean to exclude non-sworn officials from the scope, they just need another label. It should also be considered whether law enforcement should include national intelligence services and national/multi-national military services. **ECTA+M**: The definition is very broadly drafted. Should private parties interested in enforcing civil law remedies fall within such a definition? If it is intended to refer to law enforcement in the sense of public agencies, then greater care needs to be taken in the drafting. Consideration needs to be given to the range of legitimate legal proceedings whether criminal, civil or administrative, for which access to WHOIS data or extended WHOIS data, should be available. **RG**: Such a definition will only be useful if it has been decided that the WHOIS service will have (or does have)

	some special and particular intended uses unique to *Law Enforcement*. No opinion can be given until a document has been presented into which the definition fits. Should this definition grant LEA access to certain types of WHOIS then it should be drafted broadly. **IPC**: The RT reads this phrase as limited to governmental enforcement agencies but there is no evidence that the AoC drafters intended this reading. The RT should focus on whether this implementation meets the legitimate needs for the enforcement of laws, which mainly depend on the efforts of private parties. Reliable access to WHOIS data plays a significant role in advancing the legitimate needs of enforcement. **BC**: The BC accepts the definition.
Applicable Laws – Definition *Includes any and all local and national laws that regulate and/or control the collection, use, access, and disclosure of personally identifiable information. It may also include other relevant legal obligations, including U.N. Universal Declaration of Human Rights and the U.N. Guidelines for the Regulation of Computerized Personal Data Files.*	**VOL:** Exclusion process should be defined: when local laws and a UN declaration conflict, which is applicable? **ECTA+M**: The definition is narrowly focused on questions of personal data. The RT must also consider other applicable laws for the broader protection of consumers and the public at large, including laws on child exploitation, regulation of drugs and medicine, infringement of IP rights, fraud prevention and spamming. Given that the scope includes promotion of consumer trust, the RT must look beyond registrants and consider global citizens as users of Internet and buyers of goods and services. **LEX**: Refine the definition as follows: *Includes any and all locally applicable laws and legislation in force that regulate and/or control use, access, and disclosure of personally identifiable information. It may also include other relevant legal requirements, including but not limited to U.N. Universal Declaration of Human Rights etc.* National is too narrow: the regulatory system may imply transnational prescriptions (e.g. treaty of law provisions that locally apply). *Legislation in force* reflects more accurately the intended reach of regulation. *Legal obligations* relate to engagement, *legal requirements* or *legal requirements and obligations* might be appropriate formulations. *Included but not limited to*: avoid any possibility of an excessively restricted interpretation. **CAUCE:** The definition is relevant if focus is solely on registrant privacy. Since this aspect must be balanced against the need to protect citizens, the definition should be widened to recognize the applicability of all criminal and civil laws on WHOIS policy, including laws against child exploitation and child pornography, against obtaining financial information by deceit/“phishing”, against spreading malicious software, against online sale of controlled drugs, against IPR violations, against various fraudulent schemes and against spamming activities. **IPC**: This definition lacks the needed precision. The RT must focus on laws applicable to ICANN in carrying out this policy. It seems inconceivable that *any and all local […] information are applicable.* Which law is

	applicable to a particular registry or registrar in carrying out contractual obligations to ICANN regarding WHOIS? It is not helpful to assert that every law related to personal data applies. The RT should give consideration to the ICANN procedure adopted to implement a supermajority vote of the GNSO and unanimous vote of the ICANN Board for dealing with any situation in which contractual obligations appear to conflict with a law applicable to the operations of the registry or registrar. See http://www.icann.org/en/processes/icann-procedure-17jan08.htm. The policy recognizes that there will frequently be ways for registrars/registries to conform practices with applicable law in order to comply with WHOIS obligations. AoC 9.3.1 should be read in the same way. *Other relevant legal obligations* is also imprecise. ENISA has concluded that the UN guidelines are *not legally blinding, neither to natural persons, legal or countries*; see http://www.enisa.europa.eu/act/rm/cr/laws-regulation/dataprotection-privacy/un-guidelines and http://www.un.org/documents/ga/res/45/a45r095.htm. This falls short of establishing any legal obligation that could conflict with or override contractual obligations regarding WHOIS. The RT's mandate in this field is narrow; the broad and imprecise definition proposed for "applicable laws" will do little to assist the RT in carrying out its assignment. Unless it identifies a particular law that has impeded or threatened to impede ICANN's enforcement of existing WHOIS policy, it may not be necessary to reach agreement on a definition of "applicable law". **BC**: The BC accepts the definition. **RrSG**: This definition is adequate with the exception that UN declarations and resolutions are often non-binding and as such inappropriate for the RT's work. Non-binding resolutions do not meet the appropriate threshold for an applicable law and such references should be removed.
Producers & Maintainers – Definition *Producers and Maintainers of WHOIS Data:* 1. *Producers: The individuals or organizations supplying contact data for inclusion into WHOIS data.* 2. *Maintainers: The WHOIS Review Team proposes to subdivide this category in to:* ○ *Data Controllers: Individuals or organizations that define the data to be collected, require its release, and govern its use. May or may not be directly involved in these functions.* ○ *Data Processors: Individuals or organizations engaged in the collection, storage, and release of data,*	**CAUCE:** The definition of "producers and maintainers" mixes parties and roles with different perspectives and interests. A "producer" may be 1) the registrant; 2) a proxy; 3) a registrar or hosting company; or 4) a registrations service provider acting as a contractor or agent for the registrar. These roles may also change over time. The definition leads to confusion and so does the definition of "data controllers", especially the final part of the definition. **ECTA+M:** The RT needs to remember that EU data protection rules only apply to individuals. Businesses and non-persons do not generally have any legal rights to "privacy" and this is reinforced by requirements in many countries for business to register their details in public registers. Whilst the *Producers* definition is broad, ECTA+M believe it is important for the RT to recognize the multiple players that may be involved in the registration of the domain and the scope for the provision of false or inaccurate data. *Maintainers*: ECTA+M recognize the use of language derived from EU data protection legislation, established in Europe for over 20 years with well-known meaning in the context of data protection. The RT should consider carefully how they intend to use this terminology to avoid unnecessary confusion.

according to the terms defined by the Data Controller. They do -not- determine the nature or use of the data that they collect or maintain.	**IPC**: This definition does not refer to AoC wording and there is no explanation on why a definition of these terms is needed. IPC recommends that the RT drop this definition. **BC**: The BC accepts the definition. **RrSG**: Support.
<u>Consumer - Definition</u> There is no single universally agreed definition of 'consumer', and legal definitions in different jurisdictions vary widely. Some are narrow and limited to 'natural persons', while others are broader and include various types of organisations. The WHOIS review team has been considering a broad interpretation of the term 'consumer', as this would allow a broad range of perspectives to be considered by the review team. This appears to be consistent with the intention of the drafters of the AoC. In the global sense, "consumer" may mean: • *All Internet users including natural persons, commercial and non-commercial entities, government and academic entities*. And specifically within the context of this review, a "consumer" w.r.t. WHOIS data and WHOIS Service may mean: • *Any consumer that acts as a Producer of WHOIS data (see above), Maintainer of WHOIS data and provider of WHOIS Service (e.g. Registrars), or User of WHOIS data (e.g. – individuals, commercial or non-commercial entities who legitimately query the WHOIS data*).	**ECTA+M:** The definition of consumer with respect to the WHOIS review does not exclude any person. If this broad approach is intentional, it may be preferable to use a definition which can be understood by all *Consumers* (whether native English-speaker, familiar with WHOIS or not). Otherwise, discussions on possibly excluded persons may arise. On the other hand, in many jurisdictions the concept of "consumer" has well-established meanings that relate to natural persons acting other than in the course of business. In a common dictionary, a *Consumer* is a "person who purchases goods and services for personal uses". The AoC refers to *consumer protection*. If the intention was to mean all Internet users, then the focus should be that on its natural and ordinary meaning. **LEX:** *Consumer w.r.t. WHOIS data and WHOIS Service may mean: any consumer that acts as a Producer of WHOIS data, Maintainer of WHOIS data and Provider of WHOIS Service, or User of WHOIS data (e.g. individuals, commercial or non-commercial entities who query or consult the WHOIS data).* Is it opportune to postulate the "legitimate" nature of the query/consultation? Anyone can consult WHOIS data, legitimately or not and we do not presume that there is an intention to exclude the non-legitimate seeker for data. Use implies query AND consultation. **IPC**: A broad interpretation is probably consistent with the intention of the AoC drafters. The first definition is sufficient but the second one is confusing and leads to the absurd conclusion that the goal of ICANN WHOIS policy should be to promote ICANN's own trust in itself. Internet users rely upon accurate and accessible WHOIS data. The RT needs to apply common sense and conclude that public trust is diminished if this data is inaccurate, inaccessible and unreliable. The first bullet in the definition is consistent with this common sense definition and should suffice. The definition should not be limited to WHOIS users. The fact that domain owners are required to provide accurate ownership and contact data for Internet domain names has a deterrent effect against fraudulent, deceptive and illegal behavior and promotes consumer trust. No definition of Consumer Trust is needed. Consumer Trust - promoted by sound WHOIS Policy and implementation - is the expectation that actors on the Internet will be transparent and accountable for their actions. Users expect to be able to find out with whom they are dealing. If this is upheld, WHOIS can make a substantial contribution to consumer trust. If it undermines or erodes this expectation, it does not promote trust and thus fails the test set out in the AoC.

	BC: The BC supports a broad definition of the term consumer: the first definition. **RrSG**: The RrSG is concerned with the broad scope that *Consumer* may encompass. Creating an overly broad definition will complicate the further definition of *Consumer Trust*. The RrSG recommends that the RT construe the term narrowly in terms of WHOIS specifically.
Scope of Work and Roadmap **https://community.icann.org/display/whoisreview/Scope+and+Roadmap+of+the+WHOIS+RT**	**ECTA+M:** The non-exhaustive list of actions is sensible if conclusions are drawn about the effectiveness of WHOIS in relation to the AoC. In light of the new gTLD program's potential for abuse, WHOIS needs to ensure that there is *timely, unrestricted and public access to accurate and complete WHOIS information*. ECTA+M recognize the need to balance privacy right of individuals with the public nature of WHOIS by: 1) Prohibiting anonymity for legal entities other than individuals; 2) Prohibiting anonymity for individuals where the domain name is business; 3) Allowing anonymity for domains registered in the name of an individual only where there is a means of contact. EU legislation stipulates that traders must identify themselves and their contact details on website. This should apply to domain registration in a business context. Reference is made to the criteria in EU's E-Commerce Directive, see the contribution: http://forum.icann.org/lists/whois-rt/msg00008.html. Regarding IDNs, there is a need for the WHOIS records to be in standardized ASCII/English irrespective of whether the domain is ASCII/English or not. **IPC**: There should be a reference to the review of proxy and privacy registrations. They play an increasing role in the gTLD space and have grown from market need. The current ICANN policy regarding them undermines consumer trust and creates law enforcement concerns. A standardized process for the access to WHOIS data hidden with a proxy or privacy registration is long overdue. The RT needs to analyze the issues with registration data protected by a proxy or privacy service. **ALAC**: ALAC appreciates that the RT contextualized and centered its mandate on the AoC paragraph and the emphasis placed on *public interest*. **BC**: The BC supports the document and recommends that the RT identify specific examples of problems that have arisen due to restrictive, inaccurate or misused WHOIS. Examples should be highlighted and recommended mitigation measures included in the final report, as well as an assessment of whether ICANN is adequately using fact-based studies to inform WHOIS policy development. Over the years work has been done to define and advance these studies; see: http://forum.icann.org/lists/whois-rt/msg00016.html. **RrSG**: Support.
Outreach Plan **https://community.icann.org/display/whoisreview/Outreach+plan**	**ECTA+M:** ECTA+M fully support this plan for openness. Given the limited opportunities for geographical outreach, open access to calls, recordings and email is vital. **BC**: No issue with the outreach plan with the exception of the draft report release. Given that the application

	launch period for new gTLDs may coincide, it may be difficult for BC Members to devote the time needed for a thorough review of the work completed. **RrSG**: Support.
Action Plan **https://community.icann.org/display/whoisreview/Action+plan**	**ECTA+M:** ECTA+M trust the action plan will allow the RT time to process the public comments. The program of work should correlate to the scope to ensure that it meets the objectives of the review. Views should be sought from law enforcement agencies, consumer interest groups, brand owners and their representatives. **BC**: The BC recommends that the RT incorporate the collection of issues resulting from restrictive, inaccurate or misused WHOIS into the Action plan. The RT should review information already available from complete WHOIS studies (ask ICANN staff). The BC supports the inclusion of validated studies from external sources which provide such data. **RrSG**: Support.

Call for Public Comment on the WHOIS Policy Review Discussion Paper (4 March 2011)

WHOIS Policy Review Team – Discussion Paper

Comment Period Deadlines (*)				Important Information Links
				Public Comment Box
Open Date:	9 June 2011			To Submit Your Comments (Forum Closed)
Close Date:	23 July 2011	**Time (UTC):**	23:59	View Comments Submitted

Section I: Description, Explanation, and Purpose

Discussion Paper

The WHOIS Policy Review Team wishes to solicit input from the community on its Discussion Paper [PDF, 182 KB], which calls for feedback on issues identified by the Review Team. The following issues were drawn from areas of interest identified in preliminary discussions and interactions with the community:
Clarity of Existing Policy
Applicable Laws, Privacy issues and Proxy/Privacy
ICANN's compliance and enforcement activities
Other Issues

The community's participation is essential to the success of the review and all input will be carefully considered. The WHOIS Review Team also welcomes general comments and feedback on any other issues that the Review Team should consider.

Section II: Background

The WHOIS Policy Review Team was launched in October 2010 in line with the Affirmation of Commitments (AoC) provisions, section 9.3.1, which stipulates that:
"ICANN additionally commits to enforcing its existing policy relating to WHOIS, subject to applicable laws. Such existing policy requires that ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information. One year from the effective date of this document and then no less frequently than every three years thereafter, ICANN will organize a review of WHOIS policy and its implementation to assess the extent to which WHOIS policy is effective and its implementation meets the legitimate needs of law enforcement and promotes consumer trust."

The WHOIS Policy Review Team is composed of ten SO/AC representatives, two independent experts, one Law Enforcement representative, the ICANN President and CEO (Selector)'s designated nominee, and the Chair of the GAC (Selector)'s designated nominee. For full reference, please consult:http://www.icann.org/en/reviews/affirmation/composition-4-en.htm.
In March 2011, the WHOIS Policy RT submitted its scope of work and roadmap, outreach plan, action plan and list of key definitions for public comment http://www.icann.org/en/announcements/announcement-04mar11-en.htm. In San Francisco, it held sessions with a number of ICANN SO/ACs and Constituencies as well as a general interaction with the community session in order to gather feedback on its working definitions.

Section III: Document and Resource Links

The Review Team's progress, working documents, activities may be viewed on a public Wiki at:https://community.icann.org/display/whoisreview/WHOIS+Policy+Review+Team

Translations of the WHOIS Review Team Discussion Paper:

العربية [PDF, 150 KB]	Español [PDF, 149 KB]	Français [PDF, 135 KB]	Русский [PDF, 196 KB]	中文 [PDF, 224 KB]

Section IV: Additional Information

Activities in Singapore

Please note that the WHOIS Review Team will hold a full day of public face-to-face meeting on Sunday, 19 June in Singapore (Morrison). Public attendance is welcome, but comments should be submitted during the "Interaction with the Community Session" scheduled for Wednesday, 22 June, 14:30-16:00 (Canning). Sessions with ICANN SOs/ACs and Constituencies are foreseen in Singapore; the Review Team's schedule may be found at:https://community.icann.org/display/whoisreview/Singapore+Meeting.

Staff Contact:	Olof Nordling	**Email:**	olof.nordling@icann.org

(*) Comments submitted after the posted Close Date/Time are not guaranteed to be considered in any final summary, analysis, reporting, or decision-making that takes place once this period lapses.

Discussion Paper

WHOIS Review Team Discussion Paper

Questions to the Community, June 2011

INTRODUCTION

WHOIS Review

The WHOIS review team has been constituted under the Affirmation of Commitments (AoC), which was signed by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers on 30 September 2009.

In accordance with the principles set out in the AoC, in particular its paragraph 9.3.1, the scope of the review team is to assess the extent to which existing WHOIS policy in the generic top level domains (gTLDs) and its implementation:

- is effective;
- meets the legitimate needs of law enforcement; and
- promotes consumer trust.

The review team will also undertake an analysis and determination of ICANN's performance against the AoC requirements that ICANN:

- implements measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information; and
- enforces its existing policy relating to WHOIS, subject to applicable laws.

Purpose of this Paper

This paper describes of areas of interest identified by the review team to date, both in its own deliberations and in discussions with the community. The review team seeks comment from the community on any aspect of this paper, including any relevant issues not covered by the paper.

Background on WHOIS

WHOIS is a protocol that enables users to find information about Internet resources including domain names, IP address blocks and autonomous systems.

The current version of the WHOIS protocol (RFC 3912) states that while WHOIS was originally used to provide "white pages" services and information about registered domain names, current deployments cover a much broader range of information services. The review team understands that WHOIS facilitates identification and communication for a range of purposes.

Some issues are potentially beyond the scope of the review team. For example, the review team is aware of work being done elsewhere in the community on the internationalisation of WHOIS data and the technical evolution of the protocol. The review team is also aware that ICANN is considering several WHOIS studies, and that discussions are underway on potential amendments to the Registrar

Accreditation Agreement. The review team will take account of these issues when developing its recommendations.

How to comment

The closing date for comment is 23 July 2011.

Comments should be sent to: whoisrt-discussion-paper@icann.org

ISSUES FOR DISCUSSION

In its preliminary discussions and interactions with the community, the review team's attention has been drawn to several areas of interest which will inform its work going forward. Questions on each of these issues are below.

Clarity of existing policy

The Affirmation of Commitments (paragraph 9.3.1) and 2007 GAC Principles Regarding gTLD WHOIS Services appear to provide high level principles that are intended to inform WHOIS policy development and its implementation. However, it is not clear whether these principles are reflected in ICANN's consensus policies, or in its mechanisms to implement policy.

There is limited ICANN consensus policy on WHOIS, and that which does exist is supplementary to the rules set out in other documents. These include technical standards (such as Internet Engineering Task Force Requests for Comment) and ICANN contracts (such as the Registrar Accreditation Agreement). Current consensus policies regarding WHOIS are:

1. An annual WHOIS Data Reminder Policy designed to improve Whois accuracy (effective October 31, 2003)

2. A Restored Names Accuracy Policy that applies when names have been deleted on the basis of submission of false contact data or non-response to registrar inquires (effective November 12, 2004)

3. A WHOIS Marketing Restriction Policy prohibiting bulk access to Whois information for marketing purposes (effective November 12, 2004), and also

4. prohibiting resale or redistribution of bulk WHOIS data by data users (effective November 12, 2004).

Finally, there is a consensus procedure for "Handling WHOIS conflicts with Privacy Law" (effective January 2008) which details how ICANN will respond to a situation where a registrar or registry indicates it is legally prevented by local/national privacy laws or regulations from complying with the provisions of its ICANN contract regarding the collection, display and distribution of personal data via WHOIS. The procedure is for use by ICANN staff and did not change the obligations of registries, registrars or third parties when approved by the GNSO and adopted by the Board.

Questions

1. What measures should ICANN take to clarify its existing WHOIS policy?

2. How should ICANN clarify the status of the high level principles set out in the Affirmation of Commitments and the GAC Principles on WHOIS?

Applicable Laws, Privacy issues and Proxy/Privacy

The review team understands that some registrants are concerned about publicly sharing their information through WHOIS. The review team is also aware of concerns raised within the community about potential conflicts between WHOIS requirements, domestic privacy laws and consumer protection laws.

The review team is interested in ways that ICANN could balance privacy concerns with its AoC goal of making accurate and complete WHOIS data publicly accessible without restriction.

Questions

3. What insight can country code TLDs (ccTLDs) offer on their response to domestic laws and how they have or have not modified their ccTLD WHOIS policies?

One response to these concerns has been the use of privacy and proxy services, which limit publicly accessible information about domain name registrants. A recent ICANN study found that at least 18% of domain names registered under the top five gTLDs are likely to have been registered using a privacy or proxy service[1].

Questions

4. How can ICANN balance the privacy concerns of some registrants with its commitment to having accurate and complete WHOIS data publicly accessible without restriction?
5. How should ICANN address concerns about the use of privacy/proxy services and their impact on the accuracy and availability of the WHOIS data?

ICANN's compliance and enforcement activities

The review team is interested to examine any gaps between ICANN's commitments, stakeholder expectations and ICANN's actual implementation and enforcement activities. This includes whether ICANN has the power and/or resources to enforce its commitments.

A key example relates to WHOIS accuracy. WHOIS accuracy is mentioned in the AoC, and is also a requirement in policy and contractual documents. However, a recent ICANN report found that, by the strictest interpretation, only 22.8% of WHOIS records could be considered "fully accurate[2]". The report further categorized the accuracy according to the ability to contact the registrants. On this analysis, 22.8 % was considered "no failure", 20.9% "substantial failure" and 7.8 % "full failure".

Some actors in the WHOIS space appear to have little or no direct contractual relationship with ICANN (e.g. resellers and privacy and proxy service providers). The review team is interested to examine whether this raises any compliance issues for ICANN.

[1] http://www.icann.org/en/compliance/reports/privacy-proxy-registration-services-study-14sep10-en.pdf

[2] http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf

The review team is aware that there may be examples of good practice across the ccTLDs with regard to data accuracy, but notes that ccTLD policy is independent of the ICANN process, and that the contractual framework and other elements vary across the ccTLDs, and this should be borne in mind when drawing any comparisons.

Questions

6. How effective are ICANN's current WHOIS related compliance activities?
7. Are there any aspects of ICANN's WHOIS commitments that are not currently enforceable?
8. What should ICANN do to ensure its WHOIS commitments are effectively enforced?
9. Does ICANN need any additional power and/or resources to effectively enforce its existing WHOIS commitments?
10. How can ICANN improve the accuracy of WHOIS data?
11. What lessons can be learned from approaches taken by ccTLDs to the accuracy of WHOIS data?
12. Are there barriers, cost or otherwise, to compliance with WHOIS policy?
13. What are the consequences or impacts of non-compliance with WHOIS policy?

Other issues

The review team is also interested to hear from the community about any other relevant issues relating to its scope.

Questions

14. Are there any other relevant issues that the review team should be aware of? Please provide details.

Summary of Comments Received on the WHOIS Review Team's Discussion Paper

Summary of Public Comments to the WHOIS Policy Review Team's Discussion Paper

This document provides a summary of the comments received from 9 June to 23 July 2011 in response to the request for public comments on a Discussion Paper, issued by the WHOIS Policy Review Team and featuring 14 questions. The comments are grouped per question referenced and listed by contributor in chronological order of submission. Comments not referring to any specific question are grouped under "Other Comments", at the end. The original contributions should be consulted for complete information. In total, 29 comments were submitted by 27 contributors. The comments are hyperlinked below for easy access and available at: http://forum.icann.org/lists/whoisrt-discussion-paper/

Contributions provided by (in alphabetical order, by abbreviation)

AFNIC	AFNIC	InterContinental Hotels Group	IHG
At-Large Advisory Committee	ALAC	International Trademark Association –Internet Committee	INTA
Business Constituency	BC	Intellectual Property Constituency	IPC
Brendan Stephenson I II	BS	Milton Mueller	MM
CIRA	CIRA	Michele Neylon	MN
CNCERT/CC	CNCE	Motion Picture Association of America	MPAA
CNNIC	CNNIC	Non-Commercial Users Constituency	NCUC
Coalition for Online Accountability	COA	Nominet	NOM
Christopher Wilkinson	CW	Patrik Klos I II	PK
Edward Lassotovitch	EL	SIDN	SIDN
Fatima Cambronero	FC	Simon Lange	SL
Frank Ellerman	FE	Time Warner International	TWI
Hogan Lovells	HL	Valentin Höbel	VH
International Anti-Counterfeiting Coalition	IACC		

RECOMMENDATION/CONCLUSION	SUMMARY OF COMMENTS
1. **What measures should ICANN take to clarify its existing WHOIS policy?**	**FE:** Billing, law-enforcement or marketing info in public WHOIS data are not mandatory, but must be correct if present. WHOIS is mainly a last option to obtain contact info if all other ways fail. Public WHOIS data is primarily intended to help domain owners in case of technical problems. ICANN should help registrars communicate this purpose to registrants. **VH:** Remove all personal data and revoke the duty to provide personal data. Introduce a data field with an e-mail address of the registrar who forwards messages to the owner. Remove the annual reminder for registrants to keep their data up to date. **IHG:** ICANN should live up to its commitment to provide open access to accurate registrant information. Proliferation of false WHOIS data undermines ICANN's legitimacy and allows an increase of misleading activities online. Registrars should verify registrants' WHOIS data.

	INTA: ICANN should clarify its existing Whois policy and educate the public and contracted parties on the importance of the Whois policy and of compliance. The Whois policy should be clearly described on the ICANN homepage so the public can understand its purpose and the roles, rights, and responsibilities of all stakeholders. ICANN should describe the implications of providing false or misleading Whois information. A link should be created on the ICANN homepage to the WDPRS and ICANN should take other measures to inform about the WDPRS through educational programs and publications. ICANN should provide staff support to ensure system performance. **IACC:** Assurance of public access to complete, accurate and up-to-date WHOIS data is a core responsibility of ICANN, as restated in the AoC. ICANN has proved deficient in its enforcement of registrar obligations to collect such data and make it accessible. ICANN's compliance efforts amount to "too little, too late". ICANN must fulfill its promises, with emphasis on compliance, and publish policies with the intention to fulfill WHOIS obligations. Changes should be published widely so registrants get adequate notice that their domains are jeopardized if they fail to provide true, accurate and complete WHOIS data. Registrar responsibilities for WHOIS must be clearly articulated. An advisory on registrar deployment of proxy services is a helpful first step. **TWI:** The Whois policy can be discerned from the documents listed in the Discussion Paper and paragraph 9.3.1 of the AoC encapsulates the main objectives. ICANN has sought to implement this policy through contractual arrangements with gTLD registries and registrars. The Review Team should evaluate how well those arrangements advance the basic goal, and how effectively ICANN is enforcing compliance. We urge the Review Team to focus on these areas, rather than on articulating a comprehensive statement of policy in this area. **CW:** The initial purposes of Whois did not extend to the current utilization. More is expected of Whois than it is capable of delivering. Registries and registrars could be obliged to provide verified data about specific domains for which a request had been made. Applying current Whois policy to IDN registries is not obvious. **MPAA:** ICANN should establish WHOIS accuracy metrics, see NORC study for examples. Currently, there is no requirement to verify registrant name and address, nor to determine if country and region code of the phone number correspond with the address. We recommend a single, cross-referenced registry database and a registrant ID. A central database for all registrant data could be used could be used to cross check submitted contact information against existing registrations. If there are inconsistencies, the application and existing registrations could be placed on hold pending verification. These cross checks could query online resources like telephone directories, mapping programs, and credit check services, for which the applicant could pay the fee. A registrant should receive an ID number and a PIN by a trusted entity after verification. Verification could include a government issued ID card, a due diligence telephone call, or an online credit check. The ID would be submitted when applying for new domains or for renewal of an existing domain. **COA:** The documents listed in the Discussion Paper outline clearly what the community requires from Whois: that registrant contact data be publicly accessible through multiple channels, without charge or undue restrictions, and that data be current, complete, and accurate. This is the Whois system that ICANN inherited, but its stewardship has fallen short and the Review Team should issue recommendations to improve stewardship and to realize the full potential of Whois for consumers, law enforcement, right holders, and the public at large. **IPC:** Public access to complete, accurate and up-to-date WHOIS data is ICANN's responsibility, stated in the original MoU and restated in the AoC, but ICANN has not fulfilled its promises in this regard. ICANN must clarify its WHOIS policy and implement it effectively. ICANN should educate the community about WHOIS and the consequences of failing to provide correct data. ICANN must bring gTLD registries into the effort to improve WHOIS, not only attempt to fulfill its WHOIS commitments through provisions in the RAA. ICANN must emphasize contract compliance, including allocation of resources to compliance, publish policies that demonstrate the intention to fulfill WHOIS obligations, and reform proxy registration services. These changes should be widely published so that registrants notice that their

	registrations are in jeopardy by non-compliance with WHOIS requirements. The registrars have been reluctant to see clearer articulation of its obligations but the AoC commitments must override that. Efforts to provide registrar guidance with an advisory regarding proxy services is a helpful first step. RAA provisions on proxy services must be reformed to enable prompt disclosure of data in cases of abuse. **PK:** State the intent of the WHOIS policy, including why registrars are required to collect and present valid WHOIS data for each domain. **HL: T**he policies are concise but the obligations could be made clearer. ICANN must implement WHOIS policy more effectively and ensure compliance. Proxy services should have to ensure prompt disclosure in case of domain name abuse. The WDRP should prompt a registrant commitment to confirm WHOIS accuracy. Failure to confirm could constitute grounds for cancellation. The Restored Names Accuracy Policy should state a definition of "accurate" information and how registrars should ensure that information is accurate. The procedure for handling WHOIS conflicts with Privacy Law appears to allow a case-by-case analysis. ICANN should provide a report with the statistics of recourse to this procedure. ICANN could also consider outreach to registrars to remind them of their RAA obligations for WHOIS. **FC:** WHOIS predated ICANN and was not established as a written policy. There is the RFC 3912 WHOIS protocol and a number of ICANN policy documents, but an easily accessible uniform WHOIS document is needed so users understand the policy. **BC:** In the AoC, ICANN committed to a number of WHOIS obligations and the 2007 GAC WHOIS Principles emphasized the importance of WHOIS accuracy to ensure Internet security and stability, with subsequent GAC documents stating compliance concerns. However, ICANN lacks a comprehensive WHOIS policy and many RAA provisions are weak or unclear (see submission for details). ICANN cannot live up to its AoC commitments unless all stakeholders are required by contract to ensure the accuracy of WHOIS data at all stages of the domain name process. The BC recommends that a) the RAA be amended to require contracted parties to verify the accuracy of WHOIS information. Other industries have employed successful online data verification systems to ensure accuracy of information. Registrars already gather accurate information regarding credit cards and other forms of payment. Valid WHOIS data should equally be a prerequisite to complete a registration. b) ICANN should develop guidelines for contracted parties and registrants informing them about data elements considered valid for WHOIS and processes for verifying WHOIS data. c) ICANN should amend the RAA or develop guidelines instructing registrars how to correct false and inaccurate WHOIS data, including a regular practice of cancelling registrations in appropriate circumstances. d) ICANN should also consider a centralized WHOIS database. Graduated sanctions should ensure compliance with WHOIS obligations.
2. How should ICANN clarify the status of the high level principles set out in the Affirmation of Commitments and the GAC Principles on WHOIS?	**LE:** See answer under 1 above. **VH:** See answer under 1 above. **IHG:** IHG appreciates ICANN's bottom-up policy processes, where brand holders have led WHOIS discussions. WHOIS policy embodies ICANN's commitment and should be strengthened. ICANN should ensure that registrars accept liability for false WHOIS data. **INTA:** ICANN should take measures to ensure all Internet stakeholders, including contracted parties, are informed of the importance of Whois and their obligations. ICANN must bolster its contractual compliance activity to meet its AoC obligations. **TWI:** See answer under 1 above. **COA:** See answer under 1 above. **IPC:** ICANN must publicly state its dedication to the policies articulated in the AoC and make more vigorous compliance efforts. Concrete implementation of the AoC goals should take precedence over drafting a single document with all Whois policies. ICANN must enforce registrant compliance through measures designed to terminate registrations with false data. The RAA should be amended to spell out the responsibility of registrars to terminate registrations in appropriate cases. ICANN compliance should monitor and report on how registrars exercise their current discretion in dealing with registrants. Registrant rights can be protected through notice and cure provisions.

	PK: Can't really say since I haven't read them. **HL:** Provide a detailed definition of the principles and link them to registrar WHOIS obligations as part of the RAA. This would strengthen and clarify these principles, linking the importance of enforcement of the principles to effective actions against inaccurate WHOIS data. Compliance efforts need to be increased against registrars who fail to comply and registrants who fail to provide accurate WHOIS data. **FC:** Preparing a Beginners Guide on WHOIS Policy. **BC:** ICANN must create accountability mechanisms that are specific and measurable. ICANN should undertake a full audit of the WHOIS record set and measure it for accuracy. Third parties have already volunteered to assist in that effort. That audit, combined with studies on inaccurate WHOIS data, would set a baseline for measuring ICANN's compliance with its AoC obligations. ICANN must require contracted parties to live up to their WHOIS obligations, including correcting inaccurate WHOIS data. ICANN must beef up WHOIS enforcement, while allowing flexibility for the way in which registrars comply with their obligations. A public WHOIS dashboard could show performance.
3. What insight can country code TLDs (ccTLDs) offer on their response to domestic laws and how they have or have not modified their ccTLD WHOIS policies?	**LE:** National laws may prohibit mandatory contact data in public WHOIS but not voluntary data. Registrars selling domains in these ccTLDs can communicate why not publishing voluntary data will result in no trust for, e.g., anti-spam applications. **VH:** See answer under 1 above. **MN:** Many European ccTLDs offer a public WHOIS service with limited non-technical information, while law enforcement can access full details. A distinction is made between personal and business domain registrations, for example in .IE. In both cases no personal data is available in WHOIS. In .CO.UK, the WHOIS output shows if a registrant has "opted out", but a company would not have that option. While a business domain does have more data published in WHOIS there is no email address or phone number. Under .EU, WHOIS is limited to technical details and shows more information about a business domain, while a personal one's output is limited to an image of the email address, not accessible to bots. The only gTLD that has followed a similar model is .TEL, where registrants can opt out in a way similar to .CO.UK and the WHOIS output is minimal, while a business registration is more detailed. *See submission for multiple and detailed examples*. **AFNIC:** AFNIC's data publication and access policy describes how registrant data is gathered, disclosed and used during the lifetime of a domain name registration: a) Private registrants' data is not displayed in the public Whois b) AFNIC provides on line web forms to enable any interested party to send electronic messages to the domain name admin contact without disclosing its data c) Right owners or affected parties may request disclosure of registrant data. Such requests are handled by AFNIC which checks whether the affected party has some right over the domain name before disclosing. This policy was set up in 2006 with amendments in 2007 to comply with privacy laws and an instruction from CNIL. While .FR approached 2 million domains in 2010, AFNIC handled 412 data disclosure requests, whereof 356 granted. The policy reinforces trust from private registrants, as they can provide accurate data with limited risk of unsolicited communications, and customer relations suggest that the policy has a positive impact on data accuracy. **INTA:** Most ccTLDs provide the entire Whois record at the registry level, while some provide the entire record only to certain groups such as law enforcement agencies, certification authorities, and registrars that need access for administrative purposes. The extent of information that is shared is generally determined by local law. DENIC publishes all contact information, and German law requires the contact information to be placed on the website if engaged in business. France has a similar requirement. Where there is a need to balance local privacy laws with access to full Whois, mechanisms to improve transparency can be considered, as in the Netherlands. A thick Whois model has been employed in many new gTLDs for years without legal problems or objections from national authorities on privacy grounds. ICANN has a procedure, that a registry can invoke when facing a conflict between its Whois obligations and national privacy laws (see, http://www.icann.org/en/announcements/announcement-18dec07.htm). To date, this procedure has never been invoked.

	TWI: Time Warner commends the Review Team for looking to the Whois experience of ccTLDs, even though ICANN plays only a limited role in this area. ccTLDs may have much to teach the gTLD world in improving Whois accuracy , for example by registrant data verification. **CNNIC:** We provide public WHOIS service with basic and concise information. Registrant information is reachable through the provided WHOIS information. Meanwhile, complete internal WHOIS information can be accessed on LEA request. By doing so, we both protect our registrants' privacy and support legal enforcement. **NOM:** The .UK WHOIS policy was developed in consultation with stakeholders and the Information Commissioner's Office. It meets the requirements of UK law and good practice, protecting the privacy of personal information for non-trading individuals. The .UK WHOIS does not contain the same details as required for gTLDs. It lists: Domain name, Registrant, Registrant type, Registrant's address, Registrar, Relevant dates, Registration status and Name servers. We provide a service, PRSS, for searching domain names, registrants and similar names. PRSS has a web interface, allows use of wildcards and is available to anyone based in the EEA on a contract-only basis. It is aimed at in-house counsel, law firms, brand protection agencies etc, although LES and the Internet Watch Foundation have access. **IPC:** Some ccTLDs have implemented WHOIS data verification protocols that may deserve studying. ccTLDs for countries with privacy laws have experience in balancing data privacy restrictions with the need for accurate WHOIS data to law enforcement professionals, civil litigants and other requesters. ccTLDs that have thick WHOIS may provide insight into whether this leads to more accurate WHOIS data. The experience of ccTLDs that regulate or prohibit proxy registration services should be studied for models applicable to gTLDs. **PK:** If a country has stricter privacy laws than the US, that should have no impact on WHOIS policies controlled by ICANN. Companies should not have privacy in WHOIS records as only shady businesses need privacy to hide from the authorities. For personal use domains, a registrar may provids a form of privacy to the owner, but the information in the WHOIS record must contain a valid email address and phone number for access to someone who can act on technical or security issues, or get in touch with the owner in a timely manner. **HL:** Among ccTLD registries responding to EU data protection legislation, both .EU and .FR differentiate between corporate bodies and private individuals. The .EU WHOIS policy states that full data is displayed for corporate bodies, but data displayed for private individuals is limited to the email address in an image format to avoid data mining. Disclosure of full WHOIS data for private individuals to third parties is subject to requests stating legitimate reasons. .FR also differentiates the public WHOIS data between corporate bodies and private individuals. The latter can request a "restricted disclosure" meaning that no personal information is disclosed and only available to third parties on grounds of a judicial order or upon a request detailing the reasons. Although the approaches are legitimate and the systems in place allow for prompt disclosure, they create an extra burden for rights holder who incur extra costs and lose time when trying to address abusive registrations. This system also prevents rights holders from identifying patterns of illegitimate registrations since the restricted disclosure of data applies to the public WHOIS as well as to data provided to professionals. Rights holders incur the risk of action by these registries if they consider that the disclosure was illegitimate, therefore reversing the liability from potential infringers to rights holders. **BC:** A ccTLD aspect to consider is whether accuracy is improved by having "thick" WHOIS data maintained at the registry level. **CIRA:** Any WHOIS policy must reflect that a registry has to comply with local law. ccTLDs are clearly subject to local laws, and gTLDs must also comply with applicable laws, which may include privacy laws. CIRA policies are subject to local law, and take into consideration privacy and other best practices.
4. <u>How can ICANN balance the privacy concerns of some registrants with its commitment</u>	**LE:** Privacy proxies are not a problem for the primary purpose of WHOIS. Hiding e-mail addresses of domain owners who cannot resolve technical issues with their domain is a "good thing", but third parties should be able to find a technical contact. **VH:** Allow proxy services and introduce the possibility for registrars to provide such a service. Personal data should only be provided to the

	<u>to having accurate and complete WHOIS data publicly accessible without restriction?</u>	registrar and not be public. The registrar may only disclose registrant personal data to local authorities. Domain owners should be able to provide personal WHOIS data if they want to. The need for accurate WHOIS data may not overrule the domain owner's need for privacy protection. Full WHOIS data may be publicly accessible for domains which are owned by companies, authorities and institutions. **MN:** I don't think it can. There are many valid reasons why a registrant may wish to keep some of their data private. I'm also not convinced that making complete WHOIS data available without restriction is such a good idea. **IHG:** There must be a reliable access route to domain registrants, for multiple reasons: 1) Individual consumers, with concerns about their own information have a right to contact domain name administrators with questions and concerns. 2) Complete and accurate WHOIS data promotes consumer confidence in online business. 3) Trademark owners with infringement claims have a right to contact the registrant directly. Direct negotiation could save the time and cost for dispute resolution process. 4) Immediate access to information is an asset for LEA, particularly in pursuit of fraud activities. Barriers to open information trigger due-process requirements before officials can obtain information and act. This could decrease overall user confidence in the safety of the internet. Current restrictions on bulk queries of WHOIS data reasonably protect registrants from massive spamming, and helps ensure that the data will be used for legitimate purposes. **INTA:** INTA supports open Whois access to accurate ownership data for addressing legal and other issues with any domain name. Data should include the owner's identity and accurate contact details. Publishing on the Internet is a public act, and the public should be able to determine who they are dealing with. This is important for domains with commercial content, or registered by entities, where privacy interests are limited or nil. Open access should be the default and for domains registered using a privacy or proxy service, there should be procedures for relaying communications to the owner and for revealing registrant data to a party who has evidence of actionable harm. **IACC:** It is not ICANN's responsibility to balance privacy concerns given its commitment to providing accurate and complete WHOIS data. Any effort to vitiate that obligation would undermine ICANN's commitment. ICANN must accept that WHOIS does not implicate privacy concerns given all the options to engage in free speech without registering a domain name, and that the balancing issue is a matter for other entities. ICANN could quell privacy concerns by emphasizing that anonymous actions on the web are still possible but violations can best be stopped by tracking down the holders of the offending domains. ICANN should highlight that most sectors require accurate information for business licenses, trademark registration, and other services; domain name registration should be no different. The policy can be clarified by assuring that abuse will not be tolerated, and that WHOIS only serves constructive purposes that can prevent web-related offenses and fraud. ICANN should inform about existing security measures, including implementation of rate-limiting systems. **TWI:** A troubling trend is the proliferation of proxy registrations of gTLD domains, and ICANN's inability to bring these in line with its policy goals. The ability to contact the registrant depends on whether the proxy provider decides to disclose information. Not all providers are responsible and divulge information when presented with evidence of abusive activities. While proxy registration may be justified in limited circumstances, the existence of some 20 million gTLD domains with inaccessible registrant data is contrary to the WHOIS policy goal. Unless ICANN brings proxy registrations under some degree of control, its claim to responsible stewardship of Whois will ring hollow. This failure is largely due to an inadequate RAA, identified by GNSO as a top priority for revision. However, in a recent GNSO Council vote, registries and registrars blocked progress on this revision. A modest proposal to issue a registrar advisory on the applicable language in the RAA met opposition from registrars and was never implemented. The Review Team should note the proliferation of proxy services as a major flaw in ICANN's implementation and recommend corrective steps, like clarification and enforcement of the RAA provisions on licensing of Whois data, revision of the RAA to address this more effectively, and requiring thick Whois across the gTLD space. Voluntary "best practices" guidelines for registrars may have a role to play, but are unlikely to be meaningful absent the steps above. Some registrants have legitimate

	privacy concerns which may be at odds with the Whois goals, but the scope of these concerns has been exaggerated and mechanisms are already in place to help registrars or registries to manage conflicting legal requirements. Further adjustments to the implementation of ICANN policies may be called for to address specific privacy concerns, but experience shows that proxy registration is not the solution. **NCUC:** Privacy and accuracy are connected as some registrants use "inaccurate" data as a means of protecting their privacy. Other options to keep this information private may make registrants more willing to share accurate data with their registrar. The problem for many registrants is indiscriminate public access to the data, as the lack of any restriction implies an unlimited potential for bad actors to access and use the data. WHOIS access must give natural persons greater latitude to withhold or restrict access to their data. That position is consistent with EU data protection law and has even been advanced by FTC and FBI in the US. The NCUC recommends reviewing the WHOIS Task Force proposal for an Operational Point of Contact (OPOC), where registrars would publish the registrant's name, country and state/province together with contact information for the OPoC. Registrants with privacy concerns could name agents to serve as OPoC, thereby keeping their personal address information out of the public records. *See submission for multiple references.* **CW:** Unrestricted public access to personal data for individual registrants in Whois infringes EU privacy laws. Accordingly, the AoC qualification that ICANN should enforce Whois policy "subject to applicable laws" exempts registrars and registries in EU/EEA jurisdictions from those policy provisions. However, this begs the question which rule to apply if the registrant is in such a jurisdiction but not the registry nor the registrar. ICANN has a procedure for handling Whois conflicts with privacy law and it would be interesting to learn how many times this procedure has been invoked, and what decisions ICANN has taken as a result. **MPAA:** Most countries require businesses and other entities to provide accurate information in dealing with authorities and the same should apply to Whois data. Some countries have privacy laws affecting the display of ccTLD WHOIS data, but an issue is which laws to apply when a company responsible for registration services for the ccTLD is based in another jurisdiction, e.g. .TO is assigned to the Island of Tonga, yet the company handling the registrations for .TO domains is located in California and does not maintain a public Whois. **CNNIC:** ICANN should promote the enhancement of WHOIS accuracy, but WHOIS policies should respect national laws and regulations in different countries. ICANN should request accurate and complete WHOIS data, but give flexibility to registries/registrars to show tailored WHOIS data to the public, based on national privacy laws. By doing so, some balance could be achieved. Accurate and complete WHOIS information would still be available when necessary, e.g. for LEA; while basic WHOIS service would be available for proper use. **NOM:** In line with UK data protection law, a registrant who is a non-trading individual can opt to have the address omitted from WHOIS. Non-trading is interpreted strictly - the domain should not be used for any revenue-earning activities. If a domain name is incorrectly opted out, we opt it back into WHOIS and lock it to prevent renewed opt-out. We may suspend the domain for breach of terms and conditions. **COA:** There is already a mechanism for resolving conflicts between registrars' (or registries') contractual obligations and privacy laws, and no need for further policy development in this area. Registrants may also require privacy protection in special circumstances, e.g. to carry out political dissident activities in a repressive society. This category of registrants should be accommodated, but the scope of the problem has been exaggerated as there are multiple options to establish an online presence for disseminating views that do not involve registering a domain name in a gTLD, for example thru social media. A repressive state would furthermore have other means than WHOIS to identify dissidents. Further discussions should determine the scope of this problem and identify solutions, but tens of millions of anonymous domain names, just a fraction of which are used for the special circumstances above, is an irrational "solution" that inflicts greater costs than warranted upon legitimate e-commerce, consumer interests, law enforcement and the public at large. That is the "system" now in place, due to widespread proxy registration and unenforced Whois accuracy obligations. That "system" must be fixed.

	IPC: ICANN is committed "to having accurate and complete WHOIS" while the GAC Principles state that WHOIS service should provide "sufficient and accurate data about domain name registrations and registrants subject to national safeguards for individuals' privacy." ICANN is not required to implement safeguards for individuals' privacy, the burden of restricting access to such data in a particular locality falls on the locality. ICANN has a procedure for registrars or registries exposed to liability under privacy laws if they fully comply with their Whois obligations. Global norms about identification data for commercial entities make such entities unlikely candidates for WHOIS data privacy. Proxy services provided to individual registrants in accordance with best practices can satisfy the desire of individuals for WHOIS data privacy. There may be special cases in which particularly vulnerable individual registrants need to be treated exceptionally with regard to the otherwise general obligation for full public access to Whois data. This is an area in which ccTLD experience may be instructive. **PK:** See my answers to 3. **HL:** Striking an appropriate balance between privacy rights of individuals and right holders' interests is essential. The use of thick WHOIS has not led to abuse for which solutions have not been found. The RAA makes it clear that the registrar must inform registrants about the purposes personal data will be used for, the data recipients and how data can be accessed and modified. A registrar best practice for dissemination of this information to registrants would be useful. Adopting a system like .EU and .FR would be excessive as it imposes burdens on rights holders and require resources dedicated to requesting disclosure of registrant data. Such a system may prevent investigation of illegitimate registration patterns and render UDRP provisions moot. Domain names used for commercial purposes should not be allowed to use a proxy service, and should have WHOIS data public, while an individual expressing ideas, with no commercial benefit sought, could justifiably benefit from a proxy service, or a protection as per .EU or .FR. **FC:** Balancing privacy, security and the right to know means to identify minimal data requirements that allow quick identification, like Registrant Name, State/City/Country, email and telephone. The rest of the data gathered should be managed according to national legislation on privacy and data protection. However, not every country has legislated on privacy and data protection. There should be a global study on privacy law to find a model that suits everybody (if possible), with guidance from OECD and UN. **BC:** The GAC Principles note that WHOIS should provide "sufficient and accurate data about domain name registrations and registrants subject to national safeguards for individuals' privacy" in a manner that supports the stability, reliability, security and interoperability of the Internet and facilitates continuous, timely and world-wide access. There must be a balance that allows access to accurate WHOIS information while building in any processes to address privacy concerns. Most countries require businesses to provide accurate information when they apply for a business license, tax-exempt status, or inclusion in a directory of trademarks. Some countries have established that their privacy laws apply to the display of country code WHOIS data. **CIRA:** Accuracy, completeness and privacy are not mutually exclusive. It is possible to have a fully accurate and complete database that also respects privacy. A system with mandatory disclosure of WHOIS information may undermine the goal of accuracy and completeness as it may encourage the use of proxy and privacy services. For this reason, it is worthwhile considering some level of privacy, under appropriate circumstances, in conjunction with appropriate disclosure mechanisms.
5. **How should ICANN address concerns about the use of privacy/proxy services and their impact on the accuracy and availability of the WHOIS data?**	**LE:** See answer under 4 above. **VH:** Allow proxy services. **MN:** If ICANN addressed individuals' privacy concerns, many issues with privacy/proxy services would probably disappear. **IHG:** Privacy services frustrate protection of brands online, which leads to confusion and problems for consumers. Proxy services have become a tool for registrants to avoid making information available to the public. It is not our position to halt these services entirely,

	provided proxy providers maintain accurate registrant data and make that information timely available in case of a legitimate request. The studies of proxy services and their use will be influential in moving forward on this issue. *See* *submission* *for case references*. **INTA:** Where a domain has been registered using a privacy or proxy service, there should be mechanisms for relay of communications to the registrant, and for revealing registrant data upon a justified request in line with RAA provisions. Due to the high degree of non-compliance with these provisions, privacy/proxy services should be governed by rules overseen by ICANN, including relay and reveal processes. Privacy/proxy services would have to assent to these and affirm compliance in annual statements to ICANN in order to operate. **IACC:** ICANN did attempt to address the use of proxy services, with a draft advisory including best practices for the use of proxy services while reconciling with third party needs for WHOIS data. If such an advisory cannot be adopted in a manner consistent with ICANN's contractual relationships, further RAA amendments must be done to minimize the potential for abuse of the WHOIS system through proxy services. More frequent meetings between the ICANN staff and the GAC would also be beneficial to inform GAC of ICANN policy agendas. Multilingual access to Whois would call for further involvement from GAC members, which in turn would promote consensus. **TWI:** See answer under 4 above. **NCUC:** ICANN should recognize that privacy and proxy services fill a market need; the use of these services indicates that privacy is a real interest of many registrants. Concerns about the use of these services are unwarranted. **MPAA:** Proxy/privacy providers supply contact information to a registrar in lieu of registrant data, leaving Whois to identify a proxy service, not the registrant. Suspects seek these services to conceal their identities and many providers operate in a dubious way, being unreachable or not responding to inquiries. The time lapse before data is disclosed gives the suspect ample time to transfer the domain to another suspect entity or otherwise evade detection. We recommend registering and accrediting privacy/proxy companies and prohibiting registrars from accepting registrations from unaccredited proxy providers. As part of the accreditation process, ICANN must require providers to run checks on the applicant's contact data and provide a referral process to parties to disclose registrant data. Failure to disclose this information or perform checks would result in loss of accreditation and public disclosure of all Whois data collected. ICANN-mandated best practices should include a protocol for proxy services to use in responding to requests for registrant data, along with a requirement to provide an abuse point of contact, contact information and physical address of the proxy service. **NOM:** We do not recognize the use of privacy and proxy services. Our contract is with the party that is identified as the registrant. We do not have figures on the use of privacy services, but the provision of an opt-out for non-trading individuals and the fact that email and phone numbers are not in the public WHOIS reduce the need for such services. We would expect a company to use its business trading address or registered office. A sole trader working from a private address might opt to use a third party: we could probably not identify where this was being done. Registrants risk losing their domain names if they cannot be contacted through the listed WHOIS address. **COA:** ICANN must bring order, predictability and accountability to proxy registrations in order to improve accuracy of Whois data, so the service can fulfill its function. COA does not reject the concept of proxy registration in principle, but we encourage the Review Team to study the experience of ccTLDs (such as .us) that do not permit it. There may be legitimate reasons, in limited circumstances, why registrants should be permitted to submit contact details of a third party. Bona fide registrants may well use such a service, but it will inevitably prove attractive to registrants who engage in rights infringements, fraud, or other misconduct. In the experience of one COA member, the majority of sites investigated for high-volume copyright infringement are registered using proxy services. The key is whether a member of the public can gain timely access to the registrant data when it has a bona fide need to do so. The current system is inadequate and section 3.7.7.3 of the RAA is weak and ambiguous. Aggressive enforcement, while needed, will provide only limited benefits. Even

	modest efforts to clarify it through a proposed Advisory have collapsed under opposition from registrars. Whether a third party who presents a justified request to the proxy provider will get the registrant data varies wildly. Reform of the proxy registration system is long overdue and the Review Team should call for such reform as a matter of priority. ICANN could accredit proxy providers, set ground rules for their operation and prohibit registrars from accepting registrations by unaccredited providers. A first step may be to focus on proxy services offered by accredited registrars or their resellers, requiring them to verify contact data from the registrants and keep this data current, to disclose registrant data upon a justified third party request and to respect firm time limits for response. These requirements would be enforceable against registrars, subsidiaries, affiliates, or resellers. Registrars would face enforcement action if they deal with non-affiliated proxy services. A code of best practice among responsible accredited registrars would be at least as effective a way to reform the proxy registration system as RAA amendments, provided all registrars sign up to the code. *See submission for examples and models.* **IPC:** There are critical failures associated with proxy services, which now account for one-fifth of all gTLD registrations. There are many inappropriate uses of proxy services by registrants and registrars, as well as wide variances among proxy services in responsiveness to LEA and third parties request for data disclosure. ICANN should create guidelines and best practices for privacy/proxy services. Registrar cooperation in the development of guidelines and best practices should be actively solicited; but the refusal of some or all registrars to participate cannot justify delay. Given the critical failures and the ambiguity of relevant provisions, RAA amendments are also needed. **PK:** ICANN should require that the email addresses and phone numbers are accurate. It is criminal to put an auto-responder on an admin or technical contact and irresponsible for a technical contact to have a pattern-matching spam/phish filter on their mailbox, as that may prevent people from informing about a domain that has been hijacked or hacked! **HL:** Section 3.7.7.3 of the RAA addresses the obligations of the proxy provider as the Registered Name Holder for a domain, with liability resting with them if they fail to disclose the contact information. However, the ambiguity of certain RAA provisions and increasing use of proxy services push rights holders to make a request for disclosure of registrant data, adding a burden for rights holders. It should be investigated how to balance rights holders' interests in dealing with proxy services and put in place a standardized system allowing immediate disclosure of registrants' information upon request. **FC:** This is important since proxy services can help criminals and delay investigations. A quick and simple procedure should be found, drawing from the Budapest Cybercrime Convention and/or the 24/7 OAS CSIRT. Proxy services could be useful for registrants concerned about privacy or security when legitimate reasons for anonymous speech could justify anonymity. **BC:** Privacy/proxy services may provide a solution for registrants with legitimate concerns about anonymity, but there is ongoing abuse of such services both by providers and registrants, noted in studies as "critical failures". As registrants pay to protect their information using a proxy service, both the registrant and the proxy service reap a benefit and both must also adhere to the WHOIS requirement. A registrar's "proxy service" may also simply be a shell to shield the registrar's own cybersquatting and other illegal activities. ICANN should create guidelines and best practices for privacy/proxy services and step up compliance audits of such services. A study should provide data on the nature of registrants using privacy/proxy services. The findings of this study will provide understanding of the entities and activities of registrants using privacy/proxy services. The findings will set a baseline for evaluating policy changes indicated by other WHOIS studies.
6. **How effective are ICANN's current WHOIS related compliance activities?**	**VH:** ICANN's activities to keep the WHOIS data accurate did prompt our registrar to take action, otherwise the domain might have been lost. Mailing the registrars in order to check the WHOIS data is a good practice. **MN:** They are open to abuse. Many WHOIS complaints are more about disputes between 3rd parties than about compliance. **IHG:** Some registrars make little effort to comply with WHOIS requirements. This enables malicious registrants to engage in infringement,

	to the benefit of those registrars, while undermining the efforts of ICANN to maintain open access to data. Without consequences of WHOIS non-compliance for registries and registrants alike, inaccuracy will pervade the WHOIS database. *See submission for example.* **INTA:** ICANN's Whois related compliance activities are ineffective, as ICANN lacks tools or resources to be effective. Despite the rollout of new gTLDs, ICANN plans to increase its compliance staff only nominally. A key weakness is the absence of a mechanism to ensure that Whois records are accurate. **IACC:** Recent compliance efforts show improvement but remain insufficient. ICANN's studies show widespread WHOIS non-compliance and ICANN's measurements are unduly forgiving. All studies measure system-wide compliance and understate the extent of the problem with those engaging in illegal activity. ICANN is taking steps to insure compliance with the RAA, but RAA deficiencies hamper these efforts. There has been no effort to enforce registrant compliance so efficacy of this compliance activity remains untested. **TWI:** Key RAA provisions related to Whois data are weak, ambiguous or both. This inhibits ICANN's compliance efforts. ICANN's compliance staff should be more aggressive in pursuing non-compliance with the RAA and bolder in issuing interpretations of the RAA provisions. However, there is a limit to what can be achieved under the current RAA, so ICANN should accelerate efforts to revise it. ICANN could also more effectively enforce compliance with 21 registries than with 900 registrars. 19 of the 21 registries today operate a "thick Whois" in which the public may get full registrant data. The two outliers are the largest registries where public access to Whois (through registrars) is inconsistent and sometimes unavailable. The thin registry model was created in order to stimulate competition in registration services. With that market achieved, ICANN should convert the two outliers to thick registries. Compliance with Whois policies will benefit from that. **CNNIC:** The practice and performance of applying ICANN's WHOIS policies has not met the criteria defined in these policies. WHOIS accuracy of .com and .net has been poor and ICANN has failed to regulate them to maintain accurate WHOIS data. ICANN has neither been effective at developing WHOIS policies nor at regulating registrars to improve WHOIS accuracy. **NOM:** For.uk: In case of incorrect WHOIS data, we put the registrant under notice to correct it and suspend the domain name should this not happen. In specific circumstances - where a law enforcement agency has identified criminal activity under the domain name - we can use our terms and conditions to suspend the domain name. The registrant can appeal against this suspension. **COA:** ICANN should do a better job of enforcing the Whois obligations in its contracts with registrars and registries. Revision of those contracts is needed to provide clearer obligations, also extended to resellers. Current Whois-related RAA provisions are ambiguous, weak, or both. ICANN's compliance capability has improved but far from achieving the necessary "culture of compliance", which requires both resources and re-orientation. With new gTLDs, the contractual compliance burden will increase dramatically, while compliance with current contracts is not yet achieved. One third of the budget surplus from new gTLDs should be devoted to contract compliance and enforcement functions. ICANN should be more proactive in its compliance activities and respond more forcefully to complaints. We commend the compliance staff for deciding to review the WDPRS, which is plagued with problems. We hope this will result in a system that is more receptive to complaints, can handle higher volumes, monitors registrar compliance in investigating complaints, requires registrars to reject unverified corrections and encourages registrars to cancelling domains associated with uncorrected false Whois data. **IPC:** The NORC study showed that only 23% of gTLD registrations is fully compliant with accuracy requirements and that current compliance activities are inadequate to fulfill ICANN's AOC commitment. ICANN's compliance function has made progress, but a change in approach is needed in light of the addition of new gTLDs. **PK:** Not very effective. Some registrars follow up with registrants and get updates when the domain is flagged, other registrars don't care if data is correct and don't seem to care about the obligations. When I get a notice 45 days after reporting a domain and click on the "the

	information hasn't been corrected" link, I see no follow-up action taken by ICANN to attempt to get the information corrected. **HL:** The NORC study found that only 23% of gTLD registrations were fully compliant with accuracy requirements, making it clear that ICANN needs to beef up its compliance efforts. This seems to be happening if one looks at the statistics found on the ICANN Dashboard. From 2009 there was an increase in terms of enforcement with 23 registrars having their accreditations terminated or not renewed. The reasons for registrar loss of accreditation over the last four years often include WHOIS related issues. The falling number of registrars who lost their accreditation in 2010 (13) and 2011 to date (4) could be viewed as a positive indication as more and more registrars ensure that they are compliant with the RAA. However, the decline could also be due to a downturn in the ICANN Compliance Team's activities. It could be useful with an analysis of auditing activities resulting in various notifications cross referenced with actions taken by registrars. **FC:** The RAA should be revised so actors without a direct contract with ICANN can be held liable for misuse of WHOIS. **BC:** ICANN has launched additional compliance activities, including audit of Port 43 access by registrars and an inquiry into reminders to registrants regarding their WHOIS data, but these activities are just the tip of the iceberg in terms of needed compliance. ICANN's own studies show that only 23% of records are fully accurate. An organization with a 23% data accuracy record would be considered failing. Compliance resources are needed to fix this and the issue of WHOIS accuracy becomes more urgent with the rollout of new gTLDs. ICANN's compliance organization is well aware of continuing frauds and abuses. As part of the AoC, ICANN's performance in compliance should be measured to assess whether it is meeting its commitments. **ALAC:** The time has come for a change in the philosophical approach to WHOIS compliance. It has become an article of faith that ICANN Compliance is responsible for WHOIS data accuracy. There is also widespread acceptance that the registry/registrar community is responsible for data accuracy and availability. The low expectations of registrants in this area are often noted. Seeing the complexity of the issues we reject these views as unilateral and simplistic. Compliance needs a balanced approach, given the three sets of actors – registrants, registrars and ICANN Compliance. WHOIS data accuracy is a cost/value proposition with differing perspectives from registrants, registrars and users of WHOIS. 100% accuracy is laudable as an objective, but may be unobtainable and puts an unfair burden on one set of actors in the WHOIS triangle. This objective creates an insurmountable threshold for ICANN Compliance, even with best efforts and more resources available. The public interest may be better served by recognizing that the risks from bad actors tend to be cyclical – higher following the establishment of new domains and decreasing thereafter. There is no rational for the same risk to be ascribed to all domains; domains used primarily for support of business transactions on the Web run a higher risk of fraudulent activities than those used for personal or informational pursuits. Adjustments in compliance approach and expectations of the impact might benefit from a change in the philosophical construct of compliance and the processes used to affect the assurance of compliance.
7. Are there any aspects of ICANN's WHOIS commitments that are not currently enforceable?	**VH:** Item 2, that users can determine if a domain is available is useful, and many services look for free domains by checking WHOIS data, but when enough requests for a domain are submitted, those services register the domain on their own. ICANN should find a way to prevent such practices. Item 6, about user confidence in the Internet, cannot be "enforced" and most users are not even aware of the WHOIS service. Item 7, about the assistance of business and organizations, is not enforceable when a proxy service is used. **INTA:** Accuracy is one area of particular concern as noted in the response to question 6 above. **TWI:** See answer under 6 above. **CNNIC:** According to ICANN's current WHOIS policy, complete and accurate WHOIS information of registrants should be made available to the public. However, it is impossible for ICANN to fully execute the policies. Current policies have not clearly defined registrars' obligations to reach a certain WHOIS accuracy level and the policies conflict with privacy laws in some countries. ICANN should respect and consider

	privacy laws of different countries when developing WHOIS policies, and also more effectively regulate accredited registrars. **COA:** See answer under 6 above. **IPC:** Steps have been taken to resolve issues related to privacy laws. The biggest barrier to enforcement of ICANN's WHOIS commitments is the lack of consequences for the parties involved when accurate and complete WHOIS information is not maintained. ICANN’s commitments cannot be met if no negative consequences result for ICANN, registrars, registries or registrants who supply false data. Lack of due consequences gives the appearance that the commitments are unenforceable. **PK:** ICANN must be willing to cancel its agreement with a registrar if the registrar fails to comply with the terms. The biggest example of this is the misuse by DROA, using WHOIS as their mailing list, with false "renewal notices". ICANN should canceled the agreement with DROA! **HL:** There is a disconnect between compliance with the EU data protection directive and the registrar’s WHOIS obligations in the RAA. The Procedure for Handling WHOIS conflicts with Privacy Law seems to address this and it would be interesting to get an overview of how well this is working or if it is indeed open to abuse from "bad actors". **BC:** See response to Question 1. ICANN cannot meet its AoC commitments unless all stakeholders, including registrars, are required to ensure WHOIS accuracy. The RAA should be amended to require contracted parties to verify WHOIS data accuracy and penalties are needed to ensure compliance with WHOIS obligations related to accuracy and access. ICANN manages registries and registrars through contracts, so anything that can be made part of those contracts should be enforceable. That includes new consensus policies adopted by ICANN that automatically become enforceable on contract parties. Given this, all ICANN’s WHOIS commitments can be made enforceable.
8. **What should ICANN do to ensure its WHOIS commitments are effectively enforced?**	**VH:** Promote and explain the WHOIS service to normal users. **IHG:** Compliance with WHOIS data reporting should remain compulsory and included in the RAA. Noncompliance should be met with enforcement, including fines. Registrants who submit false information should have all their registrations suspended until WHOIS data is correct. Severe repercussions should be reserved for registrars who intentionally disregard WHOIS policy, and profit from illegal and unethical registrations. With no disincentive to non-compliance with WHOIS requirements, registry services have little motivation to publish registrant data that could be accessed by competing registries. This could lead to hoarding of registrant data by registrars to prevent rivals from obtaining a competitive advantage. If WHOIS requirements are fully enforced, some mechanism is needed to prevent this scenario and quell registry reluctance to publish client data. **INTA:** Include clear obligations in the registry and registrar contracts and provide clear advisories on those obligations if differing interpretations emerge. Significant resources are needed to monitor compliance and ensure that effective enforcement is in place. Another option is to implement thick Whois at the registry level in order to have a single validation point. The provision of Whois information at the registry level under the thick Whois model was deemed essential by the IRT and advanced as one of their five key recommendations. **IACC:** ICANN must amend the RAA to reflect the interest of the wider community, not only the registrars. The amendments should clarify ICANN's and registrars' responsibilities for a transparent and accurate WHOIS and should provide meaningful tools for ICANN in the event of noncompliance. ICANN should commit more resources to compliance and deploy those resources to increase WHOIS accuracy. **TWI:** See answer under 6 above. **COA:** See answer under 6 above. **IPC:** A change in enforcement policy is needed. Policies need to be developed which provide incentives for compliance by registrars and consequences for both registrars and registrants when WHOIS information is not available in line with the AOC commitments. **PK:** Cancel the agreement with DROA and take action when necessary. Don't be like the government and create rules if you're not willing to

	enforce those rules and stand up to those who would take advantage of your inaction. **HL:** The AoC requires ICANN to maintain timely, unrestricted and public access to accurate and complete WHOIS data – and enforce this. ICANN should ensure that WHOIS accuracy is a requirement with clear consequences for failure to comply by either registrar or registrant. ICANN needs to continue auditing registrars to ensure RAA compliance and to weed out non-compliant registrars who don't cure when alerted. The removal of "bad actors" is essential to provide assurance to the community. By placing the registrars under pressure with the threat of loss of accreditation, ICANN is correctly focusing its compliance efforts. The WDRP could be made more robust by stating that failure by the registrant to confirm WHOIS data would be grounds for the cancellation of a domain. **FC:** Warnings and then fines. In civil law it is commonly used when gathering personal data to assure that they are correct to sign affidavits. To provide incorrect information is a felony. **BC:** See responses to Questions 1, 5 and 6.
9. <u>Does ICANN need any additional power and/or resources to effectively enforce its existing WHOIS commitments?</u>	**VH:** I don't think so. **IHG:** The compliance task is monumental and additional compliance staff and budget will be needed to achieve complete and accurate WHOIS data. ICANN should devote one-third of the surplus revenue from new gTLD applications to contract compliance activities. **INTA:** In light of the addition of new gTLDs, the compliance department must be expanded significantly in both staff and authority to ensure enforcement of existing Whois commitments. Accreditation of privacy/proxy services would go a long way to promote compliance. **IACC:** Yes. Better tools should be provided through the RAA and ICANN should allocate resources to insure compliance with WHOIS requirements by both registrars and registrants. **TWI:** See answer under 6 above. **COA:** See answer under 6 above. **IPC:** Resources are critical and one-third of the surplus revenue from new gTLD applications should be dedicated to contract compliance activities. ICANN's compliance philosophy needs re-orientation. ICANN has stepped up its compliance efforts, but still approaches the commitment as one that may be impossible to accomplish. Compliance staff has stated that many registrars "don't know their obligations" for WHOIS and that it is unclear who is responsible to comply with the RAA provisions. Policies are needed that require registrars to take proactive steps to institute WHOIS compliance programs. Registrars should designate a WHOIS Compliance Officer responsible for WHOIS compliance. That officer should list contact information with ICANN's compliance department and failure to keep that information current should have consequences. Registrants should bear consequences including freezing and cancellation of the registration; and ICANN compliance staff should aggressively monitor registrar actions to ensure these consequences occur. ICANN should publish ratings of registrars based on WHOIS accessibility and quality, and efficiency in combating false data, to inform the public. **PK:** Additional resources? Maybe. Additional power? No. ICANN already has all the power it needs to pull the plug on registrars and registrants that are not willing to comply with long established rules for domain ownership. **HL:** Registrar and registry compliance is of growing importance and ICANN must show that it is taking this issue seriously. ICANN should also demonstrate that it has sufficient resources to enforce compliance of the agreements with the registrars and potential new gTLD registries. By doing so, ICANN will reassure the community that registrars (non)compliance with the RAA is being addressed seriously. Compliance and associated issues will increase with the new gTLDs and the issue of registry/registrar vertical integration and full cross-ownership. ICANN will require significantly more resources for compliance issues. In June 2010, the then Senior Director of Contractual Compliance, David Giza, stated that there were six people working in compliance within ICANN, that they were understaffed and

	underfunded. and that they only had one auditor, needing at least six in order to address the compliance issues. Staff lists show that there are eight people involved in compliance and this needs to be improved upon. With new gTLDs, compliance issues will increase overall. Funds from new gTLD applications need to be used to beef up compliance in proportion to the number of new gTLDs accepted. The funding of compliance activities has been lacking for years, and is the reason why many registrars have no concern about such issues.
10. **How can ICANN improve the accuracy of WHOIS data?**	**VH:** Provide a service for registrants to update their data directly on an ICANN website. The intermediate step with a registrar often fails since some don't update the information. Remove all prices for domain updates. Updating a domain should be free. **MN:** Give private registrants the ability to "opt out". **IHG:** Shifting some or all responsibility of maintaining data to the registrant could make WHOIS more dependable. Registrars have little ability to confirm that data provided by registrants is reliable, making it problematic to charge those with ensuring data accuracy. A RAA provision for compulsory data authentication would provide registries with the ability to comply with WHOIS reporting requirements. **INTA:** There are no mechanisms in place to ensure the accuracy of Whois data provided by registrants, just a presumption by registries and registrars that such data provided by registrants is accurate and a lack of incentives for registrants to provide accurate data. A validation process funded by additional fees paid by registrants should be considered, as well as penalties like loss of registration if data is found to be inaccurate. In cases where Whois data problems have been reported, there should be obligations to verify any replacement data offered by the registrant, as opposed to applying the same presumption of validity once any change has been made to the inaccurate data. **IACC:** Amendment of the RAA, enforcement of its WHOIS provisions against both registrars and registrants and publication of policies to the community to inform about these changes. **TWI:** Inaccurate Whois data is a problem that undermines the goals of the service, erodes public confidence in the online environment, complicates online enforcement of consumer protection, intellectual property, and other laws, and increases the costs of online transactions. ICANN has taken steps to quantify the scope of this problem but has done little to address it. The RAA puts responsibility for Whois data accuracy on a party with whom ICANN has no contractual relationship – the registrant. Registrars have the obligation to investigate reports of false Whois data, but no responsibility to check the accuracy of the data submitted, nor an obligation to cancel the registrations of those who submit false data. The responsibility for Whois data accuracy must be shifted to those that can achieve it and have contractual obligations to ICANN – registrars, registries or both. ICANN has taken steps toward this goal in the gTLD environment. In three registry agreements (.mobi, .tel and .asia) there are Whois data quality obligations that flow through registries to registrars. ICANN was asked to do the same for all new gTLDs, but refused. However, ICANN has given an advantage to new gTLDs that verify registrant data by giving them an extra point in the evaluation. Whois accuracy Improvement may occur once these practices become norm for new gTLDs. **NCUC:** See answer under 4 above. **CW:** Accuracy of the data has always been requested. If nearly 30% of records are still inaccurate, we might be barking up the wrong tree. Registrars have long asserted that full verification of the accuracy of all records, including a considerable backlog, would be financially unsustainable. If so, a different approach is needed. If not, then serious compliance efforts would be required, including budgetary aspects. As this matter has not been resolved since the creation of ICANN, I wonder what new elements have arisen to facilitate a solution now. **MPAA:** See answer under 1 above. **NOM:** For.uk: We have assessed the accuracy of .uk WHOIS and found that accuracy of opted-out domain names is higher than average, with 92 % traceable postal addresses. We perform overviews by batches. **COA:** Current high levels of inaccurate Whois data flow from ICANN's decision to place sole responsibility for Whois data quality on the

	registrant with whom it has no contractual relationship. Registrars insist that their only contractual obligation is to respond to reports of false Whois data, rather than to verify data accuracy or cancel registrations based on false Whois data. The largest registries have even less role to play on Whois data quality currently. Registries and registrars should share responsibility for Whois data quality, with greater involvement of registries through “thick Whois”, which all but two gTLD registries now employ. In these gTLDs with registrant data maintained by the registry operator, as well as on a distributed basis by registrars, the registries share responsibility for Whois accuracy (and availability), and provide a more accessible and accurate Whois. While there may be technical issues in transitioning .com and .net to thick registry operation, ICANN should commit to doing so and set a timetable for achieving this. There should be “Flow through” obligations to registrars. Registries in three gTLD registries (.asia, .mobi and .post) are required to hold their registrars to Whois data quality standards. ICANN should revise all registry agreements to incorporate similar standards. There should be data verification requirements when registrar collects registrant data. Currently, registrars reject any contractual obligation to ensure that data is complete and accurate. Registrars can do much to check and verify the data the registrant presents and they do check for billing information (credit card data), but not for Whois data. ICANN has never required them to take these steps, but has made it clear for new gTLDs that verification of Whois data is preferred, giving an extra point to new gTLD applicants with such a commitment. Not until this approach is made the norm will significant progress toward more accurate Whois data be achieved. **IPC:** Policies are needed that provide for proactive registrar compliance and for consequences associated with inaccurate data. ICANN should swiftly bring the last two gTLD registry outliers (.com and .net) to operate thick Whois; require all gTLD registries to pass on to their registrars Whois data quality obligations, building on provisions in the .asia, .mobi, and .post agreements; and operationalize the preference expressed in the new gTLD evaluation criteria by providing all gTLD registries and registrars with incentives to verify Whois data. **PK:** By enforcing current regulations and canceling agreements with registrars that fail to comply with obligations. Registrars should be reminded that they should cancel registrations for registrants that don’t provide accurate and complete data. **HL:** By continuing to focus on registrar compliance with their WHOIS obligations, ICANN can take steps to ensure accurate WHOIS data. Enforcement of section 3.7.7.2 of the RAA with threat of termination of the accreditation if appropriate action is not taken provides good leverage to ensure accurate WHOIS data. The citation of this section has often resulted in action by the registrar to contact the registrant and to ensure correct WHOIS data. Trade mark owners should not have to pay legal counsel to cite this section in order to clean up WHOIS! The WDRP could be made more robust by stating that failure by the registrant to confirm WHOIS data would be grounds for cancellation of a domain. For new and existing gTLDs there should be incentives for registrars to verify WHOIS data, since they verify the billing data. **FC:** The registrar has to take into account the purpose and quantity limitation when gathering data, then find a way to prove that the information is accurate by asking for proof of the information given such as a phone bill. **BC:** See responses to Questions 1, 2, 5 and 6. **CIRA:** ICANN can adopt measures to enforce compliance with accuracy requirements. In designing any measures, ICANN should consider the factors that lead to inaccurate and incomplete WHOIS data. Solutions can include registration validation; keeping in mind that the solution must be practical. Any validation program requires significant verification, maintenance, and a compliance system, duties which must considered in the design. In addition, registrants who provide false data should not benefit from privacy/proxy services.
11. <u>What lessons can be learned from approaches taken by ccTLDs to the accuracy of WHOIS</u>	**VH:** I am not aware of the approaches taken by ccTLDs. **SIDN:** SIDN is not subject to any obligation to provide any whois service on the .nl-domain at all. We do however provide such services, historically because everyone did it and currently because it is in the interest of our local internet community. Whois has been the subject

data?	of extensive discussions. Until 12 January 2010 SIDN offered a full and open whois, comparable to the gTLD's, but changed that after the last consultation with stakeholders to better protect the privacy of the users. Also in the Netherlands Whois discussions are always ongoing and what is there today might not be there tomorrow. A number of 'solutions' that we use are not exactly scalable to gTLD's. We use the fact that we are a country code TLD and for example only provide non-public whois details to Dutch law enforcement agencies and to Dutch based attorneys. We have never received any approval (nor disapproval) from the Dutch Privacy Authority with regard to our current Whois services. So do not automatically assume that what we do is completely in line with the Dutch and/or European privacy laws. **AFNIC:** In addition to the data publication and access policy, AFNIC has always been involved in enhancing whois data accuracy. Our current policy is summarized in Art. 16 of the .fr Charter. AFNIC conducts two types of accuracy checks. For companies and legal organisations, AFNIC checks public databases to ensure that data is accurate. These checks are performed no later than 30 days after registration. 10 to 20 000 checks of this kind are performed each month, with some automation. For private registrants, checks are performed on request and involve registrars checking accuracy. In 2010, AFNIC performed 386 checks of this kind. By virtue of French law, providing inaccurate data may lead to cancellation of the registration. This may only happen after the registry has offered the registrant a chance to correct the data. **INTA:** By placing a priority on contractual compliance, registries can improve the integrity of Whois data within their TLD. **IACC:** Some ccTLDs (e.g. CCNIC) have WHOIS data verification that may be appropriate to examine. Verification of registrant data combined with action to delete non-compliant domains should be considered as a compliance tool. ccTLDs for countries with domestic privacy laws have experience balancing data privacy restrictions with the need to provide accurate WHOIS data to law enforcement and civil litigants. Some ccTLDs have implemented thick WHOIS at the registry level, and may provide insight into whether such systems lead to more accurate WHOIS data. **TWI:** See answer under 3 above. **CNCERT:** With the development of the Internet, cybercrime causes losses to governments, enterprises and users. Registrants can be looked up in WHOIS, but the real users of malicious domains provide fake information to escape from investigation. In the long run, inaccuracy of WHOIS data is detrimental to the development of the Internet. The Review Team can benefit from worldwide experience and push ICANN to establish guidelines to increase WHOIS accuracy. China has strengthened verification of WHOIS authenticity and accuracy of .CN and it is very effective. Malicious domains and phishing sites have almost disappeared, although malicious users abandoning .CN domains continue to commit crimes through other TLDs. CNCERT/CC has processed domain abuse through regional platforms such as FIRST and APCERT, but the coverage of those organizations is limited. CNCERT/CC hopes that the Review Team can consider those methods in gTLDs. International coordination including most of the registries and registrars need to be established to handle domain name abuse more efficiently. **CNNIC:** In 2009 and 2010, CNNIC started to improve WHOIS accuracy by verifying registrants' data. By the end of 2010, WHOIS accuracy has reached 97% and domain name abuses plummeted to a negligible level. The most important lesson is that collaboration with registrars is key to improve WHOIS accuracy. The current policy is that registrars are asked to collect real WHOIS information from applicants, and failing to do so may imply de-accreditation. With the help of our registrars, the WHOIS accuracy of .cn has been fundamentally improved. **NOM:** ccTLDs are focused on serving the needs of specific jurisdictions, which allows them to tailor their approach to local circumstances. Privacy is an issue and ignoring it will increase the probability that data will be incorrect, even from those without malicious intent. In the case of.uk, Nominet has a contract with the registrant and can use this to require corrections. However, data may be incorrect due to misunderstandings, not updated when circumstances change or changes may not be passed on to our systems. We work on improving data quality by proactive checks and in response to complaints, and act quickly when malicious activity is suspected. This remains our priority.

	IPC: Accuracy of WHOIS data is also important for ccTLDs and many have undertaken WHOIS accuracy studies, such as Nominet and CIRA. As to actions to improve WHOIS accuracy, a prime example is CNNICs approach. In 2010 CNNIC sent out emails to the registrants of .CN requesting that they verify that their data was correct. Registrants could confirm details by clicking on a link in the email. Recipients had 15 days to respond and absent confirmation by the deadline, the domain ran the risk of being deleted. Some aspects of the CNNIC approach seem problematic, including the short deadline and the requirement to click on a link in an e-mail, a practice to avoid for security reasons, but placing the onus on registrants to confirm Whois data accuracy is worth pursuing. ICANN may consider requiring an e-mail to be sent to registrants to which they must reply, within a reasonable time limit, to confirm the accuracy of their Whois data. Alternatives might be to have registrars require users to log into their accounts and click on a box. Such an approach goes a step beyond the current WDRP and may be more effective in improving Whois accuracy. Also see answer to question 3 above. **PK:** How good are ccTLDs at enforcing their registrar's commitments? And what impact does that have on WHOIS accuracy? **HL:** Accuracy of WHOIS data is also important for ccTLDs and many have undertaken WHOIS accuracy studies, such as Nominet and CIRA. As to actions to improve WHOIS accuracy, the prime example is CNNICs approach. In 2010 CNNIC sent out emails to the registrants of .CN requesting that they verify that their data was correct. Registrants could confirm details by clicking on a link in the email. Recipients had 15 days to respond and absent confirmation by the deadline, the domain ran the risk of being deleted. This approach was criticized as CNNIC did not give any prior warning and registrants had no time to prepare. Owners of big domain name portfolios with many Chinese domains were concerned about responding for each by the deadline. However, ICANN may wish to consider 1) placing the onus on individual registrants ; 2) incorporating elements of this approach in a review of the WDRP, with notice and a longer deadline (circa 3 months); 3) requiring an e-mail to be sent to registrants to which they must reply, within a reasonable time limit, to confirm accuracy of their Whois data; 4) reviewing the various ccTLD WHOIS accuracy studies and approaches to consider whether any could be applied to gTLDs. **BC:** A ccTLD aspect to consider is whether accuracy is improved by a "thick" WHOIS data maintained at the registry level. **CIRA:** Addressing WHOIS accuracy and completeness requires much work. The longer it is left unaddressed, the worse the problem will become and the harder it will be to implement solutions as the volume of inaccurate WHOIS data will grow. WHOIS accuracy and completeness is important to CIRA as we have eligibility requirements (Canadian presence) for registrants. Revoking registration due to incorrect data is one method of ensuring accuracy and completeness.
12. <u>Are there barriers, cost or otherwise, to compliance with WHOIS policy?</u>	**VH:** Costs! Many hosting providers do not update WHOIS entries. **MN:** Validation of registrant data is costly. Registrars rely on the data received as provided in good faith. It may be possible to validate some input, such as an email address, but it is financially prohibitive to attempt to validate all registrant data. **INTA:** Aside from costs, there are no barriers to compliance with Whois policy. The costs of not maintaining accurate Whois far outweighs the cost of compliance and should be shared by registrants, registries and registrars alike. **TWI:** See answer under 6 above. **NCUC:** Even with the policy for resolving conflicts with national law in place, WHOIS poses problems for registrars in countries with differing data protection laws. Registrars do not want to wait for an enforcement action before resolving conflicts and many data protection authorities will not give opinions without a case. ICANN's response that there's no problem does not suit a multi-jurisdictional Internet. **CNNIC:** Verifying WHOIS data implies extra costs for registries and registrars. In addition, registrants, especially in .com and .net, are used to submit inaccurate WHOIS data, due to lack of obligation and verification. The cost of verifying WHOIS data and educating registrants are the biggest two obstacles to compliance with ICANN WHOIS policy.

	NOM: A main barrier is in the processes that link registrar and registry data systems. We work with registrars to improve these processes. **COA:** See answer under 6 above. **IPC:** The biggest barrier is failure to make WHOIS data a real priority. The costs incurred by registrars or registries to comply with Whois requirements are the costs of doing business in a responsible way that enhances consumer trust and meets public interest. If enforced even-handedly for all, any competitive impact of increased costs should be minimal. **PK:** ICANN's unwillingness to take action against registrars that don't take action with their non-compliant domain holders. **HL:** Cost-related barriers to compliance with WHOIS policy should not be a consideration for ICANN. Registrar and registry WHOIS compliance ise of prime importance. The task of auditing and policing registrars may be daunting, but ICANN must take it on to avoid a loss of faith in its ability to manage the situation and deal with new gTLDs. **FC:** Full and deep understanding of WHOIS Policy might be one. **BC:** A barrier to WHOIS compliance is lack of management attention to RAA enforcement. Lack of fact-based data on WHOIS and privacy/proxy registrations is a barrier to policy development, but studies underway should provide results. A significant barrier to improving WHOIS will arise if contracted parties block new policy development processes and contract amendments.
13. What are the consequences or impacts of non-compliance with WHOIS policy?	**VH:** WHOIS entries are no longer seen as a reliable source of information. **IHG:** Non-compliance with WHOIS policy reduces data reliability, burdens brand holders with protectionist activities, and detracts from user confidence in ICANN and the Internet. With the increase of new gTLDs, WHOIS compliance should be a priority and policies be developed to include accountability and enforcement measures prior to the award of any new gTLDs. **INTA:** Crime and fraud are key motivators for provision of inaccurate Whois data and use of privacy/proxy services. They are the logical outgrowth of non-compliance with Whois policy. **IACC:** Inaccurate WHOIS has a negative impact on stability of the Internet and on our members' ability to enforce IP rights. Experience with WHOIS since ICANN assumed custody has shown that unscrupulous Internet users are among the first to disregard their obligations to provide accurate WHOIS contact data. Online counterfeiting has been aided by ICANN's failure to administer the WHOIS system as stated in agreements including the AOC. Ineffective WHOIS compliance is not the only cause of online counterfeiting, but the extent is caused by the ease with which online pirates can disregard WHOIS by providing false data and, when found out, change to equally invalid contact data. **TWI:** See answer under 6 above. **NOM:** A domain can be suspended or cancelled if a registrant does not comply or does not correct data in response to a request. **COA:** See answer under 6 above. **IPC:** There are virtually no such consequences, since registrants, registrars or registries that do not comply face no penalties. The result will be increased complaints from consumers and rights holders, pressure for national legislation and an erosion of consumer trust. With unlimited gTLDs, consumer safety and fraud issues will increase when unethical registrants continue to escape enforcement. Inaccurate WHOIS data contributes to public mistrust and instability. When ICANN's approach to its AOC WHOIS commitments is judged insufficient, governments may legislate for WHOIS compliance based on concerns expressed in the GAC Principles. WHOIS compliance should have top priority and ICANN needs policies with accountability and enforcement measures prior to signing new gTLD contracts. **PK:** It makes it difficult or impossible to contact owners of compromised servers with phishing sites. The same difficulty exists when trying to contact people whose servers are used for spam. Many are frustrated by the lack of consistent and accurate WHOIS data. **HL:** There are far reaching consequences of registrar and registry non-compliance with WHOIS policy. As outlined in the GAC Principles,

	WHOIS services are used to assist LEAs, to assist trade mark and copyright enforcement and to combat fraud. Reliable and accurate WHOIS data contributes to end user confidence, encourages use and promotes good faith interactions. If WHOIS cannot be relied upon, the Internet may become the wild west where criminals and fraudsters can operate with impunity. Such a situation would be a huge loss of faith for the end users and is unacceptable for the whole community. ICANN must invest substantial resources in compliance. **FC:** Consumer trust in ICANN or the Internet decreases, impacting ICANN credibility and organizational strength negatively. **BC:** Noncompliance with WHOIS policy has a deleterious effect on ICANN’s mission and its ability to meet its AoC commitments. Inaccurate and false WHOIS negatively impacts the Internet’s security and stability, impairs the ability of consumers to understand the source of legitimate products/services, facilitates fraud, impairs law and IP enforcement investigations, and harms e-commerce. Problems with WHOIS combined with non-compliance lead to loss of confidence after the introduction of new gTLDs. A full review of the WHOIS system should be made and prompt implementation of recommendations from that review, preferably before the rollout of any new gTLDs.
14. Are there any other relevant issues that the review team should be aware of? Please provide details.	**VH:** Some providers don't update WHOIS. The community should be involved in developing the WHOIS service and protocol. **IHG:** The business community shield their brands and customers from cybersquatters' operations through defensive registrations in the thousands. In capital constriction times, these portfolios become cumbersome and detract from funds to engage cybersquatters via the dispute resolution process. Attempts to scale back defensive registrations are met by increased cybersquatting. The problems associated with inaccurate WHOIS data is a greater problem today than at any time in the past. **INTA:** The Committee has not identified additional issues for the review team at this time. **NCUC:** Permit a registrant to get a domain showing no WHOIS information at all, with the risk that the domain will cease to resolve if the domain is challenged and the registrant is unresponsive. This is the de facto situation for domains registered with false data, so make it an official option. Proposals for verification of information are unworkable for standard gTLDs, but might be launched by registries trying to differentiate. There is no standard of physical addressing that holds across geographies and cultures. Inaccurate WHOIS data should not be used as evidence of bad faith, especially in the context of ICANN's policies such as the UDRP. Within the UDRP, the need to identify a registrant is vital, but WHOIS details should not be used to make determinations concerning abusive registrations of domain names. **CW:** Who does “the public” refer to? Few members of the general public are interested in registration records, which is quite understandable. The interested parties are law enforcement and the IP community. It would be preferable to be specific and seek legally safe and workable solutions to their legitimate needs, which are not necessarily the same. In view of the large number of registrations said to be inaccurate, domains engaged in fraud would tend to be among them. **NOM:** There is a trust issue associated with inaccurate contact data, in particular for domains used for trade. This creates a question of trust for the TLD in relation to law enforcement, regulatory and other public authorities. This could impact consumer confidence, but very few users are aware of WHOIS. The EU's e-Commerce Directive has requirements for trading websites to include contact information so that third parties know who they are dealing with. For the consumer, this information is more accessible than WHOIS. Nominet has a one-stop shop portal for information and links and contributes to awareness initiatives as WHOIS data can be abused to assist fraud and spam. **COA:** The gTLD Whois database is a vital public resource and ICANN’s stewardship of it has been ineffective. The proliferation of proxy registration services has contributed to Whois data inaccuracy. Reform is needed, beginning with ICANN enforcement of standards for proxy services. Registries and registrars must assume responsibility for accurate Whois data, through adoption of thick Whois models for all gTLDs; data accuracy obligations that flow from registries to registrars; and verification of registrant data. ICANN’s compliance activities need more resources and a proactive reorientation. The AoC spells out the task of the Review Team, but another way is to evaluate how

	effective ICANN has been as steward of the Whois database. Whois is crucial for accountability and transparency on the Internet. When ICANN was established, the gTLD Whois was unified, accessible 24/7 and fully searchable, but had problems of inaccuracy. After a dozen years of ICANN stewardship, Whois is fragmented, has limited searchability and remains seriously inaccurate. A new source of inaccuracy flows from the proxy registration services with some 20 million domain names. On ICANN's watch, the value of the Whois database to the public and its role in promoting consumer trust has degraded and its stewardship has been ineffective. Reversing this degradation of Whois is the challenge ICANN must confront. This long-term view is useful for evaluating the questions the Review Team is tasked to address and in preparing recommendations for improvements. **PK:** Just fix the current system. The Review Team should describe the intentions for WHOIS and spell out why the RAA requires WHOIS data to be complete and accurate. The longer ICANN takes to address compliance, the more effort and resources will be needed to achieve it. **HL:** The issue of WHOIS is of prime importance and should be addressed by ICANN compliance. With new gTLDs, these issues need to be considered now and resources allocated to ensure a response to the Whois problems that face the community now and in the future.
Other comments	**LE:** WHOIS contact info is supposed to work for technical problems with a domain and this is typically not the case for e-mail addresses. ICANN should educate the public about WHOIS using the "annual reminders". RFC 3912 failed to cover the administrative parts in RFC 954, and failed to follow the IETF i18n policy in BCP 18 (RFC 2277). The i18n issue can be fixed, but RFC 5198 was published after RFC 3912. RFC 5198 explains how to replace US-ASCII by UTF-8 in protocols such as WHOIS. RFC 1032 covers the lost administrative parts in RFC 954, but it is not state of the art and needs updating. Even an experimental RFC would have more impact on the community than any ICANN PDF. **SL:** The Whois discussion is a phantom-discussion as most administrators are happy with it as is. Phone and fax number should stay optional, while name and postal address are necessary. For a company, a named person is still necessary as well as an email address. Persons who put false data in whois for a domain should lose the right to the domain. **VH:** WHOIS has always been important for data about domains and their registrars but customers don't understand why personal data is published, while others may use proxy services or provide false data on purpose. It is difficult to find reasons why WHOIS still has to contain personal data. Remove personal data from WHOIS but keep WHOIS alive by making it more important for technical questions. **MM:** The following paper with a historical overview of the evolution of Whois could be helpful to the Review Team's work: http://forum.icann.org/lists/whoisrt-discussion-paper/pdfDB3W7kd4BR.pdf **MN:** The RAA provisions are problematic, as they demand registrars to make public whois available, offer bulk whois access to anyone and protect registrants from unsolicited marketing. Those requirements are conflicting and at odds with EU privacy law. There is a process to handle that but it's unclear if it has been used: http://www.icann.org/en/processes/icann-procedure-17jan08.htm **EL:** All gTLD registrars must support WHOIS and have links to their WHOIS servers. Owners of domain names must be kept accountable for their actions. Even though an email address may be obfuscated, there must be some way to contact the registrant. **BS:** Whois is fine for businesses but a problem for personal websites. An individual's alternatives are to release personal information, make whois data private, insert false whois data or pay for a PO box and put that in as whois address detail. None of these choices are ideal. A solution is needed that doesn't involve sacrificing privacy. Give the option to hide the physical address for individuals. The provider should have full access to address info at all times but the public should not. **AFNIC:** AFNIC welcomes the opportunity to provide insights from our experience as ccTLD manager for .FR to questions 3 and 11 of the Discussion Paper. We stress that the framework stems from the French legal environment with legal and regulatory measures enforced by the electronic communications Act, instructions for the French privacy authority CNIL and registry policies, developed in a multistakeholder

	process, as well as AFNIC’s commitments towards the French Government. **IHG:** WHOIS helps combat malicious exploitation of trademarks by those who intentionally register domain names that are confusingly similar to those of well-known brands. Cybersquatting continues to evolve, while the means to combat it remain static. Open access to accurate WHOIS data must be reinforced to develop additional brand protection measures as well as promote trust. Inaccurate WHOIS data impedes dispute resolution and compromises the integrity of the registration infrastructure as well as trust in the Internet. **INTA:** Trademarks are a primary means for consumers to make informed choices of products and services. **IACC:** The IACC supports the review of ICANN’s compliance with its WHOIS obligations, and trusts the review can increase transparency and stability of the Internet. **TWI:** Whois data is the foundation for most Internet-related investigations and transactions and we rely upon access to this data for starting investigations of rights infringements. We also use it for routine tasks in managing domain portfolios and for domain transactions. Access is also essential to LEAs, consumer protection organizations and users who need to know whom they are dealing with. This data has to be accurate, complete, up-to-date and readily accessible as a crucial Internet resource. The Review Team’s role is to evaluate the quality of ICANN’s stewardship of this resource and recommend how to improve it. This is the most critical of the reviews mandated by the AoC. **NCUC:** The NCUC is concerned about the lack of adequate privacy protection in WHOIS and believes ICANN can offer better options for registrants and the Internet-using public, consistent with its commitments. **CW:** While commending the Review Team for assisting ICANN to address the Whois issues, it should be noted that these issues have been addressed repeatedly during the past decade, without resolution. The issues remain important, but it is not clear what new elements have emerged since the AoC to create expectations of a successful outcome on this occasion. **MPAA:** Our comments respond to some of the questions posed by the Review Team, based on our experience in combating copyright infringements carried out through the use of domain names. **CNCERT:** CNCERT collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for exchange of information and coordination of actions with International Security Organizations. **CNNIC:** CNNIC offers WHOIS services through a web-based interface implementing RFC3912. By the end of 2010, the WHOIS accuracy of .cn had reached 97% and spam emails sent from .cn URLs had fallen to less than 5% from 15% in 2009. Reported phishing websites under .cn had been reduced from 86.5% to less than 0.6%. All registrants in .cn are required to provide real WHOIS data, and CNNIC is responsible for verifying the data. Registrars are required to verify applicants’ WHOIS data, and WHOIS accuracy is used to evaluate registrar performance. **NOM:** Nominet has developed its WHOIS policy and implementation in consultation with stakeholders. Our contribution provides data about the UK environment in response to the request for ccTLD input. We have not responded to questions on the gTLD WHOIS policy. **COA:** COA has been active in a range of ICANN policy development activities, on its own account and as a member of the IPC. Whois policy has been a focus of the ICANN activities of COA and of its predecessor, the Copyright Coalition on Domain Names (CCDN). **IPC:** Our comments are keyed to the questions posed in the Discussion Paper. **PK:** My company has implemented various protocols and networking products over the years and is active in fighting spam and phishing. WHOIS is essential for contacting actors to report hacking or abuse. Those offering privacy services to registrants should only do so if they also take on the responsibility themselves. **HL:** Hogan Lovells is acting for numerous brand owners and Internet players. **BC:** The Business Constituency (“BC”) has long supported the need for greater WHOIS accuracy and access to ensure the protection and

	safety of Internet users and to enable brand owners to protect their intellectual property. We support the goals of the WHOIS Review Team to assess the extent to which gTLD WHOIS policy in the space is effective, meets the needs of law enforcement and promotes consumer trust, and its additional assessment of ICANN's performance in this area. **PK(2):** I'm surprised that people put their remarks into PDF and DOC (and DOCX) attachments rather than in the mail, expecting everyone to use external software to review comments. PDFs are universal, but people should not be forced to have Word or some other reader. **CIRA:** CIRA maintains its own WHOIS service and can offer some insight into practices that encourage accuracy and completeness of WHOIS data. CIRA's WHOIS permits queries to the .CA Registry database to determine the availability of .CA domain names or to view the administrative contact and technical data provided by registrants. Data about individual registrants is not publicly displayed in the WHOIS. Information of corporations is displayed by default. In order to contact a registrant whose information is not displayed in the WHOIS, an online Message Delivery form is used. The message is forwarded to the registrant's Administrative Contact email. For specific disputes that a user has not been able to resolve, CIRA may disclose contact information of registrants that is not publicly available, via a Request for Disclosure of Registrant Information. CIRA may provide personal information in response to a search warrant or as otherwise required by applicable law. For Canadian law enforcement agencies and the conduct of certain investigations, CIRA may also disclose contact information of registrants via a Request for Disclosure of Registrant Information for Law Enforcement. **ALAC:** The ALAC welcomes the Discussion Paper but would have liked to see additional papers identifying the problems regarding the current WHOIS definition, utilization and compliance. We endorse the community-specific conversations hosted by the Review Team in Singapore, where ALAC members participated. The most important objective for the Team is to give a perspective and/or recommend a set of policy initiatives or refinements to existing policy that balance the competing interests in the WHOIS ecosystem. The Team should be in a position to identify and define all of the problems regarding WHOIS, prioritize their impact on consumer trust and confidence in the DNS and make an unambiguous recommendation as to need and focus of correctional policy work. While we have concerns about whether the consumer-focused study authorized by Board funding will add any new information, the ALAC supports collection of as complete information as possible on this issue. The Review Team must pronounce its decisions unambiguously, declaring (1) whether WHOIS as originally devised and for the purpose intended is still necessary, (2) whether the WHOIS dataset as originally determined remains fit to its original purpose, and (3) whether the several uses made of both the WHOIS data and processes that have expanded the original intent are useful and in the public interest. We expect recommendations \ as to whether these additional uses of WHOIS are within the terms and intent of the RAA, are to be embraced by the global community and are within the remit of ICANN Compliance. Answers to these questions will allow interpretations as to (1) whether the present WHOIS dataset is good and sufficient to meet these needs and others that might be contemplated, (2) whether the current processes used for WHOIS data compliance are fit for the purpose. The Team may be able to acknowledge the instance of Privacy/Proxy Services and the role they play in the WHOIS ecosystem and recommend a workable solution that acknowledges privacy concerns, including ways that these may be met in a balanced way.

Appendix F:

Discussions with and Feedback from the Country Code Domain Names (ccTLDs)

The WHOIS Review Team has collated the various comments relating to and submissions made by ccTLDs. These comprise verbal and written comments.

Summary

National laws may prohibit mandatory contact data in public WHOIS but not voluntary data. Registrars selling domains in these ccTLDs can communicate why not publishing voluntary data will result in no trust for, e.g., anti-spam applications.

Most ccTLDs provide the entire WHOIS record at the registry level, while some provide the entire record only to certain groups such as law enforcement agencies, certification authorities, and registrars that need access for administrative purposes. The extent of information that is shared is generally determined by local law. DENIC publishes all contact information, and German law requires the contact information to be placed on the website if engaged in business. France has a similar requirement. Where there is a need to balance local privacy laws with access to full WHOIS, mechanisms to improve transparency can be considered, as in the Netherlands.

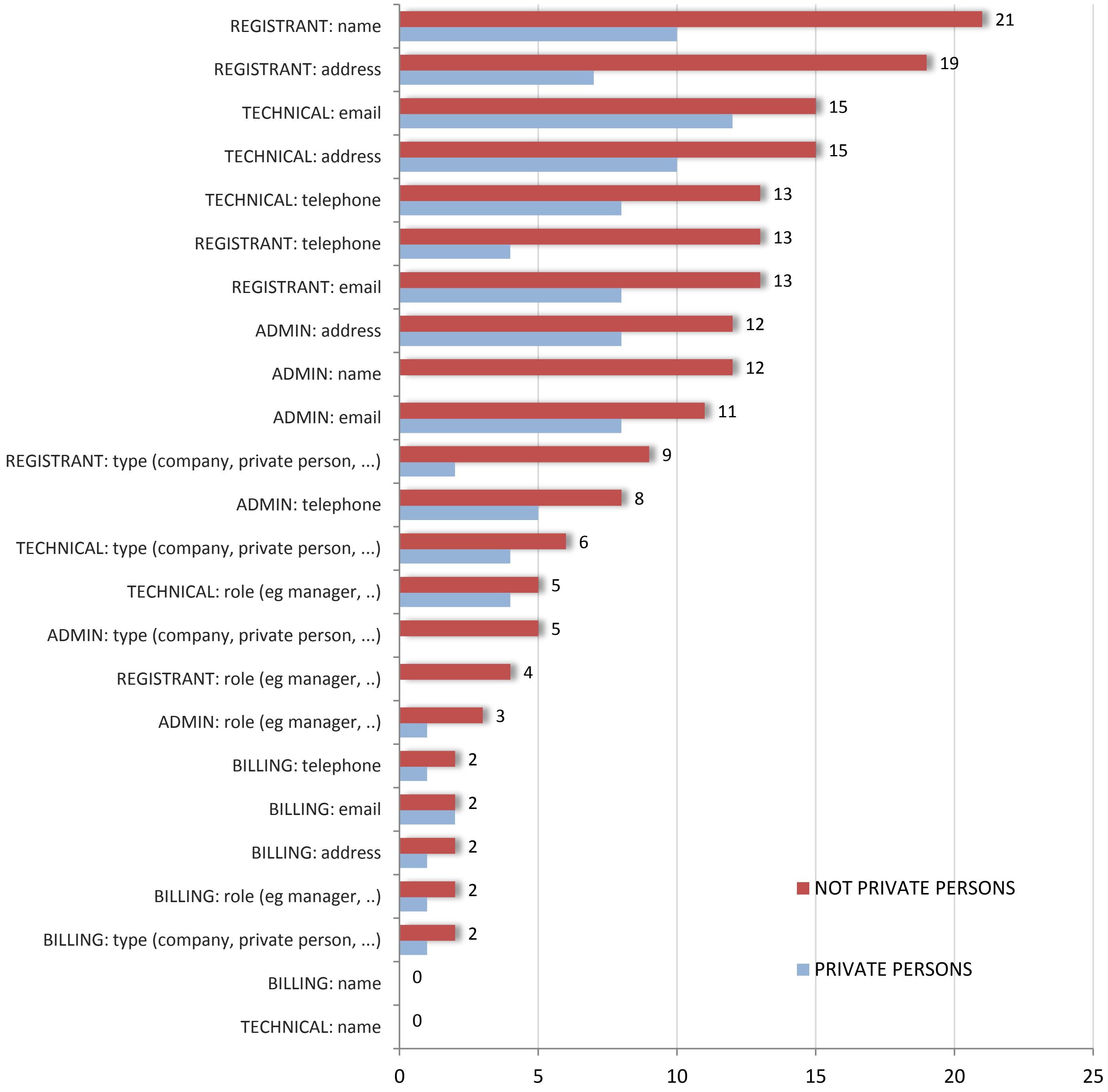
Many European ccTLDs offer a public WHOIS service with limited non-technical information, while law enforcement can access full details. A distinction is made between personal and business domain registrations, for example in .IE. In both cases no personal data is available in WHOIS. In .CO.UK, the WHOIS output shows if a registrant has "opted out", but a company would not have that option. While a business domain does have more data published in WHOIS there is no email address or phone number. Under .EU, WHOIS is limited to technical details and shows more information about a business domain, while a personal one's output is limited to an image of the email address, not accessible to bots. The only gTLD that has followed a similar model is .TEL, where registrants can opt out in a way similar to .CO.UK and the WHOIS output is minimal, while a business registration is more detailed. See submission for multiple and detailed examples.

ccTLDs are in a very different situation because they’re normally within a single jurisdiction actually and they have a much more direct relationship and they have clear, applicable law; whereas, if I understand correctly, we’re talking about gTLDs here and their global operators and it’s the old conundrum actually and therefore internet governance people about how you try and deal with global operators acting across a number of different jurisdictions, potentially conflicting applicable law. The situations are very different, the challenges are very different for developing WHOIS policy at the national level for ccTLD, compared to a body like ICANN trying to develop WHOIS policies at the global level effectively.

CENTR Report on WHOIS & Data Protection

CENTR Data from Member Survey:
WHOIS and Data Protection (January 2011)

DATA that cannot be hidden in the WHOIS in relation to private and non-private persons



Comments in relation to how holders can request to hide information in the Whois as well as some comments on proxy registrations

Non-individual Registrants (e.g. corporations, partnerships, etc.) may only get WHOIS Privacy in exceptional circumstances. In order to qualify for WHOIS privacy protection as a non-individual Registrant, they must meet both of the following criteria: 1. The nature of their operations (or activities) makes them have a greater need to protect your personal information than other non-individual Registrants; and 2. Making their personal information available on the WHOIS would likely cause harm to individuals or to the Registrant. For Question 4, certain Registrars offer privacy services, whereby their contact information will be listed in the WHOIS, although the name of the Registrant (for non-individual Registrants) will be listed in the Registrant field.

The contact (with unique id handle) can have the role of the domain holder, admin-c, tech-c etc and only this contact decides, if will hide some data or not. Generally, only "name" (filling the column "organisation" is not obligatory) and "address" must be filled. The contact may tick the data as hidden during the registration process or after through the registrar - it depends on the system of each registrar.

Not possible to hide information in the WHOIS. In very limited circumstances alternative information may be permitted. This requires the registrant to work with the registrar and the Domain Name Commission to work through the particular situation.

Contact data for a name: registrant and technical By default, no data is visible for a private person, all data are visible for a company/organisation. The whois provides facility to send an email to a private person, without showing his email address.

We do not have administrative contact or billing contact. For private registrants only email address and First name letters are shown. For legal person registrant all registrant data is shown. We treat that technical contact cannot be private, as he is doing public service in administering domain name, so all contact data is always shown.

(1) The holder cannot request to hide any information. Billing information is not presented in WHOIS as a Registry policy, not by anyone's request. (2) If there is a proxy arrangement, it is external to the registry, i.e., the holder is the entity registered as such in the registry.

3. Private individuals can choose to hide their address provided the website is not being used for commercial purposes. This can be done at any time through online systems. Note that our WHOIS only displays name, type and address at most for any registrant. 4. We do not prohibit the use of proxy services, and they are offered to registrants from time to time, but most proxy services find it too problematic and do not last - for example, because of being named as the respondent in DRS complaints.

How the holder can request to hide: It depends, if the domain name is registered through the website, then e-mail, telephone and fax is automatically hidden and it must be ticked a check box to unhide the data. If the domain name is registered per EPP-command, then it is the other way round. But this has only technical reasons.

Please note that the Registry shows different information in the public web whois, public command line whois, the registrar whois, the whois for Certification Authorities and the whois for investigative agencies.

Registrant is identified by the fields "name" and "organisation". If only "name" field is filled in, we consider the registration to be private and do not publish personale data other than e-mail address. If "organisation" field is also filled in, we consider this to be a corporate registration and publish full whois details.

By default all registrant data must be made public, unless the registrant can verify that he/she is "hidden" in the National public personal register

Holder can hide all data by paying additional fee.

There's no option to hide selected data, the WHOIS rules say: 3.1. If the Domain name holder is an organisation, the following data shall be published via the WHOIS search service: 3.1.1. official name and head office of the Domain name holder, and telephone/fax number; 3.1.2. valid electronic mail address for the Domain name holder (contact electronic address); 3.1.3. valid electronic mail address for the technical contact person; 3.1.4. data on the Registrar; 3.1.5. data on the DNS server; 3.1.6. date of registration of the Domain name and status of the Domain name; 3.1.7. date of expiry of the Period. 3.2. If the Domain name holder is a natural person, the following data shall be published via the WHOIS search service: 3.2.1. valid electronic mail address of the Domain name holder (contact electronic address); 3.2.2. valid electronic mail address of the technical contact person; 3.2.3. data on the Registrar; 3.2.4. data on the DNS server; 3.2.5. date of registration of the Domain name and status of the Domain name; 3.2.6. date of expiry of the Period. 4.

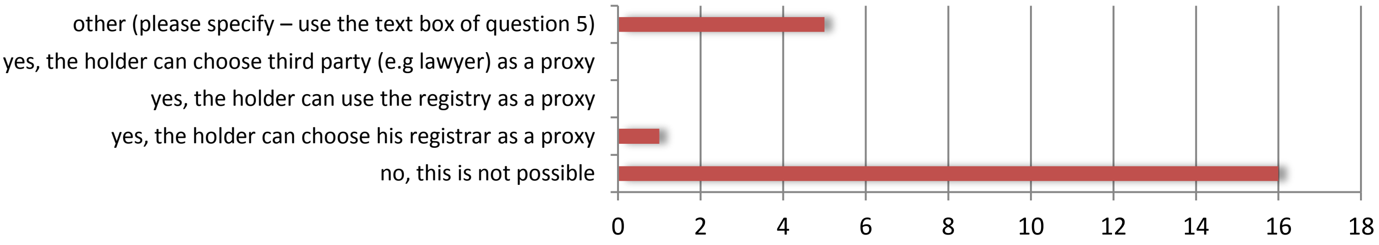
For optional data we provide a disclose mechanism via our registry/registrar interface

A private person data is hidden as a standard option. Such a person may request opt-in to make his data visible. As an admin we understand above a registrar.

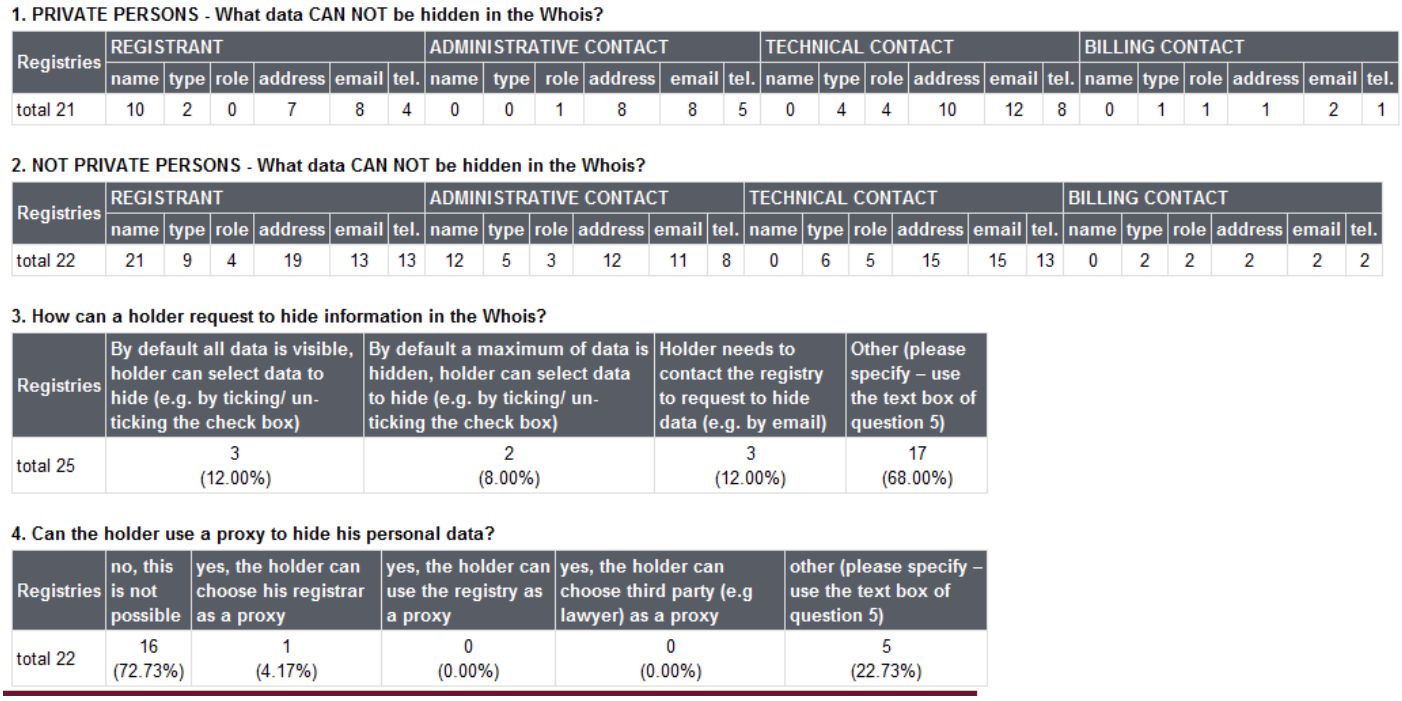
In our Country it is defined by law what data MUST be published by the registry (which operates the central WHOIS service for .ch). The Registry publishes exactly this data set. We would break this law if we publish less, and we would break the data protection law if we publish more than the defined fields.

The Registry does not explicitly allow nor disallow the use of proxies. All registrants need to agree to have read and agree to abide by the Terms and Conditions, and all other applicable documents. Please note that the billing-c and tech-c are registrar-specific contacts at the Registry. The registrant only provides us with the registrant-info, and potentially an onsite-contact (tech-c provided by the registrant).

Can the holder use a proxy to hide his personal data?



Raw number from the survey



1. PRIVATE PERSONS - What data CAN NOT be hidden in the Whois?

Registries	REGISTRANT						ADMINISTRATIVE CONTACT						TECHNICAL CONTACT						BILLING CONTACT					
	name	type	role	address	email	tel.	name	type	role	address	email	tel.	name	type	role	address	email	tel.	name	type	role	address	email	tel.
total 21	10	2	0	7	8	4	0	0	1	8	8	5	0	4	4	10	12	8	0	1	1	1	2	1

2. NOT PRIVATE PERSONS - What data CAN NOT be hidden in the Whois?

Registries	REGISTRANT						ADMINISTRATIVE CONTACT						TECHNICAL CONTACT						BILLING CONTACT					
	name	type	role	address	email	tel.	name	type	role	address	email	tel.	name	type	role	address	email	tel.	name	type	role	address	email	tel.
total 22	21	9	4	19	13	13	12	5	3	12	11	8	0	6	5	15	15	13	0	2	2	2	2	2

3. How can a holder request to hide information in the Whois?

Registries	By default all data is visible, holder can select data to hide (e.g. by ticking/ un-ticking the check box)	By default a maximum of data is hidden, holder can select data to hide (e.g. by ticking/ un-ticking the check box)	Holder needs to contact the registry to request to hide data (e.g. by email)	Other (please specify – use the text box of question 5)
total 25	3 (12.00%)	2 (8.00%)	3 (12.00%)	17 (68.00%)

4. Can the holder use a proxy to hide his personal data?

Registries	no, this is not possible	yes, the holder can choose his registrar as a proxy	yes, the holder can use the registry as a proxy	yes, the holder can choose third party (e.g lawyer) as a proxy	other (please specify – use the text box of question 5)
total 22	16 (72.73%)	1 (4.17%)	0 (0.00%)	0 (0.00%)	5 (22.73%)

CENTR Survey Summary on Registration Data Access & Dispute Resolution

The Council of European National Top Level Domain Registries

Belliardstraat 20, 6th floor
Brussels, Belgium
+32 2 627 5550
secretariat@centr.org
www.centr.org

CENTR Survey

‘Registration Data Access and Dispute Resolution’

This is a summary report of the above survey.

Full raw data can be found here: (only available to those who took the survey)

Report Details
The survey focused on two main areas: access to normally non-published Whois data; and secondly on dispute resolution process and services offered by the ccTLD respondents.

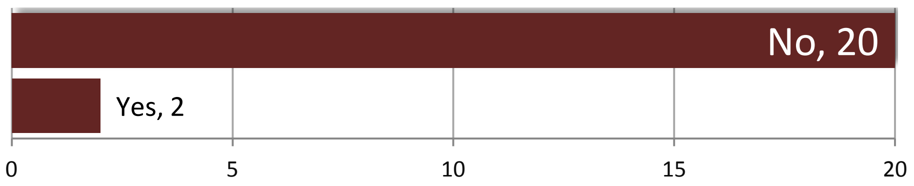
Initiated by: .EURid
Survey timing: 21 September 2011 – 3 November 2011

Respondents (22): .at, .be, .ca, .ch, .de, .es, .ie, .il, .is, .lt, .lu, .lv, .me, .mx, .nl, .no, .pl, .pt, .ro, .rs, .ru, .uk

Does the ccTLD offer enhanced search tools for those seeking to protect their brand online

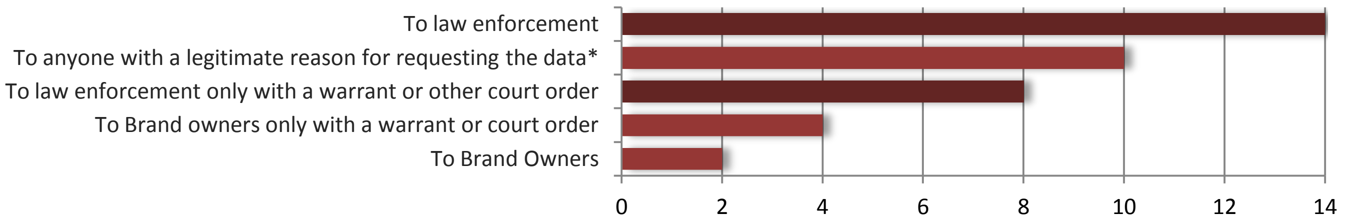
By far, the majority (90%) of responding ccTLDs stated they do not offer any enhanced search tools for those wishing to protect their brand online.

One ccTLD noted that they offer a subscription based service (with a fee) allowing users to search the Register by Registrant. For more information see question 2 in the survey raw data



In what circumstances will the Registry release non-published registrant data (eg opted out from WHOIS or otherwise not published)?

The below represents the number of ccTLD's whom give non-published WHOIS data to different requests and circumstances. 14 out of the 22 ccTLD's (64%) noted they would provide data to Law Enforcement and a further 8 stated they provide information to law enforcement only with a warrant or court order.



*****On the question 'to anyone with a legitimate reason' as well as another category, 'other' (not shown), the followed remarks were received:

We will give non-published data to anyone who has a legitimate interest and explains this interest to us.
Our public whois does not show any physical address details. We provide these details to: a. law enforcement with a legitimate order; b. to law enforcement on a contractual basis (to be used only in cases in which they are in the position to force us to provide this information); c. to attorneys and bailiffs if they need this information to start a civil court case for their clients; d. to Certification Authorities on a contractual basis in order to verify if their clients are as they claim to be the registrants of the domains they request SSL-services for
We will give non-published data to anyone who has a legitimate interest and explains this interest to us.
By registrant request. The registrant can opted out from whois
We disclose personal data in cases provided for by law to officials of State and local government institutions. Personal data may be disclosed on the basis of a written application or agreement, stating the purpose for using the data, if not prescribed otherwise by law. The application for personal data shall set out information as will allow identification of the applicant for the data and the data subject, as well as the amount of the personal data requested.
We will give non-published data to anyone who has a legitimate interest and explains this interest to us.
To other entities that have a relevant paragraph in law that allows them to request such data. E.g. the tax office may during certain audits have the right to request historical information about a domain name.
To lawyers provided they fill in the 'disclosure" document that is available on our website and return it to the Registry
To WIPO or a solicitor for dispute cases.

Domain Registration

100% of respondents stated they allow ‘individuals to register domain names. Below is some remarks based on question 7 which asked if there are any restrictions on what domain names can be registered.

Domain names that coincide with personal names and/or family names should only be registered by persons having direct relation to those names. There are reserved names (public organizations, countries, regions, municipalities) as well as a black list (terms related to Internet, TLDs). Our DRP provides some additional protection for holders of trademarks, company names, names of official organizations, celebrities...

Only registrant names or Trademarks can be registered.

Domain name shall be chosen in such a way not to infringe the legitimate rights of other parties and not to violate the existing legislation of the Republic of Latvia; - Domain names containing rude, indecent or offensive names, expressions, or character strings shall not be registered; - Full name of an individual as a domain name may be registered only by the person with the respective full name. Between the persons with identical full names the preference shall be given to the person who submitted the application first.

The domain name should not include words which contradict public interests, the principles of humanity or morality (in particular, words of obscene content, slogans of antihuman character, which insult human dignity or religious sentiments, etc).

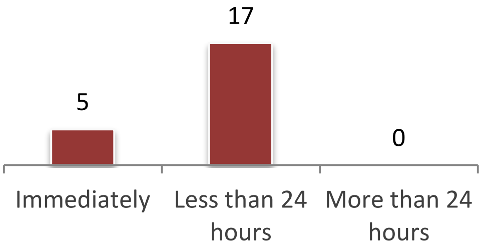
Special permission is needed for usage in domain name of the country name. Domain name should not contravene public order and first of all good morality standards. The names should not contain any labels apparently denigrating honour and dignity (business reputation) of persons or hurting different social or occupational groups.

Restrictions relating to the registration of communal names - these domains can only registered by the communes (proof is necessary)

We do not place restrictions on what domain names can be registered, though registrations are subject to the registrant submitting to the Dispute Resolution Service. This provides a route for someone with rights in a name to dispute a registration if they can establish that the registration is abusive.

How long after registration is the domain ready to go live

In most cases (17/22) the domain can go live less than 24 hours after the domain has been registered. There are no cases where it takes more than 24 hours.

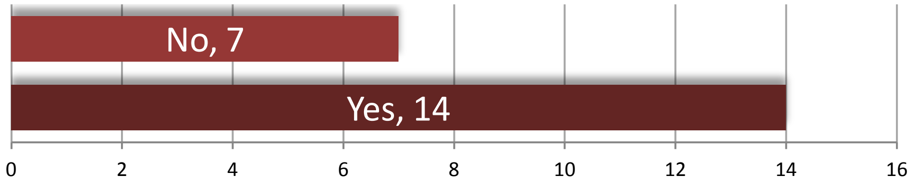


Does the Registry take any active steps to support sustainable development

A smaller number of the respondents answered this question (13) however it most cases the answer was no.

DISPUTE RESOLUTION

Does the Registry offer a dispute resolution process for resolving conflicts with Trademarks and other intellectual property?



Further comment on what the responding Registries provide:

A DRP, based on UDRP, but with some differences (see below)

Local UDRP variant with a broader scope (incl. Trade names, names of public institutions and (well known) personal names and a mediation process incorporated

In the case of disputes concerning domain names, trademarks or company names the registrants of these can agree to turn to institutionalised voluntary arbitration and there is a Arbitration Center for this kind of disputes. www.arbitrare.pt

A Local Dispute Resolution Policy (An UDRP based) since year 2000

When registering and administering domain names, the Registry is not obliged to check whether the holder is entitled to the domain. Instead, it is up to the holder to make sure, prior to registration, that he/she is not violating any distinctive sign rights of third parties. The Registry provides a non-exhaustive list of directories to this end. In the event of disputes concerning a domain name, the Registry is a party to neither the civil action nor the dispute resolution proceedings. This also applies when it is solely a matter of ensuring that judgements or rulings are enforced. Means of recourse for the third party If a third party raises a claim against the domain name holder, this is a matter for the former and the latter which is to be settled through civil action or through these dispute resolution proceedings. The present dispute resolution proceedings are mandatory for domain name holders who register a new domain name as of 1 March 2004, for domain name holders who renew their subscription after 1 March 2004 and for domain name holders who submitted by participating in the proceedings. They are designed as simple, rapid and inexpensive proceedings.

Three arbitration providers (two local and WIPO). Real arbitration, final decision must be confirmed by a state court.

DRP is through WIPO and we adhere to their decision.

The below is a selection of comments regarding the fees payable for dispute resolution as well as their timing and who the fees are payable by.

1.400 €, paid by the plaintiff when starting the procedure

1-5 domains € 500 admin + 1.000 panellist fee 6-10 domains € 700 admin + 1.300 panellist fee mediation is free of charges all amounts to be paid by complainant before the panellist is appointed

Fee paid by the plaintiff when starting the procedure 800EUR physical persons, up to 2 domains in dispute; 1800EUR legal persons , up to 5 domains in dispute 2150EUR legal persons , 5 to ten domain in dispute

75 to 150 EUR.

750 euro paid by the plaintiff -- half refundable if case is not accepted by the Appeals Board.

1-5 domains 500 USD admin + 1.000 USD panellist

440 EUR payable by complainant. In recent years the registry has tested a procedure where fee is refunded if complainant wins. We are now considering developing this to require the domain name holder to pay if he loses.

The conciliation attempt costs CHF 600. The expert's decision costs CHF 2000. But none of this money goes to Registry.

~750 euro (one arbitrator), pays a claimant after arbitration clause is signed;

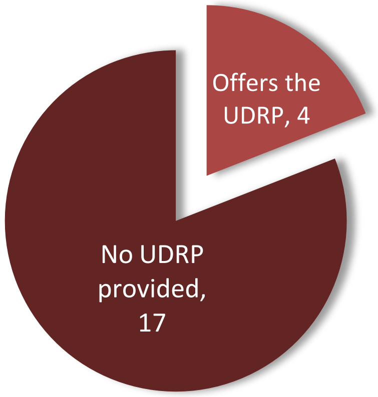
No fee

1.620 EUR to pe-paid by complainant before start of proceedings. Fully reimbursed if complainant wins the case.

It cost $4000 CDN for a 3 member panel. The entire fee is paid by the Complainant. If the Registrant does not file a response, the Complainant can elect for a 1 member panel, at a cost of $1750 CDN.

There is a minimum charge of 1,500 for WIPO paid to WIPO. We do not charge.

Does the Registry provide the UDRP



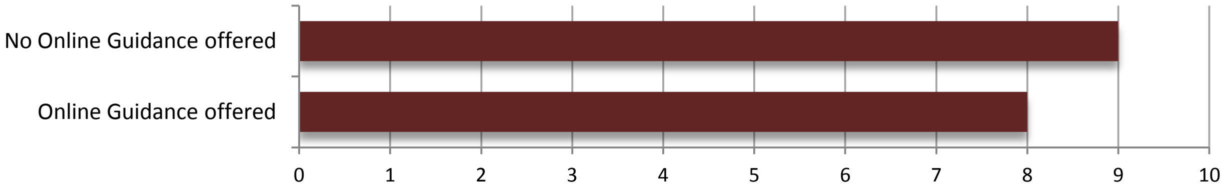
Around 81% of respondents to this question do not provide the UDRP

How the Registry Service differs from the UDRP

The Registry DRP does not only protect trademark holders, but also other groups (celebrities, owners of company names, etc.). The DRP does not require that the domain name must have been registered and used in bad faith - the rules say "registered or used". There are minor procedural differences. The dispute resolution providers are not the same
The conditions for an eligible DRP are different.
Broader scope in protected rights but rights should be valid in the country
In UDRP only Trademarks owner can use it, in our case, any right is supported, like company name, patent, etc.
Scope is narrower than the UDRP scope
Broader intellectual property rights may be used, not only Trademarks and some local considerations.
Broader scope in rights protected, but the rights have to be valid in the country. Specifically fit to National legal processes, local language used. Can complain about a domain being registered _or_ used in bad faith.
Based on local law instead of bad / good faith examination.
Dispute resolution process is handled by WIPO
Only small differences: - larger category of protected rights e.g. family name - one of criteria is bad faith during registration OR usage (is AND for UDRP)

Is guidance offered for the Registry's dispute system

Below shows how often online guidance is provided among the respondents. Further in the survey it was noted that no respondent undertakes regular structured feedback in relation to their dispute resolution service.



Please see question 18 of the raw data to see further details on cases when online guidance is provided

Submissions from ccTLD Registries

a) The Netherlands (.nl)

As submitted by SIDN[1]:
“As a ccTLD manager based in Europe SIDN is not subject to any obligation to provide any whois services on the .nl-domain at all. We do however still provide such services. Historically probably just because everyone did it and currently because it is in the interest of our local internet community.The whois, what information we show and how you may obtain the information therein has been subject to extensive discussion with and within our local internet community. Until 12 January 2010 SIDN offered a full and open whois service, comparable to the gTLD's, but changed that after the last consultation with our stakeholders to our current form in order to better protect the privacy of the users. In order to help the working group in their difficult (not to say impossible) task, I will try to give a short description of our current services underneath. Be aware however that also in the Netherlands discussions with regard to the whois are always ongoing and what is today might not be there anymore tomorrow. Secondly please note that a number of 'solutions' that we currently use are not exactly scalable to gTLD's. We make use of the fact that we are a country code TLD and for example only provide non-public whois details to Dutch law enforcement agencies and to Dutch based attorneys. Further be aware that we have never received any approval (nor disapproval) of the Dutch Privacy Authority with regard to our current whois services. So please do not automatically assume that what we do is completely in line with the Dutch and/or European privacy laws.

Description of the .nl whois

1. We have split the whois in different forms for different users:

   a. Public whois web
   b. Public whois command line
   c. Whois for registrars
   d. Whois for law enforcement
   e. Whois for CA's

2. The last three (1c - 1e) forms of whois still show all information that we provided before 2010 but they are only accessible to the groups that they were created for. (see further under 7 - 9)

3. The two public available whois services provide limited information.

   a. via the command line we only show the status of the domain, the name and physical address of the registrar and the name server data.
   b. in the public whois on our website the information is limited to:

[1] Please refer to http://forum.icann.org/lists/whoisrt-discussion-paper/msg00008.html

i. status if the domain

   ii. name of registrant

   iii. e-mail addresses of admin-c an d tech-c (protected so that they are not easy to copy)

   iv. name and physical address of registrar

   v. name server data

c. on our website we do not show:

   i. Names of admin-c/tech-c

   ii. Address details for registrant/admin-c/tech-c

   iii. Telephone numbers

4. The reason that we still provide the name of the registrant is because a name without any contact details is for most of the people not very troublesome and gives the registrant the opportunity to check if a domain is registered in the correct name.

5. We do not, like for example .net or .uk, make any distinction between private and non-private persons as we think this will only lead to an extra complaint procedure. We might consider however to give registrants the opportunity to decide for themselves if they want us to publish their address and other non obligatory contact details.

6. In order that .nl registrants can be contacted regarding legal matters, SIDN will make the address of a registrant available for that purpose to an attorney or court bailiff practicing in the Netherlands who makes an individual request for such information. A special manual procedure for processing requests has been set up.

7. The whois for law enforcement is open for investigative and law enforcement authorities that have the statutory power to require SIDN to provide full details of a registration. These authorities may obtain automated access to the whois provided that certain (contractual) conditions are met.

8. SIDN registrars can make use of a dedicated Registrar Whois service. Registrars need access to Whois data in order to undertake legitimate registration activities. So the full Whois dataset remains available to them. This is however subject to revision as we are currently not able to fully control that the information is only used for legitimate means.

9. SIDN also allows Certification Authorities (CAs) access to the full whois dataset. The procedure for CAs with regard to the issuance of SSL Certificates usually

> includes checking whether the details provided by the certificate applicant are the same as the details that SIDN has on record for the relevant domain name. Since CAs make their enquiries at the request of the registrant itself, SIDN is willing to provide them the requested information."

b) United Kingdom (.uk)

Submitted by Nominet[2]:
Nominet: ccTLDs are focused on serving the needs of specific jurisdictions, which allows them to tailor their approach to local circumstances. Privacy is an issue and ignoring it will increase the probability that data will be incorrect, even from those without malicious intent. In the case of.uk, Nominet has a contract with the registrant and can use this to require corrections. However, data may be incorrect due to misunderstandings, not updated when circumstances change or changes may not be passed on to our systems. We work on improving data quality by proactive checks and in response to complaints, and act quickly when malicious activity is suspected. This remains our priority.
There is a trust issue associated with inaccurate contact data, in particular for domains used for trade. This creates a question of trust for the TLD in relation to law enforcement, regulatory and other public authorities. This could impact consumer confidence, but very few users are aware of WHOIS. The EU's e-Commerce Directive has requirements for trading websites to include contact information so that third parties know who they are dealing with. For the consumer, this information is more accessible than WHOIS. Nominet has a onestop shop portal for information and links and contributes to awareness initiatives as WHOIS data can be abused to assist fraud and spam. Nominet has developed its WHOIS policy and implementation in consultation with stakeholders. Our contribution provides data about the UK environment in response to the request for ccTLD input. We have not responded to questions on the gTLD WHOIS policy.

c) Canada (.ca)

CIRA went through an extensive WHOIS and privacy policy reform in early to mid 2000. Prior to the reform initiatives, CIRA provided WHOIS services which were in line with the gTLD WHOIS approach, i.e., it displayed and provided all registrant information including: name, domain name, registrar of record, date the domain name was registered, contact details (email, mailing address, telephone number, and fax number), the date when the information was last changed. After extensive consultation with CIRA's stakeholders, CIRA made a distinction between two types of registrants: (1) private; and (2) corporate. Private registrants were natural persons, but also included small organizations such as a 5-person corporation (which could go up to as much as 10). The latter was in line with some rulings by the federal and provincial privacy commissioners in Canada. For those private registrants the default was not to display any personally identifiable information unless the registrant chose to make it publicly available. For

[2] Please refer to http://forum.icann.org/lists/whoisrt-discussion-paper/msg00018.html

corporate registrants, the default and only option was to have all its information publicly available.

CIRA also implemented a process by which a corporate registrant could apply for privacy protection. Once a corporate registrant check marked that it would like to keep its information private, CIRA did not display the information for 30 days during which the corporate registrant had to provide proof that its request was legitimate and in line with CIRA's WHOIS policy. Legitimate reasons may have been a battered woman's shelter or some other organization which, for security reasons, may require greater privacy than other corporate entities. If the corporate registrant satisfied the request for privacy, the information would remain private. If, however, the corporate registrant was not able to satisfy the privacy request requirements, the registrant information was automatically published after the 30-day timeframe.

At the time when CIRA launched the new WHOIS policy, there was no special access for law enforcement of any type. However, within a couple of years after launch, CIRA responded to some significant pressures from law enforcement and implemented a new policy entitled "Request for Disclosure of Registrant Information for Law Enforcement and National Security Agencies – Rules and Procedures". The policy provides a fairly limited access right to law enforcement which includes the investigation of child exploitation, espionage, or imminent threats to the Internet. The disclosure, unless prohibited by law, will be made public to the registrant whose information was disclosed, within 30-60 days.

d) France (.fr)

Submitted by AFNIC[3]:

AFNIC's data publication and access policy describes how registrant data is gathered, disclosed and used during the lifetime of a domain name registration: a) Private registrants' data is not displayed in the public Whois b) AFNIC provides on line web forms to enable any interested party to send electronic messages to the domain name admin contact without disclosing its data c) Right owners or affected parties may request disclosure of registrant data. Such requests are handled by AFNIC which checks whether the affected party has some right over the domain name before disclosing. This policy was set up in 2006 with amendments in 2007 to comply with privacy laws and an instruction from CNIL. While .FR approached 2 million domains in 2010, AFNIC handled 412 data disclosure requests, whereof 356 granted. The policy reinforces trust from private registrants, as they can provide accurate data with limited risk of unsolicited communications, and customer relations suggest that the policy has a positive impact on data accuracy.

e) Australia (.au)

Submitted by Cheryl Langdon-Orr[4]:

Despite the fact that one can have a bricks and mortar address in a system it need not necessarily be the actual address of the registrant; and that's something that we see in other

[3] Please refer to http://www.icann.org/en/public-comment/report-comments-whoisrt-discussion-paper-05aug11-en.pdf

[4] Please refer to https://community.icann.org/download/attachments/19300487/whois-review-alac-21jun11-en+%283%29.pdf?version=1&modificationDate=1315416878514

parts in some countries, even with quite strict regulations such as my own. You have the ability to have what's called 'registered office address' which is a bricks and mortar situation; but you also have in law the right, with the appropriate motivations and knocking on the right doors with if necessary the right pieces of paper

f) Trinidad and Tobago (.tt)

Submitted by Dev Anand Teelucksingh[5]:
.tt ccTLD doesn't even offer WHOIS at all.

g) Ireland (.ie)

Submitted by Michele Neylon – Blacknight Internet Solutions[6]:
in .ie the only data that appears in WHOIS is the holder, the holder name, the WHOIS output is a bit different to a standard one. So in the case of a domain that will be registered to a company, so let's say domain holder Blacknight Internet Solutions Limited, and then you would have the applicant. There's two, an applicant registration type classing type think. I mean, think of it a bit like your classes for trademarks; same kind of concept. For a private individual again, you just have the holder is Joe Soap, but no contact details for Joe Soap. There's just a nic handle, which obviously is going to be unique to the person. And if somebody needs to contact tehm for whatever reason, be that in terms of a dispute, law enforcement or whatever, they can go via the registry.
....
If you do a WHOIS look up on say Blacknight.ie for example, you're going to get back name servers, you're going to get back expiry dates, you're going to get back handles. You can't look beyond the handle. Now, in the case of the applicant, sorry the domain holder type, if the domain holder is down as a body corporate, in other words a limited company, you can of course go to our company's house type thing and get back data there. And if somebody had, if there is the case of say a WIPO dispute, as part of the process you would go to the registry, but not via command line. You'd go contact them using more manual methods to reveal the data."

Verbal Comments Made during Outreach Session

On .fr – Comment made by Michele Neylon (.ie)[7]
.fr has the option as well for a private individual to be opted out. And that is actually provided by the registry. And they provide an [atanom].fr.

[5] Please refer to https://community.icann.org/download/attachments/19300487/whois-review-alac-21jun11-en+%283%29.pdf?version=1&modificationDate=1315416878514

[6] Please refer to https://community.icann.org/download/attachments/19300487/whois-community-22jun11-en.pdf?version=1&modificationDate=1312224891000

[7] Please refer to https://community.icann.org/download/attachments/19300487/whois-community-22jun11-en.pdf?version=1&modificationDate=1312224891000

On .eu – Comment made by Michele Neylon (.ie)[8]

Michele Neylon: "The .eu registries do the same. So they don't, they're able to go along and kind of validate stuff and make sure that there aren't kind of weird inconsistencies like people registering as Mickey Mouse. .eu again, there's very little data available in standard WHOIS and if you want to get more data you have to go to a webpage, you have to go past a capture. And they also have taken measures to protect the email addresses. So they're rendered as a jpeg or a png or something like that so you can't scrape the data off there."

On .co.uk – Comment made by Michele Neylon (.ie)[9]

For .co.uk you've got the opt-out. And again, if they're a legal organization and they try to opt out, as part of the WHOIS review stuff that Nominet would do, they get opted back in.

[8] Please refer to https://community.icann.org/download/attachments/19300487/whois-community-22jun11-en.pdf?version=1&modificationDate=1312224891000

[9] Please refer to https://community.icann.org/download/attachments/19300487/whois-community-22jun11-en.pdf?version=1&modificationDate=1312224891000