WHOIS Policy Review Team (WHOIS)

Draft Report

***24 November 2011***

1. **Executive summary (content owners: Bill, Lynn, Sharon)**

The Internet Corporation for Assigned Names and Numbers (ICANN), is one of a small but important set of organizations responsible for administering certain functions critical to the operation of the Internet. ICANN's primary responsibility is to facilitate the policy maintenance and enhancement of the Domain Name System (DNS), an integral part of the Internet.

ICANN is a California, public benefit corporation that undertakes periodic reviews to assess its efficacy in serving its various constituencies and the global public at large. This report is the formal output of the Review Team responsible for assessing WHOIS and represents the culmination of a year-long effort by a diverse group, representative of ICANN's makeup.

1. **History**

ICANN was formed in 1998 to fulfill the requirement that operation of the DNS move from the government to private sector control.

WHOIS (not an acronym) was first defined as a *protocol* of the Internet Engineering Task Force (IETF) in 1982. WHOIS is one of the simplest in the suite of protocols that the IETF maintains. Any machine connected to the Internet can operate a WHOIS *service* by implementing the protocol and responding to requests as described in the *specification*.

Initially, the WHOIS *specification* described a set of information that was requested of anyone capable of transmitting information across the network. This information consisted of name and contact information which was to be stored on specific servers and would be returned upon receipt of an appropriate WHOIS request.

As the Internet grew and it became impractical to maintain a single WHOIS server, updated versions of the *specification* were developed and approved. These specifications dropped the references to specific servers and required information thereby enabling broader use of the specifications. It was then incumbent on any community desiring to use WHOIS to define required information and where that information could be found. ICANN is responsible those definitions for the Domain Name System.

In 2009, ICANN and the US Department of Commerce approved, signed, and published [**ET deleted “to the world”**], an Affirmation of Commitments (AoC) that establishes a set of principles. [**ET added ]** The AoC specifies that four periodic reviews of ICANN are to be conducted; Accountability and Transparency, Security, Stability, and Resiliency, and WHOIS.

1. **Discussion**

Domain names are the familiar sequence of characters we see in our web browsers after the "http://www." and before the next "/"; e.g. "[google.com](http://google.com)", "[redcross.org](http://redcross.org)", and "[europa.eu](http://europa.eu)". They are an integral part of the Internet, serving us as mnemonics for places we have been or wish to be, and as keys for machines to perform the necessary translation from the abstract to the real.

Domain names sit on the human side of the man-machine interface and through the DNS are translated to machine-compatible Internet Protocol (IP) addresses. Internet-connected machines use IP addresses to send and receive messages transmitted over the Internet. They are fundamental to the Internet itself, as is uniform translation from name to number, and back again.

While the DNS presents a single, complete view of the Internet, no single machine holds all of the Internet's addressing and mapping information. Rather, that information is distributed across a series of name servers that cooperate to seamlessly provide that one comprehensive view.

Domain names and the DNS are used in virtually every aspect of the Internet, not just those parts most visible to most consumers, web browsers. Every email message, song or movie download, instant message, tweet, facebook "like", or online transaction involves the DNS in some way. Without the DNS, the Internet would not exist as we know it.

As important as machine to machine communication is, there are times when human to human interaction related to the Internet is required. The reasons for this interaction are varied and include notice, abuse, and security amongst others. For these reasons, contact information (as specified by ICANN) related to a domain name must be provided in order to register a domain name, much like when registering a vehicle.

This information is stored and is available to the public through a system known colloquially as WHOIS. WHOIS predates the "commercial" Internet and remains largely unchanged since its earliest days, ca 1982. It is likely that it was selected for use in this context because it existed and was well-understood. In all probability, it was selected by default.

1. **Debate**

WHOIS is the source of long-running discussion and debate at ICANN, other Internet Governance institutions, and elsewhere. This team and its successors hopefully will inform future debate and consensus-based decision making.

Issues in the WHOIS debate are varied. Any discussion of WHOIS will likely contain all of the words accuracy, privacy, anonymity, cost, policing, and SPAM. Each of the issues is important. This is sometimes lost in the heat of the debate and it is important to remind ourselves of this on a regular basis.

In order to inform the debate, and perhaps make the decision making process easier, ICANN has adopted the age-old tradition of "the study" in lieu of or a precursor to action. Significant sums have been spent studying WHOIS, more is being spent, and yet more is planned with the span of time now stretching into decades.

Each study addresses some different aspect of WHOIS; accuracy, proxy/privacy reveal/request, availability, ... They take time to be approved, conducted, reported, and of course debated. This time is measured in years and could be called ICANN time as compared to Internet time. The one constant throughout has been WHOIS itself; protocol, service, data.

1. **Conclusion**

This summary discussion is not a condemnation of the debate, the studies, or the people that invested their time, emotion, and personal capital over the years. Rather, it is an attempt to concisely present in a balanced and fair manner the very real truth that the current system is broken and needs to be repaired.

This Review Team reflects the diversity of ICANN's multi-stakeholder model. We have been given time to conduct our review receiving invaluable feedback from the community. We agree to disagree yet we have found consensus, for each and every one of the recommendations we make. We look forward to participating the debates that follow, and monitoring their implementation if adopted by the Board.

1. **Work of this RT**

[ET] The WHOIS Review Team’s scope, guided by the Affirmation of Commitments was to review the extent to which ICANN’s WHOIS policy, and its implementation are effective, meet the legitimate needs of law enforcement and other relevant community stakeholders in order to promote consumer trust.

Formed in October 2010, the WHOIS Review Team comprised representatives from across the ICANN constituencies, a representative of law enforcement and two independent experts. The Review Team held two dedicated face to face meetings during its term, as well as working and outreach sessions at each of the ICANN meetings in 2011. Fortnightly calls were also held. Apart from rare occasions where Chatham House rules were invoked, all the Review Team’s calls, meetings and e-mail list were open to observers, and the public wiki {link] provides an archive of our activities.

1. **Findings**

One of our earliest "findings" was our inability to find a clear, concise, well-communicated WHOIS Policy. The team was assured that one existed and that it had been in force for some time. Several versions of Registrar and Registry contracts were reviewed as were compliance activities related to the policy. Throughout, we were unable to locate a document labeled WHOIS Policy as referenced by the ICANN-approved Affirmation of Commitments.

One of the findings of this review would indicate that the WHOIS policy is not clear, concise, or well-communicated; hallmarks of good policies. What once might have been simple has been allowed to become complex, difficult to understand or to identify the parties responsible for changing it.

While there is no specific policy, there has been no lack of WHOIS related effort. Rather, we find that considerable effort has been expended over the years, discussing, debating, arguing, proposing, developing, and implementing WHOIS "policy". Meaningful attempts at change have been made but it is unclear that these changes have in fact resulted in improvements.

A gross understatement is that tensions exist between the various ICANN constituencies regarding WHOIS. Issues abound including right to privacy, anonymity, intellectual property protection, security and abuse, among others. Each is important, none more so than the other.

We find little consensus on the issues. More concerning, there appears to be no coordinated effort to achieve consensus on these important, and admittedly difficult issues. It should be noted that neither ICANN, the corporation, nor ICANN the community, have seen the need to charge an individual or group as responsible for WHOIS. We find this a significant oversight and surmise that without such a coordinating effort, the small steps required for consensus may never be taken.

Perhaps it should be no surprise that in this environment, policy and implementation has not kept pace with real world. International Domain Names (IDNs) were introduced to great fanfare by ICANN 2001, and in 2010 at the root level, without a corresponding change to its policies related to WHOIS.

What this means, is that while domain names can now be written in Arabic for example, the contact information for these domains must still be transliterated into a format ill-suited to the purpose. A discussion of the issues behind this is beyond the scope of this review but the issues are well-understood and mechanisms exist to address it. Admittedly, change in this space will take time, and ICANN (and others) are taking steps to improve the situation but we find it is a case of too little too late.

Privacy and proxy services have arisen to fill the ICANN policy vacuum. These services are clearly meeting a market demand and it is equally clear that these services are complicating the WHOIS landscape. We find that ICANN has neglected to appropriately address the rights of "non-commercial" natural persons as defined in the four communiqués from the EC Article 29 W to ICANN over the years. [**ET proposed deletion :**[something on thick/thin? WHOIS Services are confusing to consumers?]

In the time since the formation of ICANN, Internet usage for ill-gain or harm has increased dramatically. Combating it has become, and remains ever-more complex both for Law Enforcement Agencies (LEAs) and those responsible for any Internet-connected service.

Governments have recognized the changing landscape and have individually enacted cybersecurity laws and cooperatively entered into international cybersecurity treaties. Certainly more needs to be done here, but steps have been taken and more are on the way.

Cybersecurity and cybercrime experts make extensive use of WHOIS to thwart and respond to a varied set of threats. Information contained within WHOIS is invaluable in these efforts and practitioners [ET] have conveyed to us their frustration at the continuing high levels of inaccuracy of WHOIS data. We find that ICANN has neglected to respond to the needs of this community both in the accuracy of WHOIS data and in response times for access and action.

**[ET]** Where does this leave the issue of “promotes consumer trust”? Having struggled with what “consumer” means in the context of WHOIS, and aware of the Affirmation of Commitments’ observation that there are key stakeholders who do not engage in the ICANN environment, the WHOIS Review Team commissioned consumer research. This found that drivers of consumer trust include knowing the entity with whom they are dealing, and being able to find reliable contact information. The vast majority of consumers were unaware of the existence of the WHOIS service, and many struggled to understand the format of WHOIS outputs. This led us to conclude that the current implementation of WHOIS services does not help to build consumer trust, and more could be done to raise awareness of the service, and to improve its user-friendliness.

For something so simple as WHOIS the protocol, it is unfortunate that WHOIS policy has become so complex and unmanageable.

1. **Recommendations**

**[TO BE ADDED]**

1. **Introduction (content owner: Kathy Kleiman)**

The first WHOIS Review Team, required by the Affirmation of Commitment, was selected in September 2010 by the President and CEO of ICANN, Rod Beckstrom, and the Chair of the Governmental Advisory Committee (GAC), Heather Dryden.  Members of the Review Team were:

* Emily Taylor (UK), Chairman
* Kathy Kleiman (US), Vice Chairman
* James Bladel (US)
* Lutz Donnerhacke (DE)
* Lynn Goodendorf (US)
* Sarmad Hussain (PK)
* Olivier Iteanu (FR)(resigned in June 2011)
* Omar Kaminski (BR)
* Susan Kawaguchi (US)
* Bill Smith (US)
* Kim von Arx (CA) (resigned in October 2011)
* Wilfried Woeber (AT)
* Seth Reiss (US) (joined in September 2011)
* Sharon Lemon (UK), Law Enforcement Representative
* Peter Nettlefold (AU), Designated Nominee of Selector Heather Dryden, Chair of the GAC
* Michael Yakushev (RU) Designated Nominee of Selector Rod Beckstrom, ICANN President and CEO

The Review Team thanks the ICANN staff who supported our work, including Denise Michele, Liz Gasster and Stacy Burnette.  The Review Team extends heartfelt thanks in particular to Olof Nordling and to Alice Jansen for their outstanding support, good humour and commitment, and to all members of the ICANN community who contributed comments during the consultations.

This report set outs out the work of the WRT: its scope of work and methodology, key definitions, identification and inventory of ICANN’s existing WHOIS policy, identification and inventory of ICANN’s implementation, a gap analysis between ICANN’s policy and expectations under the Affirmation, and recommendations of the Review Team to the ICANN Board.

Consistent with the requirements of the Affirmation of Commitments, we publish this report for public comment in October 2011. We will seek final consultation with the Community in Senegal at the ICANN meeting and issue the Final Report and Recommendations by November 30, 2011.

1. **Background (title to be improved)**
2. **A Brief Guide to the Domain Name System and WHOIS**
3. **DNS and WHOIS – How it Works**

The Domain Name System (DNS) helps people to find resources like websites and email servers on the Internet. To explain it in simple terms, every computer has a unique number called an IP address, e.g. 74.125.73.147, which could be compared to a phone number. One computer can contact another as long as it knows its IP address. Because these numbers are difficult to remember, we tend to use domain names e.g. [www.icann.org](http://www.google.com) instead. DNS is the system that translates between domain names and IP addresses. It is made up of many components which include WHOIS databases, domain name servers and root servers.

**WHOIS** is the Internet protocol that is used to query information relating to who ‘owns’ a domain name. Actually people do not *own* domains; they simply reserve the right to use them for a period of time. The databases that contain this information are referred to as WHOIS registries and these hold contact details of the registrant[[1]](#footnote-1), i.e. the person or organisation who reserves a domain. WHOIS registries are run by Registry Operators, for example VeriSign who maintain the *.com* registry.

Registry operators also maintain another vital piece of information. Within their name servers they identify the authoritative **name servers**[[2]](#footnote-2) for their domains, which hold the key to where a website is located. For example, if you type [www.icann.org](http://www.google.com) into a browser, your ISP will query the relevant WHOIS registry operator to find out which name server is associated to that domain name. That name server is then contacted and will return the IP address for that domain name. Your computer can now connect to the computer(s) that will serve up the ICANN homepage. This process is illustrated below.

As can be seen in the diagram, the selection of which registry operator is to be queried each time depends on the final part of the domain (e.g. .*com, .net, .uk*), also known as the Top Level Domain (TLD[[3]](#footnote-3)). If the ISP doesn’t already know which registry operator to ask for information on *.org* domain names, it can ask a **root server**. There are various root servers located all over the world which hold this information and can direct the request to the relevant registry operator.

In reality, the root servers, registry name servers and authoritative name servers are not usually queried directly, as the information is cached for a time by your ISP (and on name servers across the Internet) from the first time that someone requests this domain.

1. **The Domain Name Registration Process**

Like IP addresses, domain names also need to be unique so there has to be a way of associating them with a particular person or organisation. This is done through the domain name registration process. In order to reserve a domain, a registrant must register it with one of almost a thousand ICANN-accredited registrars. The registrar will check if the domain is available and will ensure that the WHOIS contact information is updated for that domain name. It is also possible to register domains through resellers. The diagram below illustrates the main functions of the parties that are usually involved in the process.

A **Registrant** is the person or organisation who has registered the domain name. In order to do so, the registrant will usually apply online to a domain registrar or one of their resellers. The registrant is bound only by the terms and conditions of the registrar with which it registers, for instance adhering to a certain code of conduct or indemnifying the registrar against any legal or civil action taken as a result of use of the domain name. Registrants have certain responsibilities which should be incorporated into these terms and conditions in terms of payment of registration fees and submission and timely update of accurate data.

In addition to registering the name, they also need to have their domains listed on name servers in order to have that domain reachable on the Internet. If this service is not offered by the registrar, or registrants opt out, then they are responsible for procuring or hosting their own name servers.

**Registrars** are organisations accredited by [ICANN](http://en.wikipedia.org/wiki/ICANN) and certified by relevant registry operators to sell domains. They are thus bound by the Registrar Accreditation Agreement (RAA) with ICANN[[4]](#footnote-4) - and also by their agreements with the registry operators. The RAA sets out responsibilities for the registrar including maintenance of WHOIS data, submission of data to domain registries, facilitating public WHOIS queries, ensuring registrants details are escrowed or that if not possible to escrow (e.g. for some proxy and privacy registrations) that registrants are aware of this, and finally complying with RAA conditions relating to the conclusion of the registration period.

Registrars are also responsible for verifying WHOIS information supplied by the registrant, and for periodic re-verification of contact information. They are required to take reasonable steps to verify contact information if notified that it is inaccurate and also to correct these inaccuracies where they are aware of them. The Registrar must maintain proper contact information for itself, including a valid email and mailing address which should be posted on their website. The RAA also requires the Registrar to take compliance and enforcement action against a Reseller violating any of the required provisions.

Some registrants may opt to register through a **Reseller**. These are affiliated to registrars, and usually offer other services such as web hosting, email mailboxes etc. Resellers are only bound by their agreements with the registrar(s) whose services they sell, they are not accredited by ICANN. However, the registrar for whom they are re-selling will still be accountable for the domains that they sell.

Under the 2009 RAA, registrars must include specific items in their agreements with resellers, such as identification of the sponsoring registrar and all of the same provisions that the registrar is required to include in its agreements with domain name registrants.

While Registrars are contracted by them to conduct the day to day business of selling domain name registrations, **Registry Operators** are responsible for maintaining the registry for each TLD. The responsibilities of the registry operator include accepting registration requests (whether from registrars or directly from registrants), maintaining a database of the necessary registration data and providing name servers to publish the zone file data (i.e. information about the location of a domain) throughout the Internet.

Finally, the **Internet Corporation for Assigned Names and Numbers** (ICANN) is the international non-profit corporation that oversees the assignment of both IP addresses and domain names. It has responsibility for managing root server and TLD name system management and has contractual arrangements with both registries and registrars.

1. **Diagrams**

**TBD**

1. **Scope of Work (content owner: Kathy Kleiman)**

In 2009, ICANN and the US Department of Commerce signed the Affirmation of Commitments (AoC), and ICANN committed itself to the following obligation regarding Whois information:

“9.3.1 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.”

<http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm> (translations available on this page)

ICANN undertook a specific obligation to form a global Review Team to assess specific Whois issues, within a year of the AoC signing, and every three years:

“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 review will be performed by volunteer community members and the review team will be constituted and published for public comment, and will include the following (or their designated nominees): the Chair of the GAC, the CEO of ICANN, representatives of the relevant Advisory Committees and Supporting Organizations, as well as experts, and representatives of the global law enforcement community, and global privacy experts. Composition of the review team will be agreed jointly by the Chair of the GAC (in consultation with GAC members) and the CEO of ICANN.”

“Resulting recommendations of the reviews will be provided to the Board and posted for public comment. The Board will take action within six months of receipt of the recommendations.”  Affirmation, Section 9.3.1.

The Whois Review Team (WRT) met for its first formal face-to-face meeting in London, England, to determine the scope and methodology of its work. The Affirmation calls on the WRT to review the commitments of ICANN regarding its Whois Policy:

9.3.1 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.

Upon close review of the Affirmation, and discussions with its drafters and signatories, including, Lawrence E. Strickling, US Department of Commerce, Assistant Secretary for Communications and Information, the WRT set out its scope broadly:

To assess the extent to which existing WHOIS policy and its implementation:

* + is effective,
	+ meets the legitimate needs of law enforcement; and
	+ promotes consumer trust

in accordance with the principles set out in the Affirmation, in particular paragraph 9.3.1.

The WRT further committed to review two key requirements of the Affirmation:

* “implementing measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information;” and
* “enforcing its existing policy relating to WHOIS, subject to applicable laws.”

In determining the scope of their review, the WRT was able to establish principles to guide its work. The first principle affirmed that the WRT exists *to evaluate policy, not create it*. Scope and methodology were set consistent with this principle.

Additional principles from the Affirmation further guided the WRT work. While each WRT member hails from a particular community within or outside of ICANN, we agreed to conduct our work pursuant to the broad public interest principles set out the Affirmation, including:

* + "decisions made related to the global technical coordination of the DNS are made in the public interest and are accountable and transparent" Section 3(a)
	+ should “promote competition, consumer trust, and consumer choice in the DNS marketplace" Section 3(c), and
	+ should "reflect the public interest...and not just the interests of a particular set of stakeholders" (paragraph 4).

The WRT adopted its Scope of Work plan together with an ambitious outreach and action plan at its first meeting in London, (what month?) 2011, and published it for community review and public comment in March 2011. These plans became the roadmaps which guided the WRT work throughout its work.

1. **Definitions (content owner: Sharon Lemon)**
2. **Introduction**

Early in the WHOIS Review Team’s work program, we attempted to identify and define key terms in the Affirmation of Commitments.

In conjunction with comments from the Community[[5]](#footnote-5), the Team found it useful for purposes of facilitating our review that we consider the following definitions as guides for our work:

AOC TERMS OF REFERENCE: Law Enforcement; Consumer and Consumer Trust; Applicable Laws:

1. **Law Enforcement**

WRT defines “Law Enforcement” as:

* Any entity charged, or otherwise mandated by government, with the regulation and control of the affairs of a community; an organised body of people officially maintained or employed to keep order, prevent or detect crime and enforce the law.

The adopted definition intentionally does not include private individuals and organizations, such as anti-spam groups or those bringing civil enforcement actions, whose efforts may be viewed as within a larger concept of law enforcement. In adopting the narrower definition, the WRT does not discount the value of private sector efforts to curb abusive uses of the DNS.

With the adopted definition in mind, the WRT consulted with law enforcement through a questionnaire seeking better understanding of the use and concerns regarding Whois data. The results of this survey are discussed in Section \_\_\_\_.

1. **Consumers and Consumer Trust**

WRT found two potential classes of consumers:

* All Internet users, including natural persons, commercial and non-commercial entities, governments and academic entities (including registrants, registries and registrars).
* The individual or organization who purchase the domain name and provide data for inclusion in the Whois.

The WRT found the definition of Consumer Trust, something the ICANN Community is also exploring in the context its policy-making processes, to be particularly challenging. Consumer Trust can be narrowly construed to mean the level of trust Internet users have in available WHOIS data; or more broadly as the level of trust consumers have in Internet information and transactions in general. WRT focused its “consumer trust” research on the WHOIS issues, and reached outside the ICANN community to engage third party researchers for multi-country research. This research, and its results, is covered in Section \_\_\_.

1. **Applicable laws**

The Affirmation commits ICANN to enforcing its existing policy relating to WHOIS, “subject to applicable laws.” The WRT, following public comment, found it reasonable to view Applicable Laws as:

Any and all local and national laws that regulate and/or control the collection, display and distribution of personal data via WHOIS.”

The Team understands the “applicable laws” reference as limited to privacy laws and regulations and notes ICANN’s existing consensus policy relating to conflicts with privacy laws. The Team considered but determined not to include within the definition international agreements and regional laws, recognizing that such laws are enforceable only to the extent incorporated into the domestic laws of contracting states.

1. **WHOIS PARTICIPANTS: Data Producers; Data Controllers; Data Processors.**

The WRT determined a need to identify and differentiate the various actors in the WHOIS supply chain, and understand their decentralized, and distributed, responsibilities for WHOIS data and its processing. We identified three categories of participants:

**Data Producers**: The individuals or organizations who purchase domain names (ie domain name holders/registrants) and supply contact information for inclusion in the WHOIS data. This group is also responsible for the accuracy of the WHOIS data.

**Data Controllers**: The organizations responsible for promulgating rules prescribing how WHOIS data is to be collected, stored, released and used (ICANN for gTLD Registries and Registrars; This group also includes governing boards and/or government entities for country code TLDs (ccTLDs), which are beyond the scope of this Review as they are independent in their policy making).

**Data Processors**: the Registrars and Registries engaged in the collection, storage and release of the data, according to terms and conditions promulgated by the “Data Controller.” Data processors may also include other entities within the supply chain, for example resellers, proxy and privacy service providers. These entities do not determine the nature or use of the Whois data they collect, maintain and process; rather the Data Controllers do.

1. **WHOIS COMPONENTS: WHOIS Data; WHOIS Protocol; WHOIS Services:**

Finally the WRT found it useful to define, the data, protocol and services that comprise the term WHOIS. In this regard, the WHOIS Review Team found the work of ICANN’s Security and Stability Advisory Committee invaluable, and extends its thanks for their valued input:

**Domain Name Registration Data**: The information that registrants provide when registering a domain name and that registrars or registries collect (registrant name, address, telephone; administrative and billing contacts; etc). Some of this information is made available to the public. [...]

**Domain Name Registration Data Access Protocol**: The elements of a (standard) communications exchange – queries and responses - that make access to WHOIS Data possible. For example, the WHOIS protocol (RFC 3912) and HTTP (RFC 2616 and its updates) are commonly used to provide public access to WHOIS Data.

**Domain Name Registration Data Directory Service**: The service(s) offered by registries and registrars to provide access to all or a subset of WHOIS Data [...]

1. **Producers and Maintainers of WHOIS Data**

**Definitions (approved 2 March 2011):**

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.

**Overview of Received Comments**[[6]](#footnote-6)**:**

Five parties provided feedback.

Two groups support the definitions given **(BC & RSG)**.

In other comments; there is a question as to whether definitions of these terms are needed, given that they are not referred to in the AoC, the WHOIS RT Scope or the WHOIS RT Roadmap **(IPC)**.

The definition of ‘producers' does not recognise the different parties that may fill this role, and their differing objectives / perspective which may have an impact **(CAUCE & ECTA+M)**.

The inclusion of ‘may or may not be directly involved…’ in the definition of ‘maintainers’ has led to some confusion, and again it was felt that roles within the definition may have been grouped too generally. It was also felt that the use of terms from EU data protection legislation may confuse some parties  **(CAUCE)**.

The WRT also need to recognise that EU data protection rules apply only to individuals; businesses and organisations do not generally have a right to privacy **(ECTA+M)**.

1. **What is a "consumer"?**

WRT found two potential classes of consumers:

* All Internet users, including natural persons, commercial and non-commercial entities, governments and academic entities(, and including registrants, registries and registrars).
* The individual or organizations who purchase the domain name and provide data for inclusion in the Whois.

The WRT found the definition of Consumer Trust, something the ICANN Community is also exploring in the context its policy-making processes, to be particularly challenging. Consumer Trust can be narrowly construed to mean the level of trust Internet users have in available WHOIS data; or more broadly as the level of trust consumers have in Internet information and transactions in general. WRT focused its “consumer trust” research on the WHOIS issues, and reached outside the ICANN community to engage third party researchers for multi-country research. This research, and its results, is covered in Section \_\_\_.

1. **CONSUMER STUDY (Content owners: Lynn Goodendorf, Susan Kawaguchi, Seth Reiss)**
2. **Introduction**

The Review Team decided to undertake an independent research study to gain a better understanding of consumer trust as it relates to the use of WHOIS. The premise for this decision was based on the AOC, Paragraph 4 which states:

“A private coordinating process, the outcomes of which reflect the public interest, is best able to flexibly meet the changing needs of the Internet and of Internet users. ICANN and DOC recognize that there is a group of participants that engage in ICANN's processes to a greater extent than Internet users generally.”

Therefore, the WHOIS review team felt that we should solicit input beyond the ICANN constituencies. Specific questions related to consumer trust were:

What factors influence consumer’s perception of trustworthy websites?

Are consumers aware of the WHOIS and WHOIS records for domain name registrations to evaluate trust in a website?

Are consumers able to locate and find domain registrant information with a reasonable ease of use?

A subcommittee was formed to address these questions. The initiative, led by Lynn Goodendorf, engaged a third party service 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.

1. **Phase One: Qualitative Phase**

The primary purpose of the qualitative phase was to determine similarities across countries as well as distinct differences resulting from unique cultures and perspectives. This further lead to a quantitative survey.

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 on that exercise;
* 11 of the 20 individuals owned a domain name and were asked to look up their own information and their feedback was captured.

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. Trust-building components mentioned in this phase included:

* Visual Aesthetics of Website and Ease of Navigation

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

* Perceptions of “.com”

Viewed as more credible and trusted

Assumptions made that .com was unavailable for websites using other TLDs

International users did not express more trust for their home country code TLD

* Strategies to find Domain Owner Information

Use of search engines such as Google, Bing, Maps, etc.

Locating User Forums with comments about websites

Overall low awareness of WHOIS as a lookup or directory service

1. **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](http://www.thecocacolacompany.com)”.

Thick, or detailed, WHOIS information for [www.thecocacolacompany.com](http://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, or limited details, WHOIS data. Consequently, the name and address of the owner 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.

The results of the survey revealed that most located the correct name and address of the owner of the [www.thecocacolacompany.com](http://www.thecocacolacompany.com) domain name, but not through a WHOIS service.

Interestingly, similar themes emerged from this phase of the study, summarized below:

* Website Trust
* Trust in a website is enhanced with safe and secure images such as VeriSign and TRUSTe when visiting ecommerce sites (68%)
* Websites of companies or brand names already known to the users also engenders trust: (63%)
* Users in France also look for https for a lock icon in order to obtain confidence in the site (50%)
* When concerned that a website is fraudulent, the majority of users will look for contact information on the website content (67%) and then search for user reviews (60%)
* When asked to locate the domain owner of www.thecocacolacompany.

com, most agreed that it was easy (72%), and correctly identified the owner of the website (66%)

* Most users agreed that they were confident they had found the information they were looking for (76%) and that the information they found was trustworthy (85%)
* WHOIS
* Overall, awareness of WHOIS is low (24%).
* When asked to find the owner of [www.thecocacolacompany.com](http://www.thecocacolacompany.com), most users did not think to utilize the WHOIS look-up service (77%)
* If concerned that a website is fraudulent, 68% of International and 65% of National users would “Find Website Contact Information” first and “Search for User Reviews” as a second step users (59% of International and 61% of National).

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.
1. **Conclusions**

Significant indications from the UserInsight study include:

Those wanting to validate the integrity or authenticity of a website use a variety of methods which indirectly lead to WHOIS data published by registries and registrars. However, the WHOIS results pages were confusing and lacked credibility because of the visual presentation and distraction of domain ads for sale.

A significant percentage of those who own a domain name are unaware of WHOIS and, therefore, unaware that their name and contact information are publicly available through WHOIS.

The study does not reveal the potential value of WHOIS to the overall population of Internet users because there is such a low level of awareness and a lack of consistency in the source and presentation of WHOIS data or domain registrant information.

The results of the study are consistent with our impression that “consumers of WHOIS” are not the same as “consumers” of Internet services generally, that is, Internet users. We think “Consumers of WHOIS” comprise, to a greater degree than others, law enforcement, the industry around law enforcement, brand protection and the domain name industry.

1. **WHOIS Policy (content owners: James Bladel, Kathy Kleiman)**
2. **History of Whois Policy and Thin/Thick Registries**

Upon its creation in 1998, ICANN undertook the management of several gTLDs, including .COM, .ORG and .NET. At the time, there was only one gTLD Registry, Network Solutions, for the top levels domains of .COM, .ORG and .NET, and it published a set of Whois data under a Whois technical protocol established by the Internet Engineering Task Force (and described in Section \_\_\_\_ earlier).

In April 1999, ICANN introduced competition into the gTLD market by creating ICANN-accredited registrars. These registrars had the right to register domain in the gTLDs, provided they signed contracts with both ICANN and the Registries. In 2000 when Verisign acquired Network Solutions and undertook the management of .COM, .ORG and .NET, competition was begining to grow in the registrar marketplace, and many more registrars were becoming accredited by ICANN. There were concerns that a competitive registrar environment could not flourish if the registry maintained a customer relationship with each and every registrant.

Accordingly, in 2000 [need to verify exact date of contract], Verisign agreed to adopt a “thin” Whois model for its Whois data. If queried on its website for Whois data of a particular domain name, it held and shared only minimal data:

* Provided only limited data (no specific contact data of registrant);
* Referred searchers to the Registrar;

Called a “Thin” Registry.

The number of registrars has now jumped to 944, in 2011, and registrations in the two largest gTLDs, .COM and .NET, remain “thin” with the customer data and contact information being held directly by the registrar.

In 2003, ICANN allowed competition applications to be submitted for .ORG, which it spun off of Verisign. The Public Interest Registry (“PIR”) won the contract for .ORG, and one of the conditions of the contract was that it become a “thick” registry, namely:

* Provide full Whois contact information for all registrants;
* Provide access to Whois data in online form and automated “Port 43” access (described below);
* Continue to all registrants to register domain names only through registrars.

Thus, with the advent of the .ORG “Thick” Registry, the full Whois data became findable in two locations: at the Registrar site and the Registry site.

Although some variations have taken place since 2003, all subsequent gTLD Registries have become “Thick” Registries, including .INFO, .BIZ, .NAME, .MOBI and .TEL. Further, ICANN's Applicant Guidebook for New gTLDs requires all future gTLDs Registries to adopt the "thick" model for Whois data.

Sample Registry Whois printouts

A Sample Thin Registry Printout – from the Verisign Whois website

 *Domain Name: IBM.COM*

 *Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE*

 *Whois Server: whois.melbourneit.com*

 *Referral URL: http://www.melbourneit.com*

 *Name Server: INTERNET-SERVER.ZURICH.IBM.COM*

 *Name Server: NS.ALMADEN.IBM.COM*

 *Name Server: NS.AUSTIN.IBM.COM*

 *Name Server: NS.WATSON.IBM.COM*

 *Status: clientTransferProhibited*

 *Updated Date: 31-aug-2011*

 *Creation Date: 19-mar-1986*

 *Expiration Date: 20-mar-2019*

*A Sample Thick Registry Printout – from the .INFO Website*

*Domain ID:D54632-LRMS
Domain Name:IBM.INFO
Created On:07-Aug-2001 20:13:19 UTC
Last Updated On:04-Jul-2011 22:31:42 UTC
Expiration Date:07-Aug-2012 20:13:19 UTC
Trademark Name:IBM
Trademark Date:1957-01-29
Trademark Country:US
Trademark Number:640606
Sponsoring Registrar:Melbourne IT Ltd. (R141-LRMS)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:C124680788152659
Registrant Name:International Business Machines Corporation
Registrant Organization:International Business Machines Corporation
Registrant Street1:New Orchard Road
Registrant Street2:attn Grace Micewicz
Registrant Street3:North Castle Drive
Registrant City:Armonk
Registrant State/Province:NY
Registrant Postal Code:10504
Registrant Country:US
Registrant Phone:            +1.9147654227
Registrant Phone Ext.:
Registrant FAX:+1.9147654370
Registrant FAX Ext.:
Registrant Email:**dnsadm@us.ibm.com* *Admin ID:A124680779471167
Admin Name:IBM DNS Admin
Admin Organization:IBM Corporation
Admin Street1:New Orchard Road
Admin Street2:
Admin Street3:
Admin City:Armonk
Admin State/Province:NY
Admin Postal Code:10504
Admin Country:US
Admin Phone:            +1.9147654227
Admin Phone Ext.:
Admin FAX:+1.9147654370
Admin FAX Ext.:
Admin Email:**dnsadm@us.ibm.com* *Billing ID:C124680788152658
Billing Name:Melbourne IT DBS*

*Billing Organization:Melbourne IT DBS Inc.
Billing Street1:487 East Middlefield Rd
Billing Street2:
Billing Street3:
Billing City:Mountain View
Billing State/Province:CA
Billing Postal Code:94043
Billing Country:US
Billing Phone:            +1.8669073267
Billing Phone Ext.:
Billing FAX:+1.6506182574
Billing FAX Ext.:
Billing Email:**billing@melbourneitdbs.com* *Tech ID:A124680779471168
Tech Name:IBM DNS Technical
Tech Organization:IBM Corporation
Tech Street1:New Orchard Road
Tech Street2:
Tech Street3:
Tech City:Armonk
Tech State/Province:NY
Tech Postal Code:10504
Tech Country:US
Tech Phone:            +1.9192544441
Tech Phone Ext.:
Tech FAX:+1.9147654370
Tech FAX Ext.:
Tech Email:**ipreg@us.ibm.com* *Name Server:NS.WATSON.IBM.COM
Name Server:NS.ALMADEN.IBM.COM*

1. **Background of Whois Policy and Registrars**

ICANN began accreditation of registrars in 1999, and this continues today. Over 944 registrars have become ICANN-accredited by completing an ICANN application and, where approved, signed a contract with ICANN called the Registrar Accreditation Agreement (RAA).

The RAA is not an individually negotiated contract and, at any given time, there is a standard contract registrars will be asked to sign. The RAA agreements tend to change and evolve according to the needs of the ICANN Community. Currently there are two RAA in force: 2001 and 2009. As registrar contracts expire and are renewed, all registrars will sign on to the 2009 agreement, and many of the largest registrars have already voluntarily done so already.

Both RAA agreements, 2001 and 2009, agreements require registrars to make available Whois data on their website for online searchers, and by “Port 43” automated access. For a registrant which is one of its own customers, a registrar Whois printout includes contact data:

A Sample Whois Registrar Printout for YAHOO.COM – from the MarkMonitor website at [www.markmonitor.com](http://www.markmonitor.com/)

 *Registrant:*

 *Domain Administrator*

 *Yahoo! Inc.*

 *701 First Avenue*

 *Sunnyvale CA 94089*

 *US*

 *domainadmin@yahoo-inc.com +1.4083493300 Fax: +1.4083493301*

 *Domain Name: yahoo.com*

 *Registrar Name: Markmonitor.com*

 *Registrar Whois: whois.markmonitor.com*

 *Registrar Homepage: http://www.markmonitor.com*

 *Administrative Contact:*

 *Domain Administrator*

 *Yahoo! Inc.*

 *701 First Avenue*

 *Sunnyvale CA 94089*

 *US*

 *domainadmin@yahoo-inc.com +1.4083493300 Fax: +1.4083493301*

 *Technical Contact, Zone Contact:*

 *Domain Administrator*

 *Yahoo! Inc.*

 *701 First Avenue*

 *Sunnyvale CA 94089*

 *US*

 *domainadmin@yahoo-inc.com +1.4083493300 Fax: +1.4083493301*

 *Created on..............: 1995-01-18.*

 *Expires on..............: 2012-01-18.*

 *Record last updated on..: 2011-10-16.*

 *Domain servers in listed order:*

 *ns2.yahoo.com*

 *ns4.yahoo.com*

 *ns5.yahoo.com*

 *ns1.yahoo.com*

 *ns3.yahoo.com*

1. **Quick Timeline**

Description of Diagram: One Long Timeline Arrow Across the page (===>) and the following dates marked beneath it:

1998, ICANN created; 1999 ICANN-accredits first competitive registrars (4);2000 Verisign purchases Network Solutions and agrees to allow registrars to hold their own customer Whois Data (Verisign becomes a Thin Registry); 2001 RAA created and signed; 2003 .ORG becomes a Thick Registry; 2009 New RAA created and signed; 2011 New gTLD Applicant Guidebook created mandating that all New gTLD registrie will be Thick Registries

1. **Goals of this Chapter**

The Affirmation of Commitments tasks the Review Team to ensure that ICANN is “enforcing its existing policy with respect to WHOIS, subject to applicable laws.”1 Thus, as a starting point, the Review Team must set out what it believes the existing Whois policy to be.

The purpose of this chapter is to examine the existing policy to:

* See where it can be found;
* Review its policy provisions, particularly for the requirements of ACCESS TO and ACCURACY OF Whois data; and
* Evaluate successes and shortcomings in ways ICANN Whois policy is set out, e.g., are the requirements clearly defined? Are they consistent?
1. **Key Components of WHOIS Policy**

For the purposes of the Whois Review Team assessment, there are two key areas of Whois policy that are important, namely, ACCESS to the WHOIS service, including method of use and availability of the Whois data, and ACCURACY of the WHOIS data. For the most part, current contractual obligations for Whois are a manifestation of one or both of these components.

Footnote: There are a few additional provisions regarding escrow (storage of the data for availability in the event a registry or registrar is unable to perform its functions), and will only be addressed lightly in this chapter.

1. **ACCESS For Registries**

As discussed above, thick and thin registries have differing obligations regarding making Whois data available. In particular, Thick Registries must provide WHOIS data to searchers via realtime web access, and bulk automated access via server Port 43.

The Port 43 server enables automated access by software tools to the Whois data. Under certain circumstances, registrars must provide third-party bulk access to Whois data. Other obligations require registries to ensure that the data is not misused.

Each Registry, to date, has negotiated a separate contract with ICANN. All of these contracts are posted on the ICANN website at [www.icann.org/en/registries/agreements.htm](http://www.icann.org/en/registries/agreements.htm).

All registries have a section labeled “Whois Specifications,” and they are largely similar. For the thick registries of .INFO, .BIZ, .ORG, etc., the contracts require that:

“Registry Operator’s Whois service is the authoritative Whois service for all second-level Internet domain names registered in the (dot).INFO top-level domain and for all hosts registered using these names. This service shall be available to anyone. It shall be available via port 43 access and via links at the Registry Operator’s web site.... Registry Operator’s Whois service will be updated on a near real-time basis... The Whois servers shall provide results in ASCII for standard and IDN .info domains. INFO Agreement Appendix 5

As the growing internationalization of the domain name space takes place, and an increasing number of non-ASCII scripts come online, the underlying data of a Whois registration may be in a different language and character set. The IDN requirement sets out that: *The Registry Whois server must provide results for both ASCII domain names and Internationalized Domain Name (IDN), although the latter may be expressed in an ASCII representation.*

1. **Limitations for ACCESS of Registry Whois data**

Through the bottom-up, policy-making process, the GNSO created a few restrictions to access of Whois data, which was originally unlimited. Specifically, the GNSO Council voted that Registries and Registrars not be permitted to allow Whois data to be used for mass-marketing or other high volume automated systems. This policy recommendation was adopted by the ICANN Board in 2004, and accordingly, all Thick Registries now have, as part of their Whois obligations a requirement for detection and limitation of abusive usage of the Whois:

“Provisions for the detection of abusive usage of Registry Operator’s Whois system (e.g., excessive numbers of queries from one source), and corresponding protective measures, have been implemented, and Registry Operator may implement further countermeasures against abuse as necessary.” INFO Agreement, Appendix 5, Section 1.

1. **Specific Restriction on ACCESS to Registry Whois data based on nature of the gTLD**

Two registries have requested, and received, changes to the ICANN Whois data access system, specifically .TEL and .NAME. [additional details to follow]

1. **ACCESS for Registrars**

Registrars, within the ICANN context, are the parties who have the right to sell domain names directly to the general public. Specifically:

1.11 "Registrar Services" means services provided by a registrar in connection with a TLD as to which it has an agreement with the TLD's Registry Operator, and includes contracting with Registered Name Holders, collecting registration data about the Registered Name Holders, and submitting registration information for entry in the Registry Database.

Both 2001 and 2009 Registrars Accreditation Agreements.

Registrars have an obligation to collect registrant Whois data, and to make it available both on a webpage and via the automated “Port 43” service. The language of the two RAA versions is identical:

At its expense, Registrar shall provide an interactive web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar for each TLD in which it is accredited. The data accessible shall consist of elements that are designated from time to time according to an ICANN adopted specification or policy. Until ICANN otherwise specifies by means of an ICANN adopted specification or policy, this data shall consist of the following elements as contained in Registrar's database:

2001 and 2009 RAA, both Section 3.3.1

Both set out the same requirements for data elements of the Registrar's database:

3.3.1.1 The name of the Registered Name

3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);

3.3.1.4 The original creation date of the registration;

3.3.1.5 The expiration date of the registration;

3.3.1.6 The name and postal address of the Registered Name Holder;

3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and

3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.”

2001 and 2009 RAA, both Sections 3.3.1.1-3.3.1.8

Both note that the requirements of a specific Top Level Domain Registry may differ, and that the Registrar will respond accordingly:

The appendix to this Agreement for a particular TLD may state substitute language for Subsections 3.3.1.1 through 3.3.1.8 as applicable to that TLD; in that event the substitute language shall replace and supersede Subsections 3.3.1.1 through 3.3.1.8 stated above for all purposes under this Agreement but only with respect to that particular TLD.

2001 and 2009 RAA, both closing language of 3.3.1

Both include a requirement that Registrars must provide “third-party bulk access” to the Whois Data:

Registrar shall make a complete electronic copy of the data available at least one time per week for download by third parties who have entered into a bulk access agreement with Registrar.

Registrar may charge an annual fee, not to exceed US$10,000, for such bulk access to the data.

2001 and 2009 RAA, both closing language of 3.3.6

1. **Limitations**

In both RAA contracts, Registrars agree to restrict third parties from selling or redistributing Registrar's Whois data:

“Unless and until ICANN establishes a different policy according to Section 4, Registrar shall permit use of data it provides in response to queries for any lawful purposes except to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass, unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.” 2001 RAA, Section 3.3.5. [emphasis added]

2001 and 2009 RAA, both Section 3.3.5

Further, other limitations may be added by the Registrar:

Registrar's access agreement may require the third party to agree not to sell or redistribute the data except insofar as it has been incorporated by the third party into a value-added product or service that does not permit the extraction of a substantial portion of the bulk data from the value-added product or service for use by other parties.

2001 and 2009 RAA, both Section 3.3.6.5

1. **Subject to ICANN Consensus Policies**

Both agreements note that the Registrar must abide by future ICANN Consensus Policies as they may apply to Whois data:

Registrar shall abide by any ICANN specification or policy established as a Consensus Policy according to Section 4 that requires registrars to cooperatively implement a distributed capability that provides query-based Whois search functionality across all registrars. If the Whois service implemented by registrars does not in a reasonable time provide reasonably robust, reliable, and convenient access to accurate and up-to-date data, the Registrar shall abide by any ICANN specification or policy established as a Consensus Policy according to Section 4 requiring Registrar, if reasonably determined by ICANN to be necessary (considering such possibilities as remedial action by specific registrars), to supply data from Registrar's database to facilitate the development of a centralized Whois database for the purpose of providing comprehensive Registrar Whois search capability.

Both 2001 and 2009 RAA, Section 3.3.4

[NOTE TO REVIEW TEAM MEMBERS: THIS IS THE END OF THE NEWLY-REVISED SECTION OF THIS REPORT. IT INCORPORATES REQUESTS OF THE TEAM FOR ADDING HISTORY, TIMELINE, MORE DISCUSSION AND DIFFERENTIATION OF THICK AND THIN WHOIS, SCREENSHOTS OF THICK AND THIN REGISTRY WHOIS AS WELL AS REGISTRAR WHOIS DATA.

IF YOU LIKE THIS APPROACH, WE WILL CONTINUE AND REVISE THE “ACCURACY” SECTION ACCORDINGLY.

COMMENTS WELCOME!

JAMES AND KATHY

1. **Component: ACCURACY**

ICANN require its accredited Registrars to maintain specific data (RAA Sec. 3.4.1), to retain this data for three (3) years (RAA Sec. 3.4.2) and to make it available to ICANN for inspection (RAA Sec. 3.4.3). The Registrar must periodically submit the data to a third-party Data Escrow service (RAA Sec. 3.6).

Additionally, ICANN establishes that the Registrant of the domain name is ultimately responsible for WHOIS data accuracy (RAA Sec. 3.7.7.1) and that providing or failure to correct inaccurate or unreliable information can mean the loss of the domain name registration (RAA Sec. 3.7.7.2).

Registrars agree to promptly investigate any reports of inaccurate or incomplete WHOIS data (RAA Sec. 3.7.8), submitted via ICANN’s WHOIS Data Problem Reporting System (WDPRS) or to the Registrar Directly.

Finally, Registrars are required to remind Registrants to view and (if necessary) update their WHOIS data at least annually, via the WHOIS Data Reminder Policy (WDRP)5 and promptly submit contact updates to the Thick Registries (RAA Sec. 3.3.2).

Similarly, Registry Agreement require that “Registry Operator's Whois service will be updated on a near real-time basis” to pass on any changes they receive to the community as quickly as possible.

1. **Component: AVAILABILITY**
2. **Consensus Policies**

In addition to the “static contracts,” such as the Registrar Accreditation Agreement (RAA)2, gTLD Contracted Parties are also obligated to comply with “Consensus Policies,” created by the GNSO pursuant to the bottom-up, policy-making process of the GNSO (called the “Policy Development Process” and adopted by the ICANN Board after notice, comment, discussion and a Council vote. The policy process is set out in the ICANN Bylaws (Annex A defines the GNSO process). [keep]3

There have been three (four?) Consensus Procedures adopted by the GNSO to date:

Registrar Data Escrow Program, referenced above as RAA 2009 Section ?

Whois Data Reminder Policy (effective 31 October 2003) reminds registrants of their obligation, and gives them an opportunity to update their Whois data elements as needed, e.g., a changed phone number or address.

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 inquiries, also intended to improve Whois accuracy (effective date 12 November 2004)” [provided by Liz Gasster]

In compliance with these Consensus Policy, as required by ICANN Bylaws, ICANN has made changes and revisions to the RAA and Registry Agreement, many adopted as entities join and renew with ICANN.

1. **Compliance**

Upon adoption of a Policy obligation, either through the original Contract or a new Consensus Policy, responsibility for enforcement then falls to ICANN Compliance. Depending upon the nature of the obligation, Compliance will create an ongoing programmatic monitoring scheme, or conduct periodic audits of Contracted Party data or practices. In some cases, Compliance may initiate an investigation in response to complaints by another Contracted Party or from the public.

1. **Policy Gaps**

**β**

**α**

An analysis of these overlapping principles yields two potential Gap Classes:

**α Gap**: A material difference between ICANN contractual requirements and its enforcement activities.

**β Gap**: A material difference between ICANN’s commitment in the AoC and its commitments in the Registrar and Registry contracts, as well as consensus policies.

**α Gap**

Looking at the material difference between ICANN contractual requirements and consensus policies, and ICANN's enforcement activities is an important evaluation area of the Whois Review Team.

[Lots of area for work and recommendations here; I think we are working on this area on Monday in MDR for all who come early.]

**β Gap**

Evaluating key difference between ICANN’s commitment in the AoC and its commitments in the Registrar and Registry contracts, as well as consensus policies, if any, is also an area in which the Whois Review Team has spent some time (as have those who commented to us).

[still room for some analysis here... ]

It should be emphasized that the AoC is not a Policy document, and does not define WHOIS Policy. Rather, ICANN implements WHOIS policy in gTLDs via its contracts with Registries and Registrars, and Consensus Policies. Only when these obligations are accepted in to the contracts can ICANN Compliance enforce them.

[I flipped alpha and beta above, but not yet below]

Plus a theoretical4 Gap class:

**γ Gap**: A conflict between the AoC and ICANN Contracts.

If they are found to exist, Gap Class (β) ICANN Staff (esp. the Compliance team) can take action to address them. This could entail a new or modified Compliance program that targets the Gap, with the aim of aligning enforcement activities with the obligations of contracted parties.

Gaps Class (α), however, can only be addressed via the Policy Development Process (PDP) as defined in Annexes A (GNSO) and B (ccNSO) of the ICANN Bylaws. ICANN Compliance does not have the ability to enforce the Affirmation of Commitments, because it is not an expression of WHOIS Policy.

Finally, Gap Class (γ) presents a particular challenge. It indicates an area where the language of the Affirmation of Commitments conflicts (or is perceived to conflict) with language of a Policy obligation. It is possible that at least one such Gap Class (γ) currently exists, specifically with regard to the AoC’s claim of “unrestricted and public” WHOIS access, while ICANN’s contracts allow for some restrictions and terms of data use.

Also did we want to keep the other table in the references? :

Items to include in later draft:

The downside of the "thin" model, as seen with some failed registrars, is that Registrar WHOIS systems may contain invalid or out of date data.  Although this could easily happen under both "thin" and "thick" models, it presents a challenge when dealing with a distributed registrar WHOIS system, versus a centralized registry WHOIS system.

1. **Implementation: ICANN’s compliance effort**
2. **Implementation**

*[****NB – In Dakar, I think we agreed to include here:***

* ***policy as implemented in the registry/registrar contracts (James/Kathy’s section)***
* ***some high level comments on compliance***
1. **The components of implementation**

The term implementation covers a number of aspects which are dealt with below. Implementation involves both contracted parties and the wider population of Internet users.

The WHOIS Review Team considers that key elements of successful policy implementation are promoting awareness, the effective communication of policies, fostering a “culture of compliance”[[7]](#footnote-7) and effective enforcement of contractual provisions.

In this report, the term “compliance” is has a wider meaning than “enforcement”. The WHOIS RT’s view is that ICANN should encourage compliance through education, awareness raising and communication. The term compliance is proactive in nature, and involves all parties (ICANN, registries, registrars, registrants and Internet users), acting cooperatively to achieve shared policy goals. In contrast, “enforcement” is a narrower concept, and refers specifically to how the legal obligations of ICANN and its contracted parties, the registries and registrars, are monitored and followed up.

1. **ICANN’s Compliant effort**

The WHOIS Review Team has had extensive contact with ICANN’s compliance team throughout 2011. Having conducted an in-depth review of the Compliance Team’s webpages and their WHOIS related work, the WHOIS Review Team wrote a letter to the Compliance Team (see Appendix [ ] to this report), which sets out the Review Team’s detailed observations, and some suggested improvements, which do not have the status of recommendations to this report, but are offered in a spirit of collaboration.

In general, the WHOIS Review Team’s observations of ICANN’s WHOIS Compliance efforts can be summarized as follows:

* Conducting audits
* Investigating complaints of non-compliance
* Escalating cases where informal efforts to bring parties into compliance have failed.

These have had mixed results (see Appendix for further detail). Key observations for the future include:

* The Compliance Team has developed a set of operating principles, which in the WHOIS Review Team’s opinion provide a useful framework for organizing, and communicating the Compliance Team’s actions.
* The Compliance Team has to date been inadequately resourced. Open positions have remained vacant for long periods. Recent strengthening of the Team is welcome. This needs to be followed by the publication of plans for measurable, targeted improvements.
* Given that demand will always exceed available resources, the compliance effort must be strategic focus on achieving measurable, stated objectives, and should be proactive rather than reactive.

One of the key challenges facing the Compliance Team is the lack of clarity as to who “owns” WHOIS as an issue, where responsibility lies within the organisation. The fact that policy is made by the GNSO is a feature of the ICANN environment. However, there appears to be a disconnect in determining how, or whether to follow-up, on the numerous studies which have been commissioned (eg Data Accuracy, WHOIS abuse and others).

In the WHOIS Review Team’s view, this is an issue which requires resolution in order to improve the effectiveness of ICANN’s Compliance effort, and to avoid waste.

1. **Gap Analysis (content owner: Peter Nettlefold & Emily Taylor [Compliance gaps])**

**This chapter examines gaps between ICANN’s policies and their implementation, and between ICANN and its contracted parties’ respective commitments and the services they actually deliver.**

**Consistent with the review team’s scope, the chapter focuses on the extent to which existing WHOIS policy and its implementation is effective, meets the legitimate needs of law enforcement, and promotes consumer trust.**

**The chapter covers three broad areas:**

1. **WHOIS data accuracy**
2. **Data accessibility and privacy**
3. **The roles and responsibilities of contracted parties**
4. **Compliance gaps**
5. **WHOIS data accuracy**
6. **ICANN’s commitment to WHOIS data accuracy**

**The Affirmation of Commitments provides that** ICANN will implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information**. ICANN has two consensus policies that address WHOIS accuracy. To varying degrees, the commitment to accuracy is also echoed in the contractual commitments of registries, registrars and registrants.**

**[Details of these policies and contractual provisions are at sections xx of this report.]**

1. **Concerns about WHOIS data accuracy**

In January 2010, ICANN published a study conducted by the National Opinion Research Council of the University of Chicago (NORC) that had been commissioned by ICANN to obtain a baseline measurement of what proportion of WHOIS records are accurate. Examining an internationally representative sample of 1419 records, NORC found that, based on a strict application of the criteria, only 23% of records were fully accurate, though roughly twice that number met a slightly relaxed version of the criteria. The study also found that 21.6% of data was not sufficient for the registrant to be located, with either missing or deliberately false information.

Concerns about the accuracy of WHOIS records was raised in a number of responses to the WHOIS review team’s public Discussion Paper. A number of law enforcement agencies expressed a view that inaccurate or incomplete WHOIS data can potentially cause serious problems during the course of a criminal investigation. For example, one law enforcement agency stated that:

Accurate WHOIS data is a very important tool for law enforcement but false, out-of-date and inaccurate records are a barrier towards successful criminal investigations. WHOIS data is often the only way law enforcement agencies can investigate criminal offences that occur via the internet so it is therefore vital the data is accessible and accurate.

On the importance of accurate WHOIS data another law enforcement agency stated:

The WHOIS database contains many inaccuracies. Presently there is insufficient due diligence conducted towards ensuring records are accurate and criminals are quick to take advantage of this. The value of any database is in its accuracy.

Inaccurate WHOIS data can also significantly impact businesses and consumers. For example, Time Warner International argued that:

Inaccurate data 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.*[[8]](#footnote-8)*

The concerns of businesses include issues relating to online counterfeiting and their ability to protect their intellectual property rights. For example, the International Anti-Counterfeiting Coalition stated that:

Years of experience with WHOIS since ICANN assumed custody over its management and operation has clearly demonstrated that the unscrupulous Internet users who are willing to infringe the intellectual property rights of others are also among the first to disregard their contractual obligations to provide true and accurate WHOIS contact data.

Consumers could also benefit from accurate WHOIS data to establish the legitimacy of online traders. For example, the Intercontinental Hotels Group stated that:

Complete and accurate WHOIS data also provides a level of consumer confidence when conducting business online. Having a failsafe avenue to contact administrators should all other extensions fail, could increase individual propensity to partake in online activities and transactions.

**In regards to the importance of accurate WHOIS data being available without restriction a law enforcement agency argued that it:**

“…allows internet users to know who they are dealing with and create a level of trust online transacting and searching. It is a thin layer of protection for the average internet user.”

**Concerns about the accuracy WHOIS data have also been raised previously by the Government Advisory Committee (GAC). In March 2007, the GAC presented ICANN with a series of principles regarding gTLD WHOIS services. Among other things, the GAC recommended that:**

“,,. stakeholders should work to improve the accuracy of WHOIS data, and in particular, to reduce the incidence of deliberately false WHOIS data.”[[9]](#footnote-9)

In its Singapore Communiqué, the GAC emphasised “the need for effective compliance activities, noting that legitimate users of WHOIS data are negatively affected by non-compliance.”

Some stakeholders argued that there is an urgent need to address the issue of inaccuracy in WHOIS data. For example, the Canadian Internet Registration Authority argued that:

Addressing the accuracy and completeness of WHOIS will require a large amount of work; however, the longer it is left and not addressed, the worse the problem will become and the harder it will be to implement solutions as during that time, the volume of inaccurate WHOIS information will become larger.[[10]](#footnote-10)

In their 2009 study, the National Opinion Research Council of the University of Chicago (NORC) found that there are various “barriers to accuracy” from the point of data entry onwards with the combined involvement of registrants, registrars, registries and ICANN itself. The following analysis focuses on the individual roles of these actors, and the chain of responsibilities between them.

1. **Role of ICANN**

The effectiveness of ICANN’s current compliance activities to ensure access to accurate and complete WHOIS data was questioned in numerous submissions to the review team’s public Discussion Paper, and in responses to the law enforcement questionnaire. For example, in response to the discussion paper, the China Internet Network Information Center stated that:

ICANN to some extent has failed to regulate .com and .net in terms of maintaining accurate WHOIS information. Therefore, we suggest that ICANN has neither been effective at developing WHOIS policies nor well regulating registrars in terms of helping improve WHOIS accuracy.[[11]](#footnote-11)

**Additionally, the Intercontinental Hotels Group stated that:**

ICANN should carry through on its commitment to provide open access to reliably accurate registrant information, as this information is essential to maintain the integrity of the internet itself. The proliferation of false WHOIS data undermines ICANN’s legitimacy and allows cyber squatters and others to increase their misleading and damaging activities online.

**The Intellectual Property Constituency also raised concerns about ICANN’s current approach to WHOIS accuracy compliance, especially in light on the new unlimited Top Level Domains becoming available, and stated:**

The 2010 the National Opinion Research Council of the University of Chicago (NORC) study demonstrated that the WHOIS data for only 23% of gTLD registrations is fully compliant with accuracy requirements. Thus, the facts support the conclusion that the current compliance related activities are woefully inadequate to fulfil ICANN’s commitment in article 9.3.1 of the AOC to “implement measures to maintain timely unrestricted and public access to accurate and complete WHOIS information.” Although some progress has been made in upgrading ICANN’s contract compliance function, a radical change in approach is needed, especially in light of the impending proliferation of new unlimited Top Level Domains.

**At the 2011 Singapore meeting, a participant of the Commercial Stakeholder Group argued that:**

The reality is there are contractual obligations that clearly set out what registries and/or registrars have to apply or provide on a query and whether they're complying with that. In the situations where ICANN has enforced the contracts, and there have been some, not just on WHOIS issues, it seems to have worked very effectively. The question is: is ICANN actually taking actions? Concerned about resources (staff and funding) to continue and do the auditing needed to take action. This is an organization whose private regulatory ability is based completely and solely on contracts. Unless you enforce the contracts, you have absolutely no ability to self regulate.

**A number of law enforcement agencies also expressed concern with the performance of ICANN in ensuring the WHOIS service is accurate, with one agency stating that:**

Since WHOIS is regularly incomplete, inaccurate and non-public, ICANN is not fully performing its duties. In addition, the continued issue of not being able to quickly identify the true owner of a domain name, indicates a need for improvement in this area.

Another law enforcement agency stated:

“ICANN should enforce its own contractual obligations with registrars, require that registrars, registries and resellers, collect and verify the appropriate WHOIS information. ICANN needs to increase staff levels if there is any hope that compliance can be enforced.”

Additionally, **at the 2011 Singapore meeting** Mark Carvell from the Government Advisory Committee stated:

“A lot of this problem would be solved by the validation of the registration information at the time of the registration and periodically audited throughout. That was a big issue that we spoke with the registrars about, stating that that’s something that we need to look at that would be a difficult issue.”

ICANN has sought to improve the accuracy of WHOIS data in several ways. At the registry level, ICANN has imposed contractual obligations that flow through registries to registrars in three of ICANN’s registry agreements, namely .mobi, .tel and .asia[[12]](#footnote-12). [Is there any data on WHOIS accuracy levels in these TLDs?]

ICANN also plans to implement a more comprehensive evaluation process for gTLD applicants, which includes an assessment of the applicant’s ability to maintain a higher standard of WHOIS data accuracy. Improved accuracy in WHOIS data will be actively promoted by ICANN throughout the evaluation and selection process so that applicants will be motivated to improve accuracy standards in their bid for a new gTLD.[[13]](#footnote-13)

In response to questions from the review team, ICANN’s compliance team stated that ICANN is continuously assessing and enhancing its WHOIS compliance program, and that key improvements undertaken and under consideration by ICANN include:

* Providing a mechanism for greater transparency and communication with registrars concerning how they investigate each alleged WHOIS inaccuracy report.
* Considering potential amendments to the RAA, including trying to achieve more clarity around the RAA contractual provisions 3.3 and 3.7.8 to help provide certainty and predictability for compliance enforcement purposes.
* Continuously improving all aspects of ICANN’s WHOIS compliance program including audits and investigation processes and well as enhancing systems and tools.
* Considering additional registrar training and enhanced registrant awareness through registrant targeted initiatives and how-to documents to improve WHOIS accuracy.
* Considering having registrant WHOIS changes tracked for a certain period of time after registrants receive WHOIS data reminder policy (WDRP) notices; this might give ICANN and the community data regarding whether an appreciable number of WHOIS changes are made as a result of registrants receiving WDRP notices and whether the WDRP is serving its intended purpose.

A number of respondents believe that the accuracy of the WHOIS service can be improved by amending the RAA to give ICANN greater and more enforceable powers. The International Anti-Counterfeiting Coalition has argued:

ICANN must amend the RAA ... The amendments should clarify responsibilities of both ICANN and registrar with respect to the operation of a transparent and accurate WHOIS system accessible to the broader internet community and should provide clear tools available to ICANN which are both reasonable and meaningful in the event of non-compliance. ICANN should commit greater resources to compliance and ensure that those resources are deployed to increase accuracy and reliability of WHOIS data.

In addition to regulatory compliance activities, several respondents to the public Discussion Paper suggested that ICANN should play a greater role in education and awareness raising, and ensure that all parties are aware of their obligations and are required to comply with these policies. For example, the International Trademark Association-Internet Committee stated:

“ICANN should clarify its existing WHOIS policy by taking measures to inform and educate the public and its business partners, such as its registrars and registries, on the

importance of the WHOIS policy and of complying with its terms.”

In order to measure the success of any new compliance activities, it has been suggested by the Business Constituency that:

Huge compliance resources are needed to fix this situation and the matter of WHOIS accuracy only becomes more urgent with ICANN’s planned rollout of hundreds of new gTLDs. ICANN’s compliance organization has already been made aware from its own work.......of continuing frauds and abuses in the WHOIS space. As part of the AoC, ICANN’s continued performance in the compliance area should be carefully measured to assess whether it is meeting its WHOIS commitments.

The importance of data on accuracy levels was raised by William Dee from the Government Advisory Committee **at the 2011 Singapore meeting:**

We know that law enforcement are unhappy with the current compliance policies and we know there’s problems with data accuracy. It would be interesting to have the number of complaints received, interventions, correction actions and de-accreditations for non-compliance. Then evaluate how effective the compliance policy is. The GAC has not been provided with this information yet.

1. **Role of Registries and Registrars**

Registries and registrars play a key role in ensuring the accuracy of WHOIS data because they are the parties responsible for collecting WHOIS data from registrants and ensuring that the data is available. However, several respondents to the public Discussion Paper argued that ICANN’s current contracts and policies do not require registries and registrars to actively ensure WHOIS data accuracy. For example, INTA argued that:

At present there are no mechanisms in place to ensure the accuracy of WHOIS information provided by registrants. Instead there is a presumption by registries and registrars that WHOIS information provided by registrants is accurate and a lack of incentives to encourage registrants to refrain from providing misleading or inaccurate information.

[As noted in section xx of this report], there are currently no requirements for registrars or registries to pro-actively monitor or verify registration data for accuracy. If a registrar is notified of an inaccuracy in data, RAA 3.7.8 provides that the registrar will take reasonable steps to investigate the claim of inaccuracy and correct the information if needed. If data is found to be intentionally false registrars are not obligated to cancel the registration. This point is echoed by WHOIS compliance staff, who stated in response to the Review Team's questions that:

currently the RAA requires registrars to investigate alleged WHOIS inaccuracies but there is no requirement in the RAA for registrars to ensure that WHOIS data is accurate.

Several respondents to the public Discussion Paper raised concerns about the lack of clear and enforceable provisions in the RAA. For example, the Business Constituency argued that:

Registrar’s obligation to provide accurate WHOIS data is ... subject to loose contractual language and vague promises to comply with future ICANN policies. The absence of clear contractual obligations regarding WHOIS accuracy stands in strong contrast to ICANN’s clear obligations to provide accurate WHOIS in the AoC.

At the meeting with the **Commercial Stakeholder Group in Singapore,** Mike Rodenbaugh argued that:

Overall the WHOIS general policy (requirement to have accurate WHOIS information) has proved to be unenforceable essentially. ICANN gets thousands of complaints a month, basically showing false WHOIS and those reports generally go into a black hole 99% of the time. It takes months and sometimes never to get a response from ICANN. And the reason is because there is no, there are no firm commitments on registrars or registries as to responding to those requests. So ICANN kind of does its best, it forwards off the complaint to the registrar and registry, but there's no obligation on the registrar or registry really to do anything.

Time Warner International stated that it is:

*‘*not surprising that this system produces unacceptably high levels of inaccurate data’*.*[[14]](#footnote-14)

[content on registry provisions, and input from the compliance team that ICANN does no compliance work with registries?]

[content on thick/thin WHOIS from Susan here, or elsewhere?]

In order to ensure the WHOIS information collected from registrants is accurate, several respondents to the public discussion paper argued that registrars should be obliged to verify data provided to them during the registration process. A similar principle could also apply to registries. For example, the Coalition of Online Accountability argued that:

The current intolerable levels of inaccurate WHOIS data flow directly from ICANN’s decision to place virtually sole responsibility for WHOIS data quality on a party with whom it has no contractual relationship: the registrant. Registrars insist that their only contractual obligation is to respond to reports of false WHOIS data, rather than to verify data accuracy at the time of collection or even to cancel registrations based on false WHOIS data. The largest registries have even less role to play on WHOIS data quality currently. This problem will not be solved or even ameliorated until registries and registrars both share responsibility for WHOIS data quality.

Additionally, the Intellectual Property Constituency provided:

There is a need to develop policies that provide for proactive registrar compliance and provide for consequences associated with inaccurate data.

Further, the Intercontinental Hotels Group argued that:

ICANN should require that registrars actually confirm the WHOIS data provided by registrants and not merely allow registrars to blindly accept any data provided by registrants with a meaningless and unenforceable reminder to registrants that accuracy is required.

Some organisations have already improved accuracy levels through implementing a verification process. The China Internet Network Information Center reported that since the organisation began verifying data provided to them, accuracy levels of .cn have reached 97 per cent[[15]](#footnote-15).

Many of the proposals to improve accuracy put forward in responses to the public Discussion Paper would require the implementation of new procedures by registries or registrars, and could increase their costs. The National Opinion Research Council of the University of Chicago (NORC) report concluded that:

the cost of ensuring accuracy will escalate with the level of accuracy sought, and ultimately the cost of increased accuracy would be passed through to the registrants in the fees they pay to register a domain.

In relation to this, Christopher Wilkinson noted the following:

Registrars have long asserted that full verification of the accuracy of all records, including what by now must be a considerable backlog, would be financially unsustainable.[[16]](#footnote-16)

Several respondents to the public Discussion Paper argued that some increase in costs would be inevitable. For example, the Intellectual Property Constituency argued that:

The costs incurred by registrars or registries to comply with reasonable WHOIS accuracy and accessibility requirements are simply the costs of doing business as responsible players in a way that enhances consumer trust and the global public interest.

Cooperation among all registrants and other ICANN constituents will be needed to eliminate any commercial disadvantage accruing from enforcing greater accuracy.

Similarly, INTA argued that:

Consideration should be given to the implementation of a validation process funded by additional fees (validation fees) paid by registrants at the time of registration as well as penalties, such as loss of the registration if information is found to be inaccurate in the validation process.

This view was supported by participants in the **Commercial Stakeholder Group at the 2011 Singapore meeting:**

Registrars have tremendous market pressures: very low margin business, no upfront costs (consolidation is obviously an upfront cost). If, however, that cost is forced upon them, I think everyone in this room would be perfectly happy to pay more money for domain names and have that validation done. Nobody in here believes there's a God given right to a $10 domain name, yet everybody in the registrar and registry constituency believes there is and they can't sell them if they have to charge more than that. Well if they all have to charge more than that, then that seems to me, and I think to most folks in this room, it would go a long way towards solving the problem.

In the meeting with the At-Large Advisory Committee in Singapore, Cheryl Langdon-Orr argued that:

Many of us at the consumer interest end and the user end of the spectrum know who’s going to bear the costs under normal circumstances and that will be us because costs will be passed on. If they are not passed on there is probably a good market differentiation reason for them not to be passed on, and it will probably mean that we are buying other services at greater costs from our suppliers to compensate for that anyway. Many of us have no choice, and the difference between $7.50 or $11.00 is virtually nothing when we are simply wanting to get our name registered, licensed and safe for whatever period of time we’re purchasing it for.

Some respondents to the public Discussion Paper argued that relevant precedents for this type of verification exist, and that ICANN could leverage or adapt these processes for WHOIS purposes. For example, the Business Constituency argued that:

The RAA should be amended to require contracted parties to take reasonable steps to verify the accuracy of WHOIS information when a registration first occurs and when a registrant renews their domain name. ICANN can look to best practices from other industries, including the financial sector and e-Commerce industries, which have employed successful online data verification systems to ensure the accuracy of information and to prevent fraud and abused. After all, processes to gather accurate information are already undertaken by Registrars in the collection of credit card and other form as of payment. Valid WHOIS data should not be an exception and should be a prerequisite to complete the registration of a domain name.

This view was supported by J. Scott Evans, in the meeting with the **Commercial Stakeholder Group in Singapore:**

They [registrars] are getting paid and I don't understand why the information that they so accurately rely on to make sure they keep the domains active, they can't use the same technology to make sure that the information is accurate. I think they know how to get it but just don’t want to. Because in many instances, bad actors own a lot of domain names and they want to go to those areas where it's easier for them to perpetrate their bad acts because they can hide.

With regard to serious breaches of WHOIS obligations, the Intercontinental Hotel Group stated:

Compliance with WHOIS data reporting should continue to be compulsory and included in the Registrar Accreditation Agreement. Noncompliance should be met with a stern enforcement mechanism, including severe monetary fines. ... The most severe repercussions should be reserved for those registrar organizations who intentionally disregard WHOIS policy, and profit as a result of illegal and unethical registrations of individuals registering with them.

1. **Role of Registrants**

Sections 3.7.7.1 and 3.7.7.2 of the RAA outline the contractual responsibility of the registered name holder to provide accurate and up-to-date personal information to the registrar, and that they must notify the registrar if information needs updating. Despite these obligations, many registrants do not provide accurate personal information or keep this information up-to-date.

The 2009 National Opinion Research Council of the University of Chicago (NORC) found that one reason why registrants do not provide accurate information may be due to a lack of understanding of the purpose and uses of the WHOIS service[[17]](#footnote-17). During their 2009 study, NORC found that of registrants that could be found, many admitted to error on their behalf and did not realise that accurate WHOIS data was a valuable asset for the internet community in general. The study also found that many registrants were confused by the forms they were required to complete during the registration process, mainly due to terminology used or difficulties in translating text.

Several respondents to the public Discussion Paper argued that ICANN should be proactive in educating registrants on the purpose of the WHOIS service and their obligations to provide accurate information.

[need to insert supporting quotes here]

This view was also supported by participants in the **Commercial Stakeholder Group at the 2011 Singapore meeting:**

ICANN needs to do a better job of educating everybody in a uniform way about what the WHOIS commitments are. It needs to be clear, easy to understand, easy to find, consistent material that is provided to registrants....The lack of clear communication is still a problem today. The registrant needs to be advised of their obligation and of the consequences. ICANN needs a lot more willingness to accept the fact it has that obligation.

In response to questions from the review team, ICANN’s compliance team stated that:

Time and resources are the two most often cited challenges for registrars in complying with WHOIS. Some registrars have indicated that the cost and time of initial and ongoing verification of WHOIS data is burdensome.

Challenges inherent in achieving WHOIS compliance with regard to registrants seem to generally revolve around privacy concerns or a lack of due diligence. Some registrants have expressed concerns about making their contact information publicly available and fail to provide complete, accurate information. Some registrants inadvertently provide incorrect contact data in the WHOIS fields, or fail to maintain correct data, due to carelessness.

The  [National Opinion Research Council of the University of Chicago (NORC) report](http://www.icann.org/en/announcements/announcement-3-15feb10-en.htm) found that because no proof of identity or address is required when registering a domain name, this removes many barriers to entering inaccurate information. The report also notes barriers to maintaining accurate data, noting that even if information can be made accurate at the point of data entry, the maintenance of accuracy requires the registrant to keep the information current. NORC notes that:

currently, the only penalty for a registrant for letting information get out of date is a communication from their registrar that they need to update it or their domain name will be suspended and possibly their ownership revoked. Even this is not a significant concern for many registrants when only a small proportion of domain names lead to web sites that the registrant has a vested interest in maintaining uninterrupted access to.

Some respondents to the public Discussion Paper argued that registrants should have their accounts suspended for intestinally submitting false information. The Intercontinental Hotel Group stated:

Additionally, registrants who intentionally submit false, faulty or no information should have all registrations associated with their account suspended until WHOIS data meets the full reporting requirements.

Valentin Hobel has also suggested that it should be easier for registrants to update their WHOIS data:

Provide a service which lets domain owners update their data directly on an ICANN website. The intermediate step of having the domain registrar to update the WHOIS data often fails since some of them don’t update the information.

With regard to how privacy concerns impact on the accuracy of WHOIS data, the Non-Commercial Users Constituency found that:

Rather than putting sensitive information into public records, some registrants use "inaccurate" data as a means of protecting their privacy. If registrants have other channels to keep this information private, they may be more willing to share accurate data with their registrar.[[18]](#footnote-18)

Privacy issues, and specific recommendations to address the privacy concerns of some registrants, are discussed in [section xx] of this report.

1. **Data Accessibility and Privacy**
2. **ICANN’s commitment to unrestricted public access**

**The Affirmation of Commitments provides that ICANN will** implement “its existing policy” of timely, unrestricted and public access to accurate and complete WHOIS information.

In responses to the public Discussion Paper, several respondents **supported this commitment to open access, and argued that it is consistent with practices and arrangements in comparable offline situations. For example, INTA stated that:**

**it supports open access to accurate ownership information for every domain name in every top-level domain registry via a publicly accessible WHOIS database...in most circumstances, publishing on the internet is a public act, and the public should be able to determine who they are dealing with.**

**Similarly, the IACC argued that:**

**WHOIS is only an address book: something that does not adversely affect free speech, and one that carries far more benefits than potential drawbacks ... most other parts of the world require accurate information for business licenses, trademark registration, and other services; domain name registration should be no different.**

**Yet others argue that the uses of Whois has been extended beyond that intended by the existing policy and original plan:**

 ***Former GAC Member Christopher Wilkinson*:**

**“Purpose of Whois: I rather doubt that the initial purposes of the Whois protocol and**

**database extended to their current utilisation. It would appear that rather more is expected of Whois than it is capable of delivering in view of the legacy of past practice and the current and prospective scale of the Internet.”**

**Others in the ICANN Community warn that one size does not fit all for Whois purposes and uses:**

The problem for many registrants is indiscriminate public access to the data. The lack of any restriction means that there is an unlimited potential for bad actors to access and use the data, as well as legitimate users and uses of these data.

1. **Concerns about privacy**

**This universal commitment to unrestricted public access to complete WHOIS data was questioned by some respondents to the Discussion Paper, who argued that it raises a range of privacy related concerns. These concerns primarily relate to:**

* **the potential for conflict with privacy or data protection laws;**
* **the potential for misuse of openly-available WHOIS data (e.g. for spamming, stalking and other forms of physical and online harassment); and**
* **protecting the privacy of organizations individuals, including potentially vulnerable registrants (e.g. political dissidents, political dissident organizations, religious minorities and their institutions) These groups largely use the Internet to post ideas and information, with any “e-commerce activities” as limited and incidental.**

**Under the current WHOIS arrangements, ICANN has established procedures and policies to try to address some of these issues, but comments received by the Whois Review Team indicate that communities which represent individuals and non-commercial organizations consider the policies below to be neither sufficient nor properly protecting of privacy:**

With regard to potential conflicts with privacy laws, ICANN has established a consensus procedure for “Handling WHOIS conflicts with Privacy Law” (this became effective in January 2008). This procedure 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.

**Several respondents argued that this procedure is appropriate, and that ICANN had therefore taken sufficient measures to address potential conflicts with privacy law. For example, the IPC argued that:**

**ICANN is subject to a commitment ‘to having accurate and complete WHOIS’ ... ICANN is not required to implement national safeguards for individuals’ privacy. Given ICANN’s commitment to having accurate and complete WHOIS data, the burden of restricting access to such data in a particular locality should fall on the locality, not ICANN.**

**Similarly, the COA argues that:**

**The issue of balancing registrant privacy against the need for publicly accessible WHOIS data has two aspects. The first involves situations in which registrars (or registries) are authoritatively advised that their compliance with ICANN contractual obligations would bring them into conflict with applicable national privacy laws ... ICANN policy already provides a mechanism for resolving such conflicts. COA is unaware of any need for further policy development in this area.**

**Yet the Noncommercial Users Constituency argued:**

Even with the provisions for resolving conflicts with national law, WHOIS poses problems for registrars in countries with differing data protection regimes. Registrars do not want to wait for an enforcement action before resolving conflicts, and many data protection authorities and courts will not give rulings or opinions without a live case or controversy. ICANN's response, that there's no problem, does not suit a multi-jurisdictional Internet.

ICANN staff have advised that the consensus procedure has only been used on one occasion, by Telnic, to address concerns raised in relation to UK privacy law. In that case, it was agreed that some public WHOIS data could be limited for natural persons who had elected to withhold their personal information from disclosure by the WHOIS service. We should note that another gTLD, .NAME, negotiated Whois changes upfront in its registry agreement on becoming a gTLD registry as the nature of the private individuals within its scope was clear, and consistent with the data protection laws of its country of incorporation.

The consensus procedure also appears to be consistent with **the GAC Principles on gTLD WHOIS services, which state that:**

gTLD WHOIS services should provide sufficient and accurate data about domain name registrations and registrants subject to national safeguards for individuals' privacy.

With regard to potential misuses of WHOIS data, the ICANN community has developed consensus policies to prohibit bulk access to WHOIS information for marketing purposes (effective November 12, 2004), and prohibiting resale or redistribution of bulk WHOIS data by data users (effective November 12, 2004), although there is little in the way of enforcement action on this issue.

 ICANN has also commissioned a study to examine the scope of WHOIS misuse in detail.[[19]](#footnote-19) This study will analyse the extent, nature, and impact of harmful actions taken using WHOIS contact information, and is intended to provide the ICANN community with the empirical data needed to inform any future actions in this area.

With regard to the potential need for special protections for some registrants, **the most widespread way of addressing these concerns is the currently unregulated use of ‘privacy’ and ‘proxy’ services.**

1. **Privacy and proxy services**

**Privacy and proxy services are offered commercially by a wide range of service providers, including some registrars, and limit publicly accessible information about domain registrants:**

*Privacy* services limit certain user details from WHOIS by offering alternate contact information and mail forwarding services, while not actually shielding the user’s identity.

*Proxy* services have a third-party register domain names on the user’s behalf and then license the use of the domain name so that a third-party’s contact information (and not the licensee’s) is published in WHOIS.

**As noted earlier in this report, privacy and proxy services are referred to in provisions** 3.4.1 and 3.7.7.3 of ICANN’s RAA [confirm that both are covered]. The review team notes that the current use of these services is widespread, with a 2009 study determining that privacy and proxy services are used in 15%-25% of WHOIS records.

There are diverging views from stakeholders about the use of privacy and proxy services. For example, the NCUC argued that “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 domain registrants”.

On the other hand, one law enforcement agency argued that ‘if an entity is engaged in legitimate business activities, then a proxy service should not be necessary’. Another stated that ‘privacy/proxy services can be abused’, and that ‘criminals do use proxy and privacy registrations to hide their identities’. (Note on deletion: as cited by James in email, Knujon is not considered to be objective data.)

1. **Do privacy and proxy services undermine WHOIS?**

A significant number of public responses to the WHOIS discussion paper, and input from law enforcement agencies via the review team’s targeted questionnaire, argued that privacy and proxy services undermine the effectiveness of the WHOIS service**, both in terms of its ability to meet the legitimate needs of law enforcement and to promote consumer trust**. One law enforcement agency argued that

proxy services play right into the hands of organised crime, they hide all their business behind them and this is a huge issue, not only for law enforcement, but for the wider internet community as a whole.

**Another law enforcement agency argued that: “The time routinely invested by law enforcement to validate WHOIS data that may be false, unavailable, incomplete, or proxied impedes investigations”. Similarly, the International Hotel Group argued that:**

privacy services have frequently frustrated our ability to protect our hotel brands online, which, unfortunately, often leads to confusion and other problems among consumers.

**S**ome respondents to the Discussion Paper also questioned whether the use of privacy and proxy services was consistent with ICANN’s commitment to the provision of unrestricted public access to complete WHOIS data. For example, Time Warner urged the review team to:

identify the proliferation of proxy registration services, and the consequent inaccessibility and inaccuracy (for all practical purposes) of a huge swath of gTLD WHOIS data, as a major flaw in ICANN’s implementation of its WHOIS policies.

The COA also stated that:

Until ICANN is able to bring some semblance of order, predictability and accountability to the current ‘Wild West’ scenario of proxy registrations, it will be impossible to make significant progress toward improving the accuracy of WHOIS data, so that the service can better fulfil its critical function to internet users and society as a whole.

Yet others expressed strong support for privacy and proxy services:

The Noncommercial Users Constituency wrote:

“Privacy and accuracy go hand-in-hand. Rather than putting sensitive information into public records, some registrants use "inaccurate" data as a means of protecting their privacy. If registrants have other channels to keep this information private, they may be more willing to share accurate data with their registrar.

Other groups noted in oral comments that proxy/privacy services, as private entities, are outside the scope of ICANN to regulate, and in many cases, are not apparent to the registrars (as in a lawyer registering domain names for a client).

In a discussion of the WRT and the Intellectual Property Constituency, the use of proxy and privacy services arose and the beneficial use of the services to protect trade secret and confidential commercial information was noted (e.g., as in the name of an upcoming movie, a new product or service, or a potential acquisition target together with the proposed new name of the entity).

Thus, in spite the broad level of concern about privacy and proxy services, a significant number of concerned respondents to the public Discussion Paper and law enforcement questionnaire did not advocate for their abolition. For example, some law enforcement agencies noted that privacy and proxy services are a ‘tool to remain anonymous which may be useful and justified in certain limited cases’, such as ‘if someone has a Family Protection Order (or similar) and displaying their information may put them at risk of harm’.

Rather than arguing against the use of proxy and privacy services *per se*, many stakeholders identified the unregulated environment in which they operate as a major underlying problem. For example, Time Warner noted that while it did ‘not oppose the concept of proxy registration in limited circumstances’, it did see:

the development of a vast universe of 20 million or more gTLD domain name registrations, for which the identity and contact data of the registrant is hidden and, all too often, completely inaccessible, [as] a direct attack on ICANN’s chief policy goal for WHOIS.

Similarly, the COA acknowledged that some registrants may require specific privacy protection, but that these only accounted for ‘**an infinitesimal fraction’ of current privacy and proxy registrations, and that the:**

creation of a vast unmanaged database of tens of millions of effectively anonymous domain names ... is an irrational and socially damaging ‘solution’, one that inflicts far greater costs than warranted upon legitimate e-commerce, consumer interests, law enforcement and the public at large.

**Specific concerns with the current unregulated environment include that:**

* it impedes investigations and makes determination of the competent jurisdiction difficult. In this context, **one law enforcement agency argued that they are ‘aware of an online company providing a domain privacy protection service that actively promotes that they cannot be contacted by any other means except through their website. This service is regularly utilised by criminals to register criminal based domains’;**
* **it increases risk for law enforcement agencies by exposing investigative activities to unknown and non-trusted parti**es. The BC clearly illustrates this risk when it states that its members have ‘experienced situations where the registrar’s ‘proxy service’ is simply a shell behind which to shield the registrar’s own cybersquatting and illegal activities’); and
* **the responsiveness of proxy or privacy service providers varies widely, with no current recourse for failure to disclose data.**

In terms of responsiveness, the MPAA stated that:

To date, only one proxy service has complied with MPAA requests to reveal contact information that would enable the service of a cease and desist notice to suspect operators. Seven other have refused to do so or have simply not responded. Even the one more compliant service has recently changed its policies so that it takes up to ten days or more (after notifying its customer) before it will disclose the information. This gives the suspect ample time to transfer the domain name to another suspect entity or take other steps to evade detection.

Similarly, Time Warner International argued that:

Whether or not a member of the public would ever be able to learn the identity or be able to contact the party actually responsible for the registration ... depends entirely on whether this proxy registration provider chooses to make that information available. In Time Warner’s experience, some proxy registration providers are responsible, and will divulge this information upon being presented with evidence that the registration is being used to carry out abusive activities. Many others, however, do not.

On this issue, the GNSO has approved and ICANN has commissioned two studies on proxy/privacy services to take place within the next year:

1. WHOIS Registrant Identification Study Motion May 2011 (“this exploratory study would examine Whois data for a representative sample of gTLD domain names and provide the ICANN community with empirical data regarding the types of entities that register domains, including natural persons, various kinds of legal persons and Privacy and Proxy service providers – to help inform any future actions in this area). [http://gnso.icann.org/resolutions/#201106](http://gnso.icann.org/resolutions/%22%20%5Cl%20%22201106) (**20110609-1)**
2. Whois Privacy and Proxy "Relay and Reveal" pre-study survey, authorized by the GNSO Council on April 28, 2011, to examine the responses of proxy and privacy services to requests to RELAY information (as in a request to know whether the domain is for sale) and requests to REVEAL information (as in when the party demanding the Whois data asserts that it has a legal claim). [http://gnso.icann.org/resolutions/#201106](http://gnso.icann.org/resolutions/%22%20%5Cl%20%22201106) (**20110428-1)**
3. Whois Privacy and Proxy "Abuse" study to evaluate a broad sample of domains registered with a proxy or privacy service provider that are associated with alleged harmful acts with overall frequency of proxy and privacy registrations [http://gnso.icann.org/resolutions/#201106](http://gnso.icann.org/resolutions/%22%20%5Cl%20%22201106) (**20110428-1**).

Together these studies would indicate a substantial interest and investment in the study of key issues on which the community asserts varying facts and perspectives. As stated in each of the approving GNSO Council resolutions, they are intended to be responsive to the GAC letter requesting detailed WHOIS studies (<http://www.icann.org/correspondence/karlins-to-thrush-16apr08.pdf>). The studies, together and individually, are intended to provide the ICANN community with the empirical data needed to inform any future actions in this area. ICANN has allocated over $400,000 for the studies.

1. **Balancing privacy and public access**

We haven’t cited a single recommendation of any of the stakeholder groups representing individuals or non-commercial organizations below (e.g., ALAC and NCUC). There are some very interesting proposals in the ALAC statements and comments in NCUC that should be incorporated below... for a later draft ☺!

**To address these concerns about lack of regulation, several respondents to the public Discussion Paper and the law enforcement questionnaire argued that:**

**ICANN needs to regulate privacy service providers.**

**In most cases, respondents argued that:**

**this should include the accreditation of service providers and the imposition of minimum conditions for their operation.**

**For example, the IPC argued that**

ICANN should undertake to create an official set of guidelines for what constitutes a valid privacy/proxy service and best practices for such services.

**Several law enforcement agencies suggested that:**

**this type of regulation could mitigate some of their concerns with privacy services, and assist in the investigation and shut down of criminal domains.**

Suggestions for regulatory conditions put forward by respondents to the public Discussion Paper and the law enforcement questionnaire related to the development of clear, workable, enforceable, and standardized processes to regulate access to registrant data when requested. For example, INTA recommended that:

where a domain has been registered using a privacy or proxy service, there should be clear, enforceable contract mechanisms and procedures for the relay of communications to the beneficial owner, and for revealing the identity and contact information of the beneficial owner ... privacy/proxy services should be governed by a uniform body of rules and procedures that is overseen by ICANN, including standardised relay and reveal processes.

Compliance issues are substantively addresses in the next section of this chapter. Consistent with that section, the review team considers that an important part of any privacy accreditation process will be to ensure that appropriate and graduated enforcement mechanisms are in place.

Several stakeholders also emphasised the need to limit their use of privacy services in various ways – for example, to private individuals not involved with selling products or otherwise collecting or soliciting money.

Another issue raised by respondents to the public Discussion Paper and the law enforcement questionnaire relates to which data fields should be able to be limited by a privacy service. This issue is central to reaching an appropriate balance between personal privacy and ICANN’s commitment to publicly available information. In this context, one law enforcement agency argued 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.

As noted above, several respondents argued that there may be a case to limit access to some registrant information, and some respondents focused on specific data fields (such as personal addresses, phone numbers and email addresses). For example, NOM stated that ‘in line with UK data protection law, a registrant who is a non-trading individual can opt to have their address omitted from the WHOIS service’.[[20]](#footnote-20) Similarly, FC argued that:

Balancing privacy, security and the right to know is the question. Minimal data requirements that allow a quick identification would be ideal, like Registered Name Holder, State/City/Country, email and telephone.

**In terms of balance, some respondents argued that it was important to retain enough publicly available data to establish domain name ownership and registrant identity. For example, INTA argued that:**

**INTA supports open access to ownership information for every domain name in every top-level domain ... Available information should include the identity of and accurate, reliable contact details for the true owner of the domain name.**

**The question of ownership and identity is central to the distinction between privacy and anonymity, and several stakeholders raised specific concerns about lack of public access to a registrant’s name and identity.** For example, one law enforcement agency argued that:

The ability to hide ones identity in the global e-commerce marketplace creates and environment that allows illegal activities to flourish. It is imperative that law enforcement is able to identify the who, what, where of domain name operators immediately in order to effectively investigate.

**While several law enforcement agencies argued that privacy services could be regulated to provide special access to underlying registrant data (including registrant name) for law enforcement agencies, this would not address the broader consumer trust concerns associated with anonymity. For example, INTA argues that ‘in most circumstances, publishing on the internet is a public act, and the public should be able to determine who they are dealing with’. The GAC Principles similarly note that WHOIS data can contribute:**

**to user confidence in the Internet ... by helping users identify persons or entities responsible for content and services online.**

**The review team is not aware of any compelling reason to hide a registrant’s name, and notes that a registrant’s name is not allowed to be hidden as a result of the only existing use of ICANN’s consensus procedure to address potential conflicts with privacy law. I don’t think there is complete agreement on this issue, and I have recently learned that at least one national data protection commission has raised the issue of registrant name privacy in the Whois database; besides, this seems to be the essence of a policy recommendation.**

1. **The roles and responsibilities of contracted parties**

**[PLACEHOLDER]**

1. **Internationalized Registration Data and Associated Data Services**

Looking into the past, at a first glance it would seem that the issue of non-Latin scripts would only exist since the creation of IDNs. However, the basic problem has existed for much longer. As WHOIS data represents contact information of the domain registrant, the need of WHOIS data to support non-Latin scripts has been around as long as domain names have been registered by registrants globally, who need to represent their local names, postal addresses and other contact and technical information in the script(s) which they use. It is important to note that this requirement even exists for registrants who use Latin script, where additional annotations or special characters are needed beyond core ASCII to represent a language, e.g. Swedish, French, Vietnamese, Wolof, etc.

This lack of support for non-ASCII characters within the registration data has triggered two sources of inaccuracies in the data. For the languages using an extended set of letters in Latin script, limitations of use have forced registrants to “simplify” their information, e.g. document it without the use of accents and/or marks used by their language and community. For languages and communities which use non-Latin scripts, registrants have been forced arbitrarily to transliterate and/or translate their contact information into an ASCII based writing system. Communities which use syllable-based or an ideographic writing systems, e.g. Chinese, are even more disadvantaged in this respect, compared to other languages which use a sound based writing system.

Where the lack of local script support has been too much of a barrier, some ccTLD registries and registrars have implemented ad hoc solutions, using ideosyncratic mappings of local script onto ASCII code points and interpreting the data in their script instead of ASCII as a result. This has included using alternate international 8-bit standards for such mapping, e.g. ISO 8859-x or even local national standards. However, as this encoding information is not part of the WHOIS data, it is not possible for a user to know or predict this. As a result, the data can appear as a nonsense sequence of ASCII characters. This is also a major source of inaccuracy of data (highlighted by the 2010 National Opinion Research Council of the University of Chicago (NORC) Data Accuracy Study), not due to its content, but due the lack of mechanisms available for its interpretation.

Thus, lack of support of non-ASCII characters introduces an additional barrier for non-ASCII users to provide accurate and consistent domain name registration data. This has implications for their tractability for law enforcement and associated organizations. Further, many people attach some pride and fondness to the correct representation of their name and other data. While this is not a purely technical or administrative requirement, it is relevant in the context of Consumer Trust.

Assessing the current situation, domain names have been (partially) available in local languages since 2000 Since 2010, complete domain names in local languages have been more extensively deployed through the IDN ccTLDs approved through the Fast Track process – a process in part enabled through the adoption of a new technical standard, IDNA2008. However, even though millions of IDNs have already been registered within the domain space, there still does not seem to be a mechanism in place for domain name registration data to be gathered and made available in local languages. This is providing further motivation to ad hoc implementations of collecting and making the data available in local languages, or possibly introducing non-standard translation or transliteration inaccuracies, where registrant information from different language is being made available in a ASCII based existing WHOIS system, as already discussed.

Looking forward, the new gTLD process may result in a number of new IDN gTLDs which will be introduced from 2012, targeting registrants who are not familiar with Latin script. The latest version of Draft Applicant Guidebook[[21]](#footnote-21) makes a couple of references to domain name registration data in local languages. It stipulates a need for the registrant information to be available in local languages in the scoring chart given in the Attachment to Module 2: Evaluation Questions and Criteria. Point # 44 in this chart asks:

State whether the proposed registry will support the registration of IDN labels in the TLD, and if so, how. For example, explain which characters will be supported, and provide the associated IDN Tables with variant characters identified, along with a corresponding registration policy. This includes public interfaces to the databases such as Whois and EPP.

 In Section 5.2.3: Test Elements: Registry Systems, in “IDN Support” sub-section (pg. 5-7), it elaborates on the mechanism stating:

Requirements related to IDN for Whois are being developed. After these requirements are developed, prospective registries will be expected to comply with published IDN-related Whois requirements as part of pre-delegation testing.

Anticipating this need, work has already been going on to decide how such data should be collected, maintained and distributed. Internationalization Registration Data Working Group (IRD-WG), a joint GNSO and SSAC effort, was formed as a result of a Resolution of the ICANN Board in 2009[[22]](#footnote-22). IRD-WG is aiming to build consensus on how this registration data will be made available in local languages (including determining which fields can be internationalized)[[23]](#footnote-23). The need for internationalized registration data has also been highlighted in the recent SSAC report SAC 051[[24]](#footnote-24). Work is also underway (but in early stages) to look into how internationalized data will be associated with variants of internationalized domain names through the IDN Variant Issues Project (IDN VIP)[[25]](#footnote-25) and more recently the discussion list related to internationalization of Domain Name Registration Data at WHOIS-based Extensible Internet Registration Data Service (WEIRDS) through IETF[[26]](#footnote-26).

The situation highlights a general unpreparedness and lack of urgency in the community to support registration data in non-ASCII letters. This is highlighted by not taking up measures to store data and making it accessible for global registrants for ASCII domain names, not addressing this issue for the Fast Track program, and still having no agreement on how to resolve this for the upcoming gTLD program. Interestingly, scoring of internationalized registration data is in place for new IDN gTLD application without stipulating the mechanism to implement it in this program, which will increase the likelihood of increased ad hoc measures being instituted.

The community needs to urgently address the following issues:

* What data is needed from the registrant,
* How this data will be represented in the data model, and
* How this data will be accessed through registration data services.

There are some (partial) technical solutions[[27]](#footnote-27), but the community needs to evaluate the alternatives, choose between them, and/or adapt them and clearly define the data model and service to be supported. Best practices from ccTLDs should be studied in this context (as already highlighted by IRD-WG) and a consistent policy, through cooperation between ccNSO, gNSO and other relevant constituencies, e.g. ALAC and SSAC, needs to be defined, to limit ad hoc practices and resulting data inaccuracies or inconsistencies. Whilst the WHOIS Review Team understands and respects the independence of ccTLD policy making, nevertheless, a consistent policy across ccTLDs and gTLDs would make it much easier for consumers and law enforcement to use WHOIS data. Such policies need to be clearly articulated in current and future registry and registrar agreements (where applicable), with clear directions to the ICANN Compliance Team on how to measure accuracy of internationalized registration data (an aspect which remains undefined). Once the basics are in place, only then can work begin towards improving the accuracy and consistency. Thus, in many ways, the internationalized registration data issues are much deeper than the issues with ASCII based data available already, and need more urgent, if not equal, attention (especially in the context of the full roll out of the IDN program in 2012).

1. **Compliance Gaps**
2. **Communication**
* Locating information on the website is extremely difficult, compliance pages are hidden away, laden with jargon, and assume a level of knowledge by users which may not exist in practice. Documents referred to in the compliance team’s answers to the WRT as plain English guides should be front and centre to the user experience. Poor or ineffective communication generates costs, inefficiency and support load. It also creates frustration for everyone.
* Operating principles are generally good, but the use of jargon is out of place in high level principles.
* Reporting of contractual compliance activities is far from timely (operating principle 8), eg “monthly” newsletters and “semi-annual” reports have not been published at all in 2011. If these have been replace by other forms of communication, this is not clear.
* Key documents (eg the Privacy/Proxy study 2009) are missing, or only possible to locate with specific URLs.
1. **Audits**
2. The 2010-11 Registrar WHOIS Data Access Audit is an example of a successful compliance intervention. Areas for improvement include communication, sustaining the momentum and delivering performance measures/goals over time. A summary of the detailed report would be helpful to the new comer. This should also be linked to the operating principles, as a successful example of working in partnership with registrars to foster a culture of compliance.
3. The acronyms WDRP and WDPRS are confusingly similar, especially as they are two of the most significant ongoing compliance activities undertaken by the compliance team. The use of the acronyms without explanation gives ICANN an unnecessary communications challenge.
4. The WHOIS Data Reminder Policy is an example of a poorly thought through compliance effort. It involves both ICANN and its registrars engaging in significant economic activity and disruption. The effect on WHOIS data quality is unknown, and 83% of registrars are unable to track any changes resulting from WHOIS Data Reminder Notices. Therefore it is impossible to measure the impact of this flagship policy for improving data accuracy.
5. **Investigating complaints of non-compliance**
6. Given the prevalence of inaccurate WHOIS data, both the number of Whois Data Problem Reports, and the number of individual reporters (in 2007, 10 people were responsible for 87% of all WHOIS inaccuracy reports) are unacceptably low, indicating a low awareness level of this service amongst the target users of the system – consumers. It was striking that members of the WHOIS Review Team, whose daily job involves conducting hundreds of WHOIS queries, were unaware of the service or how to report inaccurate data to ICANN.
7. The system for WHOIS Data Problem Reporting generates a high level of duplicates. ICANN’s compliance staff have inadequate workflow systems or automation to enable them to keep on top of their existing workload – this provides a disincentive to ensuring that the system is better known and more widely used.
8. **Other WHOIS Related work and efforts – Data Accuracy**
9. Data accuracy – the low level of accurate WHOIS data is unacceptable, and decreases consumer trust in the WHOIS, in the industry of which ICANN is a quasi-regulator, and therefore in ICANN itself. The organisation’s priority in relation to WHOIS should be to improve WHOIS data accuracy and sustain improvement over time. It should publish performance targets, and develop incentives for registrars and registrants to improve data accuracy.
10. Just as there is no shared understanding, or statement of the purpose of WHOIS, key concepts, such as “data accuracy” mean different things to different stakeholders. Further work is required, involving all interested stakeholders, to develop a common understanding and statements of the purpose of WHOIS and key concepts within it.
* The WHOIS Data Accuracy Study identified that a key cause of inaccuracy was confusion amongst registrants when completing WHOIS data. If the industry wants to improve accuracy of data, it is necessary to think through the core WHOIS data set from the perspective of a commonly understood WHOIS Purpose, and creating a streamlined, understandable data set for registrants to complete. A number of stakeholder groups, notably SSAC, have been thinking deeply about these issues for a number of years.
* The WRT is aware that over the next 12-18 months, four independent studies on WHOIS will be published, representing an investment of [ $xxx,000,000]. It is hoped that these will improve understanding of key elements of the WHOIS environment, and provide an evidence base for the effectiveness of ICANN’s WHOIS policy and implementation. However, this effort and investment will be worthless if there is no follow-up. Regrettably, that is the impression given by the failure on ICANN’s part to publish an action plan and targets in response to Data Accuracy Study, 2010.
* It is unclear what the response of the Compliance team to the Data Accuracy Study has been. This leads to the impression that expensive, time consuming studies are being undertaken, and then left to languish. An action plan should already have been published by now, including measurable targets, and key performance indicators. If this has happened, the WRT is unaware of it.
1. **Recommendations**
2. **Recommendations from our Brainstorming Session (Saturday afternoon in Dakar)**
3. ICANN's WHOIS policy is poorly defined and decentralized. The recommendation is to create a single WHOIS policy document, and reference it in subsequent versions of agreements with Contracted Parties

ICANN should document the current gTLD WHOIS policy as set out in the gTLD Registry and Registrar contracts and gNSO consensus policies and procedure.

1. ICANN should make WHOIS a strategic priority. This should involve allocating sufficient resources, through the budget process, to ensure that ICANN compliance staff is fully resourced to take a proactive regulatory role and encourage a culture of compliance. ICANN Staff should nominate a person responsible for overseeing WHOIS compliance.
2. [ICANN should ensure that WHOIS policy issues are accompanied by] Cross-community outreach including outreach to the community outside ICANN with specific interest in this issue.
3. ICANN should take appropriate measures to reduce the number of unreachable Whois registrations (as defined by the National Opinion Research Council of the University of Chicago (NORC) Data Accuracy Study, 2010) by 50% within 12 months and by 50% again over the following 12 months.
4. ICANN be able to produce an accuracy report on an annual basis.
5. (ICANN should provide) status report (+references) on its progress towards achieving the goals set out by this WHOIS Review Team, published by the time the next Whois RT starts. Tangible, reliable figures needed.
6. **MDR Recommendations as Reviewed and Agreed upon in Dakar (originally from the Peter and Emily documents)**
7. ICANN should ensure that the requirements for accurate WHOIS data are widely and pro-actively communicated to current and prospective Registrants. As part of this effort, ICANN should ensure that its ‘Registrant Rights and Responsibilities’ document is pro-actively and prominently circulated to all new and renewing registrants.
8. ICANN should ensure that there is a clear, unambiguous and enforceable chain of contractual agreements with registries, registrars, and registrants to require the provision and maintenance of accurate WHOIS data. As part of this, ICANN should ensure that clear, enforceable and graduated sanctions apply to registries, registrars and registrants that do not comply with its WHOIS policies. These sanctions should include de-registration and/or de-accreditation as appropriate in cases of serious or serial non-compliance. Implementation Dispute language: any intermediary
9. ICANN should allocate sufficient resources to be proactive in enforcing its WHOIS policies and contracts.
10. Building on the 2009 National Opinion Research Council of the University of Chicago (NORC) study, ICANN should commission regular studies to periodically measure WHOIS accuracy. These studies should provide time series data to enable definitive assessment of ICANN’s performance in improving WHOIS accuracy.
11. ICANN should develop and manage an accreditation system to allow registries and ICANN-accredited registrars to become privacy service providers. [the rationale for this limitation to already contracted parties needs to be developed, and centres on concerns that unknown parties with little or nothing to lose from de-accreditation pose a significant risk to the system] See James’ voluntary accreditation comment, and concern about reaching to non-contracted parties.
12. **Privacy Recommendations as written on Monday Morning in Dakar by Peter, Kathy and Bill and reviewed with Team that Monday**
13. **Findings**
* The community has not handled the issue of privacy in a timely or effective manner.

As the community hesitated a private industry arose offering proxy and privacy services to millions of registrants. The industry is largely unregulated.

* Law enforcement and the private industry around law enforcement and the security industry users of WHOIS have a difficult time finding those responsible for websites.
* ICANN’s attention has been drawn to this situation, for example: Data protection commissioner communiqués have told ICANN that natural non-trading persons need privacy protection under EU and other national data protection laws.
* There are protections for free speech and freedom of expression that need to be taken into account. Proxy and Privacy services meet a market demand
* Proxy and Privacy services are terms used in the 2009 RAA but are undefined.
* There is a risk that in the current privacy services regime that the registration data could be seen as invalid on its face as inaccurate (registrant name, privacy service contact info)
* Technical contact information has special relevance and use for operational and security community
1. **Conclusions**
* The current proxy and privacy regime is flawed and we direct ICANN, the Board, and GNSO as appropriate to fix it.
* For the avoidance of doubt, the WHOIS Policy should include an affirmative statement that clarifies that a proxy means a relationship in which the registrant is acting on behalf of another.  The WHOIS data is that of the agent and the agent alone obtains all rights and assumes all responsibility for the domain name and its manner of use.
* Remove proxy services from the RAA since the proxy, as an agent, is the registrant. Expand and ? affirmative sentence
1. **Recommendations**
2. ICANN should develop and manage a system of clear, consistent and enforceable requirements for all Registrar-operated privacy services consistent with national laws. This should strike an appropriate balance between stakeholders with competing but legitimate interests. At a minimum this would include privacy, law enforcement and the industry around law enforcement.
* WHOIS entry must clearly label that this is a private registration
* Privacy service must provide full contact details for itself, including name, address, phone, email, 24 x7 contact.

LUTZ: Privacy services must provide full contact details as required by the WHOIS

Privacy services must provide phone and email contacts to be put into the whois record which are available and responsive as required by the framework mentioned above.

* Standardized relay and reveal processes and timeframes.
* Rules for the appropriate level of publicly available information on the registrant
* Maintenance of a dedicated abuse point of contact for the privacy service provider
* Privacy service provider shall conduct periodic due diligence checks on registrant contact information
1. ICANN should develop a graduated and enforceable series of penalties for privacy service providers who violate the requirements with a clear path to de-accreditation for repeat, serial or otherwise service breaches.
2. **Definitions**

**Proxy**:  A relationship in which the registrant is acting on behalf of another.  The WHOIS data is that of the agent and the agent alone obtains all rights and assumes all responsibility for the domain name and its manner of use.

**Privacy**: Registrant Name and a subset of other information (possibly null set) but consistent across ICANN

1. **IDN Recommendations**
2. ICANN Community should form a working group within 6 months of publication to finalize (i) encoding, (ii) modifications to data model, and (iii) internationalized services, to give global access to gather, store and make available internationalized registration data. Such working group should report no later than one year from formation, using existing IDN encoding and translation mechanisms. The working group should aim for consistency of approach across the gTLD and – on a voluntary basis – the ccTLD space.

[Quick Question: Does this Disregard or Displace any of the Existing IDN Committees now meeting?]

1. The final data model and services should be incorporated and reflected in Registrar and Registry agreements within 6 months of adoption of the working group’s recommendations by the ICANN board. If they are not finalized in time for the next iteration of such agreements, explicit placeholders for this purpose should be in place in these agreements (as is the case for adoption of consensus policies).

[Unfortunately, the above is almost impossible. Contracts are renegotiated when they expire. Occasionally with major changes to the Registrar Accreditation Agreement, such as the 2009 RAA, a number of the Registrars will quickly sign up to the new contract, but that happened only once.

We can work with ICANN's General Counsel's office to find the best language to most quickly include the new Final Data Model and Services into Existing Contracts – should we ask Denise Michel to work with us on it?

1. Requirements for registration data accuracy and availability in local languages should be finalized (following initial work by IRD-WG and other similar efforts) by [deadline]. Metrics should be defined [by when?] to measure accuracy of data in local languages and/or corresponding data in ASCII, and compliance methods and targets should be explicitly defined accordingly.

Questions:

Are the standards for accuracy and availability the same in IDNs as they are in ASCII, for example, is the purpose of this section to require that all of the ACCESS and ACCURACY requirements we set for ASCII be the same for IDNs? (If so, does that pose any additional problems that our ASCII-focused WRT has not considered?)

Alternatively, are you saying that a separate set of ACCESS and ACCURACY standards for IDNs be created?

Or possibly does the above paragraph have nothing to do with access and accuracy? Is the purpose to talk about the access and accuracy of the data transcription and translation? Michael shared those words on the Call. If that is the case, would the following wording capture the idea (and please edit!!)?:

Revised #3: The requirements for the processing of data transcription and translation from the local languages to ASCII should be finished by [deadline] given the current work of the [?] Working Group. The ICANN Board should direct the development of Metrics to measure the quality of the translation of data from local languages to ASCII, publish the results to the Community, and set out further compliance methods and targets accordingly.

1. **Proxy Recommendations**
2. **Definitions**

**Affiliate retail proxy service provider** is an entity that operates under a common controlling interest of a registrar. “

**Retail proxy service provider** – provides a proxy service with little or no knowledge of the entity or individual requesting the service beyond their ability to pay and their agreement to the general terms and conditions.

**Limited proxy service provider** – provides a proxy service for an entity or individual in which there is an ongoing business relationship bound by a contract that is specific to the relationship.

1. **Findings & Recommendations**

A registrar that owns or manages a subsidiary that provides a proxy service or enters into a partnership or recommends a proxy service at the time of registration has knowledge of the contractual agreement between the proxy service provider and registrant. Both the proxy service provider and registrar should be held responsible for engaging in best practices outlined below.

1. A registrar is required to disclose their relationship with a Retail proxy service provider to ICANN. If the relationship is one of a subsidiary, partnership or recommended by the registrar and the registrar collects fees associated with the proxy registration the registrar’s accreditation will extend to the service and they will be governed by the RAA.
2. As a condition of providing the proxy service in conjunction with a registrar relationship the providers should be required to comply with best practice guidelines. These should provide for:
	1. standardised relay and reveal processes and timeframes;
		1. establish a standardized process for requesting contact information for a proxy registration
		2. 24 hour response to provide requested contact information when requested by Law Enforcement;
		3. 5 day business response when requested by a non LE third party
	2. guidance on the appropriate level of publicly available information on the registrant;
	3. maintenance of a dedicated and available abuse point of contact;
	4. public disclosure of contact details and the physical address of the privacy service provider; and
	5. proxy service providers to validate registrant contact information.
3. As a condition of providing the proxy service in conjunction with a registrar relationship, the proxy and privacy providers shall be required to very clearly disclose to the Registrant at the time of registration:
	1. their relationship with the registrar;
	2. a clear explanation of the meaning of the proxy or privacy service (depending on what is being offered);
	3. a very clear understanding of what registrant data will be published in the globally-available Whois database, and particularly whether the domain name;
	4. Registrant's name is published in the global Whois directory

[yes for privacy services; no for proxy services]; and

a very clear explanation of who will “own” the domain name if the Registration chooses the privacy or proxy service, pursuant to then-adopted ICANN rules.

1. The best practice guidelines should be developed in close consultation with the GAC, privacy advocates, law enforcement, and other interested stakeholders.
2. ICANN should develop a graduated and enforceable series of penalties for proxy providers and registrars who violate the terms of the RAA.
3. **References**

For full details of the longer recommendations discussed and debated, please see the following documents:

1. Recommendations from our Brainstorming Session (Saturday afternoon in Dakar) [https://community.icann.org/display/whoisreviewprivate/Brainstorming+in+Dakar](https://community.icann.org/display/whoisreviewprivate/Brainstorming%2Bin%2BDakar) (V2; date: 23Oct2011)
2. MDR Recommendations as Reviewed and Agreed upon in Dakar (originally from the Peter and Emily documents) [https://community.icann.org/display/whoisreviewprivate/Draft+Recommendations](https://community.icann.org/display/whoisreviewprivate/Draft%2BRecommendations) (Draft MdR Recommendations discussed in Dakar; V1; 23Oct2011)
3. Privacy Recommendations as written on Monday Morning in Dakar by Peter, Kathy and Bill and reviewed with Team on Monday in Dakar [https://community.icann.org/display/whoisreviewprivate/Draft+Recommendations](https://community.icann.org/display/whoisreviewprivate/Draft%2BRecommendations) (Draft Recommendations discussed in Dakar; V1; 24Oct2011)
4. Current IDN paper [https://community.icann.org/display/whoisreviewprivate/Internationalization+of+Domain+Name+Registration+Data](https://community.icann.org/display/whoisreviewprivate/Internationalization%2Bof%2BDomain%2BName%2BRegistration%2BData)
1. Most registries are ‘thick’, i.e. they hold all WHOIS information within their TLD. Other registries such as ‘.com’ run by VeriSign actually contain only basic domain information and a pointer to smaller (or ‘thin’) WHOIS databases held by individual registrars. [↑](#footnote-ref-1)
2. Authoritative name servers are those that can give an authoritative answer on where a domain is located rather than one that has simply cached a response received from another name server [↑](#footnote-ref-2)
3. This Guide covers only generic top level domains (gTLDs), which come under the control of ICANN, however there are also hundreds of country-code top-level domains (ccTLDs) such as .uk that correspond to countries or territories around the world. [↑](#footnote-ref-3)
4. An ICANN accreditation is currently granted for a term of 5 years. In order for a registrar to maintain its accreditation, it must renew its RAA every 5 years. This means that the 2009 RAA might not be applied to all existing registrars before 2014. [↑](#footnote-ref-4)
5. A full discussion of the Team’s work to define the selected AOC terms of reference, including comments received from the stakeholder communities and the Teams responses thereto, can be found in the Appendix at \_\_\_\_\_\_\_\_. [↑](#footnote-ref-5)
6. For full comments, please see Appendixes – Public comments [↑](#footnote-ref-6)
7. ICANN Compliance Team’s Operating Plan, item 1 <http://www.icann.org/en/compliance/>, accessed 7/7/11 [↑](#footnote-ref-7)
8. Time Warner Inc., *Comments of Time Warner Inc.*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.3 [↑](#footnote-ref-8)
9. GAC Principles Regarding gTLD WHOIS Services (28 March 2007), section 4.1 [↑](#footnote-ref-9)
10. Intellectual Property Constituency, *Comments of the Intellectual Property Constituency*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.5 [↑](#footnote-ref-10)
11. China Internet Network Information Centre, *CNNIC Comments on the WHOIS review team discussion paper*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.2 [↑](#footnote-ref-11)
12. Coalition of Online Accountability. *WHOIS Review Team Discussion Paper Questions to the community, June 2011*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> [↑](#footnote-ref-12)
13. ICANN, *gTLD Applicant Guidebook* (30 May 2011) [↑](#footnote-ref-13)
14. Time Warner Inc., *Comments of Time Warner Inc.*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.3 [↑](#footnote-ref-14)
15. China Internet Network Information Center, *CNNIC comments on the WHOIS review team discussion paper*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p. 1 [↑](#footnote-ref-15)
16. Christopher Wilkinson, *WHOIS Review Team Discussion Paper Questions to the community, June 2011*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.1 [↑](#footnote-ref-16)
17. [↑](#footnote-ref-17)
18. Non-Commercial Users Constituency, *NCUC Comments on the WHOIS Review Team Discussion Paper*, <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00014.html> (23 July 2011) [↑](#footnote-ref-18)
19. <http://blog.icann.org/2011/04/cylab-at-carnegie-mellon-university-selected-to-conduct-study-of-whois-misuse/> [↑](#footnote-ref-19)
20. The review team notes that this is consistent with ICANN-approved arrangements in place in the UK based Telnic. [↑](#footnote-ref-20)
21. Available at <http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf>. [↑](#footnote-ref-21)
22. See <http://www.icann.org/en/minutes/resolutions-26jun09.htm#6>. [↑](#footnote-ref-22)
23. Current version (at this time) available at [www.gnso.icann.org/issues/ird/ird-draft-final-report-03oct11-en.pdf](http://www.gnso.icann.org/issues/ird/ird-draft-final-report-03oct11-en.pdf) [↑](#footnote-ref-23)
24. Availble at <http://www.icann.org/en/committees/security/sac051.pdf>. [↑](#footnote-ref-24)
25. See <http://www.icann.org/en/topics/idn/> for more details. [↑](#footnote-ref-25)
26. See <http://www.ietf.org/mail-archive/web/weirds/current/maillist.html> for archive of the discussion. [↑](#footnote-ref-26)
27. See WHOIS++ (RFC 1834), RWhois (RFC 2167), and CRISP (RFC 3707). [↑](#footnote-ref-27)