WHOIS Policy Review Team (WHOIS)

Final Report

*Draft 11/27/2011*

***[Chapter 1***

***Executive Summary]***

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. In 2009, ICANN and the US Department of Commerce approved, signed, and published an Affirmation of Commitments (AoC) in which ICANN commits to undertake a number of high level reviews, including on Accountability and Transparency (completed December 2010), and WHOIS.

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 for those definitions for the Domain Name System.

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 . 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**

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 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 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.

Unfortunately, we find that in this case policy is divined from its implementation. As a consequence, it 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 :within the ICANN community on the issues. More concerning, there appears to be no coordinated effort to achieve consensus on these important, and admittedly difficult issues. 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 have not kept pace with the 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 an ICANN policy vacuum. These services are clearly meeting a market demand and it is equally clear that these services are complicating the WHOIS landscape.

In the time since the formation of ICANN, Internet usage for ill-gain or harm has increased dramatically. Combatting 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 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.

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 the policy has become so complex and unmanageable.

1. **Recommendations**

**[Chapter 2**

**A Brief Guide to the Domain Name System and WHOIS]**

**A. DNS and WHOIS – How it Works**

The Domain Name System (DNS) (LD) proposed addition: is a hierarchical distributed database to lookup information from unique names, i.e. to help people connect to 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. 2620:0:2d0:200::7, 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 used to translates between domain names and IP addresses.

**WHOIS** provides information sufficient to contact a responsible party for a particular internet resource who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name or the DNS name servers.[[1]](#footnote-2) Unfortunately the term “WHOIS” is overloaded, referring to protocols, services, and data types associated various resources, i.e., domain names, Internet Protocol (IP) addresses, and Autonomous System Numbers (ASNs).[[2]](#footnote-3)

WHOIS registries are (LD) proposed addition: mainly run by Registry Operators, for example VeriSign who maintain the *.com* registry. IANA runs the central registry[[3]](#footnote-4) for all kinds of Internet ressouces, pointing to the whois server of the responsible (sub)-registry as well as the contact details of this registry.

DNS Registry operators also maintain another vital piece of information. ) The glue to the downside authoritative **name servers**[[4]](#footnote-5) 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 name servers starting from the hard coded root servers to find out which name servers are associated to that domain name. One of those name servers is then contacted and will return the IP address for that domain name. Your computer can now connect to the a computer 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 an ever increasing trailing part of the domain (e.g. .*com, .net, .uk*, *co.uk, ip6.arpa*), also known as the Top Level Domain (TLD[[5]](#footnote-6)). If the ISP doesn’t already know it can askfrom former questions which name server need to be ask for a given part of the domain name, it starts asking a **root server**. There are various root servers located all over the world which point to the appropriate downstream name servers.

WHOIS is designed to work in the same way: Starting at whois.iana.org follow the references to the downstream WHOIS servers unless the required information is obtained. This process is illustrated below.

**B. 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 create a WHOIS record with the registrant’s information. 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 **Registran**t 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 and registry 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) or certified by the registry operators to sell domains. They are thus bound by the Registrar Accreditation Agreement (RAA) with ICANN[[6]](#footnote-7) - or 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 (SK) comment: Not really but not sure what this is getting at information supplied by the registrant, and for periodic notifications to the registrant to verify the information is correct. Once notified that the WHOIS information may be inaccurate the registrar is required to notify the registrant to review and correct any inaccurate information in their WHOIS record ; (SK) comment: The registrar simply sends a notification to the registrant and relies on an honest reply. 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 with 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 the sponsor for the domain name registration and accountable for the domains sold by the re-seller.

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 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 with both registries and registrars.

**[KK Add:**

**Chapter 3**

**The Whois Review Team, Scope of Work &**

**Key Definitions]**

**A. The Whois Review Team and Its Affirmation of Commitments Work**

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:

[KK recommended add: All, I would recommend that add the groups from which we hail to the list below, e.g., Kathy Kleiman (US), Vice Chairman, Registries Stakeholder Group, GNSO. I think it provides good information and background re: our diversity for the readers.

Alice, if all agree, could you do this?]

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 the our work, including Denise Michele, Liz Gasster and Stacy Burnette. [KK delete The Review Team extends] [KK add: We extend our] 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.

[KK delete: This report set outs out the work of the WRT, its scope of work, 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.

[KK replace for the above paragraph] Our Final Report sets:

* Executive Summary
* Our Scope of work
* Our Key Terms and Definitions
* The Complex History of WHOIS Policy
* An Audit of ICANN's Compliance Department
* Our Detailed Discussion with Whois Consumers
* Gap Analysis
* Recommendations

As well as our detailed Appendices, including:

* Overview of Review Team's Method of Work,
* Research of and Written Comments of ccTLD Whois services and data (not covered by this gTLD report),
* Letter to Compliance (with additional details of our audit)
* Other [feel free to fill in!!]

KK end of add]

[Note from KK: I am having a lot of trouble with formatting this section, so if later editors do too, you are not alone. Alice, would it be possible for you to lead a clean-up of this section to remove all unnecessary formatting characters and character sets? Tx you!!]

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

**B. Scope of Work**

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.” [KK Note: footnote citation needed]

[The Affirmation of Commits sets out who shall be represented on the Whois Review Team:

“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.” [KK Note: footnote citation needed]

The AoC also sets out how our recommendations are to be handled:

“Resulting recommendations of the reviews will be provided to the Board and posted for public comment. [KK Note: footnote citation needed]

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

* + 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.”

[KK Note: footnote citation needed]

In setting out its scope, the WRT established 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 guide 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). [KK Note: footnote citation needed]

The WRT adopted its Scope of Work plan together with an ambitious outreach and action plan at its first meeting in London, 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.

**C. Key Definitions**

*Overview*

Early in the WHOIS Review Team’s work programme, we attempted to identify and define key terms in the Affirmation of Commitments and concerning other aspects of WHOIS most relevant to our review and to the work of the groups the Team intended to reach out to.

In conjunction with comments from the Community[[7]](#footnote-8), the Team found it useful for purposes of facilitating our review that we consider the following definitions as guides for our work:

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 the explanations (and engagement throughout the process:

**WHOIS 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. [...]

**WHOIS 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.

**The Whois Service**: The service(s) offered by registries and registrars to provide access to all or a subset of WHOIS Data […]

***2) Key Terms in Affirmation of Commitments***

**The Affirmation of Commitments used key, but undefined terms. In conjunction with the Community, the Review Team undertook to define these terms – working definitions for our work and analysis.**

***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.

[SK – Alice can you find the definition prior to the revision in September? I looked for it and could not find it] (AJ): Law Enforcement shall be considered to be an entity authorized by a government and whose responsibilities include the maintenance, co-ordination, or enforcement of laws, multi-national treaty or government-imposed legal obligations.

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. By adopted the narrower definition, the Team does not intend to discount the value of private sector efforts to curb abusive uses of the DNS.

With the adopted definition in mind, the Team consulted with to 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 \_\_\_\_.

*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(, and including registrants, registries and registrars).

(SK) comment: I agree with comment we should delete everything after All internet users

* 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, are covered in Section \_\_\_.

*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:

Including 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 regulation (SK) comment: I agree with Emily should change to “encompass all laws but many mainly focus on 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.

**[KK: I propose we END this Chapter right here – for the reasons discussed with each section below. All sections still exist, but some are relocated to make them more prominent or group them with similar material.]**

**[KK Delete this entire section as it is moved to the Policy Chapter]**

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

(SK) comment: These terms are confusing and main not be understandable to the general community. We should either revert to registrant registrar etc. or link the terms in clear definitions.

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.

**[KK Note: Delete section below as it is moved to Defintions 1) above]**

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 the explanations (and engagement throughout the process:

**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 […]

[KK Delete section below as it duplicates section 4) above and has been moved to Policy Chapter]

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.

**[KK recommend deleting this comment section below.]**

**Overview of Received Comments**[[8]](#footnote-9)**:**

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 team 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)**.

**[KK Move: Two defintions of “consumer” are now above. Have shared email with Lynn that it is OK to move the Consumer Study section below to a more prominent place in N ew Chapter.]**

**[KK Start Move]**

**What is a "consumer"?** (SK) comment: Isn’t this a duplicate from page 15 or am I missing the point?

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, are 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 provider tasked with obtaining information sufficient to provide the answers.

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

1. **Phase One: Qualitative Phase**

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

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

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

This small focus group of 20 users included:

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

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

These tasks included:

* Review and feedback regarding a known fraudulent website that appeared credible;
* Observations of the individuals attempting to locate domain name registrant information and feedback 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 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 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.

**[KK End Move]**

(SK) comment: will create a doc for the appendix on doing a WHOIS search in WHOIS.com and will circulate.

**[KK Add:**

**Chapter 4**

**The Complex History of WHOIS Policy**

1. **The Complex History of WHOIS Policy**

**A. Thick and Thin Registries and Their Different Whois Results**

There is nothing simple or clean about ICANN's Whois Policy. It is a process that ICANN inherited and built upon, and like a rickety structure built without a clear plan, is difficult to navigate and understand.

In 1982 Ken Harrenstien of SRI International wrote and the Internet Engineering Task Force (IETF) published “RFC 812” titled NICNAME/WHOIS creating a protocol for a directory service of ARPANET users. In 1985 RFC 954 replaced RFC 812 and set out a new series of commands for the text-based, Whois protocol. In 2004 RFC 3912 modified RFC 954 to remove information no longer applicable to the modern Internet. The current Whois protocol, the set of rule for communication of Whois searches and commands between computers, is largely based on the 1985 standard, and the IETF has indicated it may be reviewing the protocol shortly.

When ICANN was created in 1998, it inherited the Whois protocol and a set of existing gTLDs – .COM, .ORG and .NET – with their Whois search service and Whois data. Network Solutions managed the three top level domains as the distinction between registry and registrar had not yet been created.

In early 1999, ICANN introduced competition into the gTLD market by creating registrars, organizations accredited by ICANN to register domain names to Registrant. There are now 944+ gTLD Registrars, with GoDaddy being the largest. At the outset, there was deep concern that registrar competition could not flourish if Network Solutions, still in the registry and registrar businesses, held a full set of customer data of all gTLD registrants. ICANN agreed and .COM became a “Thin Registry,” holding only limited data about a domain name, and providing a link to the Registrar's database when someone seeks Whois data.

Thus, the Whois search of the .COM Registry, now managed by VeriSign, shows limited data:

**Thin Registries: .COM and .NET – Sample Thin Registry Whois Response**

The ***Referral URL***, [http://www.melbourneit.com](http://www.melbourneit.com/), provides a link to Registrar Melbourne IT which, in turn, provides the full, or “thick,” Whois response with the full Registrant Whois contact data:

**Thin Registries: .COM and .NET –**

**Sample Registrar Whois Response (Melbourne IT)**

[KK: Table is missing]

The .COM registry currently numbers over 100 million domain names, with over 944 Registrars.

The other gTLDs, including .ORG, .BIZ, .INFO and .JOBS, are “Thick Registries.” Both Registries and Registrars hold the full Whois data, and both publish full contact data in response to Whois searches.

Thus, for ***amnesty.org***, of Amnesty International, both PIR (the Registry) and Network Solutions (the Registrar) respond with the full contact data listed in the “sample registrar Whois model” above.

Although the .COM and .NET Whois models have remained unchanged for 11 years, there are some recommendations underway within the GNSO asking the community to consider the value of moving thin registries to a “thick Whois” model. Published on November 22, 2011, the comments asks the Community what “positive and/or negative effects” may arise from such a change.[[9]](#footnote-10) As this evaluation is now taking place, it is not an existing policy which the Review Team could evaluate. However, we note the proceeding could lead to significant changes in the area.

B. Whois Policy: Buried in the Contracts of Registry and

Registrar Agreements

Modern Whois Policy is buried in the contracts of current Registry and Registrar Agreements. To the best of the Review Team's knowledge, there is no “one Whois policy” and no single place or one web page to find it. Rather, we pieced Whois policy together through multiple contracts, appendix sections, and web pages. Findings at the end of this chapter will show that we consider way of sharing policy unsatisfactory, and we hope to improve it.

*It is in the contracts*

The Whois Policy for ICANNs current Registries is largely set out in their contracts with ICANN. Currently, each Registry negotiates its own contracts with ICANN, and ICANN sets out requirements for the Whois service and Whois data. Generally, the “Whois Specification” can be found in the appendices of the Registry Agreements, all posted individually on the ICANN website. [www.icann.org/en/registries/agreements.htm](http://www.icann.org/en/registries/agreements.htm).

In contrast, contracts for ICANNs 944+ Registrars are not individually negotiated. Currently, they are signed onto one of two contracts: the 2001 Registrar Accreditation Agreement (RAA) or the 2009 RAA. Both contracts contain numerous provisions regarding Whois service and data, and set out requirements for the ACCESS and ACCURACY of Whois data. 2001 RAA:<http://www.icann.org/en/registrars/ra-agreement-17may01.htm> and 2009 RAA: [www.icann.org/en/registrars/ra-agreement-21may09-en.htm](http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm) The Whois provisions of the two contracts are very close in their language, intent and goals.

This Policy chapter attempts to place the Whois Policy in one place for the first time. It provides an overview of ICANN's Whois Policy as pieced together through the Registry and Registrar Agreements and contracts as well as “Consensus Procedures” passed by the Generic Names Supporting Organization and ICANN Board to supplement this policy.

1. **ACCESS to the Whois Service – Registry Contracts**

Both Thick and Thin Registries commit themselves to providing access to the Whois Service, and Whois Data, in two ways:

* + via a free web page, and
  + through a free Port 43 service.

The web page allows realtime access to Whois data in individual searches; the Port 43 access allows automated queries by machine. There is a further obligation to provide third-party bulk access, provided the Whois data is not misused.

“Thick Registries” are those that agree to host the full Whois contact data, as provided to them by the Registrars (who register the domain names and receive the data directly from the Registrants). Afilias' .INFO Registry is an example of existing Registry contractual obligations:

**Whois Specifications, .INFO Agreement, Appendix 5**

**[KK: Table is missing]**

The web page access is basically the same across websites:

**Whois Website Access**

The Port 43 Access is more complicated, and the contractual requirements set out some standards for this machine-based access:

**Port 43 Access to Whois Data**

**[KK: Table is missing]**

As discussed above, the .COM and .ORG Registries, both run by VeriSign, operate on more streamlined rules, with VeriSign publishing only the data it collects from Registrars, including domain name, Registrar and name servers, with a “Referral URL” to the Whois search of the appropriate Registrar.

Occasionally, Registries serving more targeted communities have received slight modifications to their Whois requirements to reflect specific needs.

1. **ACCESS to the Whois Service – Registrars**

GTLD Registrars sell domain names directly to the public. They hold the “registrant relationship,” and thus collect the personal information, including the Whois data, for their business purposes, e.g., renewal notices, for Whois service purposes and to provide to the Registry, if it is a thick top level domain.

On the Whois topics of ACCESS to the Whois service and its data, the 2001 and 2009 RAAs reflect the same policy with almost identical language. Specifically, like the registries, Registrars must provide free access to a web service for individual searches, and Port 43 for automated ones:

**Free web page and Port 43 Whois Service Access**

**Both Section 3.3.1**

**2001 and 2009 Registrar Accreditation Agreements**

**[KK: Table is missing]**

Further, the agreements state the data to be published,

**Whois Data**

**Both Section 3.3.1.1-3.3.1.8**

**2001 and 2009 Registrar Accreditation Agreements**

[KK: Table is missing]

Additional contract sections provide additional requirements of Registrars, including escrow and prompt updates:

**Additional RAA ACCESS Provisions**

**2001 and 2009 Registrar Accreditation Agreements**

[KK: Table is missing]

Both RAAs feature a major ACCESS limitation that the Registrars must allow Whois searches for lawful purposes, but limit those supporting “mass, unsolicited commercial advertising” and similar abuses:

**One ACCESS Limitation**

**2001 and 2009 Registrar Accreditation Agreements**

**Both Section 3.3.5**

[KK: Table is missing]

Both Registrar contracts require Registrars to agree to accept future policies as set out by Consensus policies that may be passed by the GNSO and ICANN Board. Four such Consensus Policies for Whois have been passed and are discussed in Section C below.

1. **ACCURACY of the Whois Data – a Registrant and Registrar Responsibility**

Among the most important of the Registrar's Whois requirements is the obligation to work closely with the Registrant, its customer, to collect accurate and reliable Whois contact details.

**Specifically, ICANN policy makes the Registrant, called “the Registered Name Holder” in the contracts, responsible for providing accurate Whois information.**

**ACCURATE Whois Data Requirement**

**Both Section 3.3.7.1**

**2001 and 2009 Registrar Accreditation Agreements**

[KK: Table is missing]

Failure by the Registrant to provide such data can result in cancellation of the domain name:

**Failure to Provide ACCURATE Data**

**Section 3.7.7.2**

**2001 and 2009 Registrar Accreditation Agreements**

[KK: Table is missing]

The Registrar, in turn, is required to share with the Registrant a clear idea of the purposes of how the data will be used, which largely consists of open and public access to the Whois data:

Sec. 3.7.7.4 – 2001 and 2009 RAAs

* The ***purposes*** for which any Personal Data collected from the applicant are intended to be used for;
* The ***intended recipients or categories of recipients of the data*** (including the Registry Operator and others who will receive the data from Registry Operator);”
* ***Which data are obligatory*** and which data, if any, are voluntary; and
* How the Registered Name Holder or ***data subject can access and, if necessary, rectify the data*** held about them. Sec. 3.7.7.4, 2001 and 2009 RAA

The Registrar further commits to processing the data appropriated and taking reasonable steps to protect it from misuse:

Sec. 3.7.7.7 and 3.7.7.8, 2001 and 2009 RAA

* ***Not process the Personal Data*** collected from the Registered Name Holder ***in a way incompatible with the purposes and other limitations about which it has provided notice to the Registered Name Holder***
* ***Take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access or disclosure, alteration, or destruction***.

Under more recent ICANN Consensus Policies, Registrars send annual notices to Registrants asking them to review and update contact information that may have changed over time, e.g., a new cell phone number or an updated business address (***Annual Data Reminder Policy*** discussed under “Consensus Policies” in Section C below).

Further, Registrars agree to take reasonable steps to investigate claimed inaccuracies, and seek correction from Registrant as appropriate. [Susan, James, include a further citation. It is in the contracts as an “area for further development].

As you will see in the RAA language a registrar is required to verify information at the time of registration but in practicality this does not happen. In our discussions with ICANN compliance they only expect the registrar to notify the registrant of the inaccuracy report. 3.7.8 Registrar shall abide by any specifications or policies established according to Section 4 requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

The registrant has a responsibility to respond to the yearly notice to update registration information and respond when it is reported as inaccurate but it is simply “I have reviewed the information and it is correct” I do not know what happens when a registrant does not respond.

The Review Team created an overview of the responsibilities of the Whois Data and its Accuracy below:

**Summary Analysis by Review Team**

**Whois Data Responsibilities Under Existing Policies**

[KK: Table is missing]

1. **PROXY and PRIVACY Registrations**

A special set of cases exist in which the Registrant seeks additional protections for its personal data so that it will *not* be easily found in globally-available Whois databases. The Review Team heard from all members of the ICANN gTLD communities on the importance of this type of service.

Specifically, companies, organizations and individuals shared their need, use and value of proxy and privacy services, including:

* For companies where an upcoming merger, new product or service name, new movie name, or other new product launch, involves a domain name which should not yet be directly associated with the business (to avoid market speculation and other negative business consequences). Companies use proxy services or individuals such as attorneys who act as proxies.
* Organizations noted the danger of operating in a country or region in which they are a religious, political or ethnic minority, or share information about moral or sexual issues that may be controversial in some areas, such as gay rights. A synagogue in an unfavorable country might use a proxy service so that it can operate a website to share its service times, but not its street address, to avoid further bombings.

(SK) comment: I agree with Peter that we should tone this language down]

* Individuals serve as proxies for their friends and family to bring parents and children online and provide them with websites.
* Webmasters and Webhosts regularly register domain names for an array of clients as a first step in beginning the development of their websites.

Two types of services have emerged as a market response to the need for special services. Called proxy and privacy services, the terms are used interchangeably, but the Review Team found their meanings have some key differences:

* ***Privacy Services*** provide the Registrant's Name, but the Privacy Service's contact information. The Privacy Service passes on non-spam messages to the Registrant, particularly legal notices, acting as a type of “registered agent.”

* ***Proxy Services*** register the domain name and license it to another for use.

**(AJ) comment: please decide whether you wish to adopt these definitions of privacy services /proxy services or if you would rather go for these instead:**

*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.

Law enforcement shared its concern over the abuse of proxy services by criminals seeking to hide, companies defrauding customers, and parties attacking the security of the Internet including by botnets and malware.

The Registrar Accreditation Agreements speak specifically to the issue of registering a domain name through a third party, but do not use the terms “proxy and privacy.” Rather they talk about the “Registered Name Holder” and the Licensee and require “timely resolution” of problems that may arise:

**Ownership and Responsibility of the Domain Name by the Proxy**

**Section 3.7.7.3, Part 1**

**2001 and 2009 RAA**

**[KK: Table is missing]**

The RAAs also call on Registered Name Holder to be responsible for the “wrongful use” of the domain name unless it “promptly discloses” the current contact information of the licensee on “reasonable evidence of actionable harm.”

**Disclosure of the Underlying Licensee**

**Section 3.7.7.3, Part 2**

**2001 and 2009 RAA**

[KK: Table is missing]

Proxy and privacy services are among the least developed of the Whois policy areas. As discussed in Section \_\_\_ of Chapter \_\_\_, the Review Team heard many complaints about these services from Law Enforcement and others, suggesting that additional policies may be appropriate in this area.

1. **Four ICANN Consensus Policies and One Consensus Procedure**

In addition to the “static contracts” of the RAA's and Registry Agreements, both sets of Contracted Parties (Registries and Registrars) agree to comply with ICANN “Consensus Policies.” Developed through ICANN's bottom-up, policy-making process, these Consensus Policies go through the “policy development process” with:

* + Working group research and development,
  + Community notice and comment
  + Final recommendations to the GNSO Council, and
  + If appropriate, review and approval by the GNSO Council, and then the ICANN Board.

Since ICANN's creation in 1999, eight Consensus Policies have been created by the Generic Names Supporting Organization, and four of those have been Whois consensus policies. The four Consensus Policies, posted at <http://www.icann.org/en/general/consensus-policies.htm> are:

***- Whois Data Reminder Policy (2003)***

***- The Restored Name Accuracy Policy (2004)***

***- Whois Marketing Restriction Policy (2004) which contains the results of two separate recommendations to try to bar use of the Whois data for marketing and re-use.***

In greater detail, each Consensus Policy creates a new requirement for Registrars, and seeks an improvement to the Accuracy of the Whois Data, or a Limitation to the Abuse of the Whois Data:

1. ***Whois Data Reminder Policy –*** at least once a year, Registrars must email all Registrants and remind them to review and update their Whois data.

[www.icann.org/en/registrars/wdrp.htm](http://www.icann.org/en/registrars/wdrp.htm)

1. ***The Restored Name Accuracy Policy –*** If the Registrar has deleted a domain name because it had incorrect contact data, or there was no response to the Registrar's requests for information, the name must remain on Hold until the Registrant provides updated and accurate Whois data.

<http://www.icann.org/en/registrars/rnap.htm>

1. ***Whois Marketing Restriction Policy*** – This policy, a combination of two distinct GNSO policy recommendations, creates two policy changes to the Registrar Accreditation Agreement:

a. Registrars must require third parties “to agree not to use the [Whois] data to allow, enable, or otherwise support any marketing activities.”

b. Registrars must “agree not to sell or redistribute the [Whois] data” (with some exceptions). <http://www.icann.org/en/registrars/wmrp.htm>

While some feel that the path towards progress on the Whois has been too slow, others see the fairly large number of Consensus Policies devoted to Whois as an indication of attention spent on important issues.

*And a Consensus Whois Procedure*

PN: delete [~~Strangely,~~] ICANN has yet another process in the gTLD Whois policy. Called a “Consensus Procedure” it was adopted in 2008 and lays out “how ICANN will respond to a situation where a registrar/registry indicates that 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.” ***ICANN Procedure For Handling WHOIS Conflicts with Privacy Law,*** <http://www.icann.org/en/processes/icann-procedure-17jan08.htm>

The Procedure allows a Registrar or Registry to come to ICANN to discuss how it will respond to a active investigation of illegality taking place by government and/or law enforcement officials. Specifically, there must be an active investigation underway:

* 1. At the earliest appropriate juncture on receiving notification of an investigation, litigation, regulatory proceeding or other government or civil action that might affect its compliance with the provisions of the Registrar Accreditation Agreement (“RAA”) or other contractual agreement with ICANN dealing with the collection, display or distribution of personally identifiable data via WHOIS ("WHOIS Proceeding"), a registrar/registry should provide ICANN staff with the following:

The procedure was criticized at the time of its creation for requiring Registries and Registrars to be the target of an investigation or litigation *before* they can seek to change their Whois practices to reflect their understanding of local and national laws. It was noted that most businesses seek to proactively comply with laws, prior to being challenged.

To date the Procedure has been used only once by .TEL. [Liz can you share the details... ]

*C. Government Advisory Committee Calls for Additional Policy Review*

Numerous parties outside the GNSO have exhibited a great interest in the Whois proceedings, including the Government Advisory Committee (GAC) which has issued four key Communiques with guidance on Whois. The GAC recommended studies on the use and misuse of public Whois data, among other recommendations.

In response, the GNSO has put together four Whois studies, now in progress, at the cost of $530,000 to:

**The 4 GNSO Whois Studies Now in Progress**

| **Whois “Misuse” Study** – This study will assess whether public WHOIS significantly increases harmful acts and the impact of anti-harvesting measures. | **Whois Registrant Identification** – This study will examine information about how domain name  registrants are identified and classify the various types of entities that register domains, including natural  persons, various types of legal persons and Privacy and Proxy service providers. |
| --- | --- |
| **Whois Proxy and Privacy “Abuse”--** This study will compare a broad sample of Privacy and  Proxy-registered domains associated with alleged harmful acts to assess: 1) how often bad actors try to  obscure identity in WHOIS; 2) how this rate of abuse compares to overall use of proxy and privacy  services; and 3) how this rate compares to alternatives like falsified Whois data, compromised machines,  and free web hosting. | **Whois Proxy and Privacy Relay and Reveal Study-**  The original study would analyze communication  relay and identity reveal requests sent for privacy- and proxy-registered domains to explore and document  how they are processed, and to identify factors that may promote or impede timely communication and  resolution. |

Letter from ICANN Chair Peter Dengate Thrush to GAC Chair Heather Dryden, on the Whois Studies funded and underway, June 11, 2011, <http://www.icann.org/en/correspondence/dengate-thrush-beckstrom-to-dryden-22jun11-en.pdf>

It is expected that the results of these Whois studies, due in 2012, will provide important information for future Whois policy discussions.

**Chapter 5:**

**An Evaluation (Audit?) of**

**ICANN's Efforts to Monitor and Enforce Its Policies “Compliance Efforts”**

**A. 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 successful policy 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”[[10]](#footnote-11) 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 Compliance effort**

The WHOIS Review Team has had extensive contact with ICANN’s compliance team throughout 2011. Having conducted an indepth 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.

In order for a policy to be effective, it must not only be implemented, but also communicated effectively. Communication of policy is important because it feeds a public awareness of the norms and standards expected. Without effective communication, the legitimate expectations of the distinct stakeholder groups who rely on WHOIS will remain unmanaged, leading to sometimes unnecessary conflict, or complaints.

Our analysis of your website, and the effectiveness of your programme endorsed what you yourselves told us – ICANN’s compliance effort has historically been overstretched, and under resourced. It has struggled to obtain priority (in terms of strategy, budget or visibility) within the organisation, and to fill vacant positions.

As we are poised for the launch of new gTLDs, bringing a larger landscape, and new actors, this is a matter of deep concern to the WHOIS Review Team, which the entire community should share. For industry self-regulation to continue, it should be effective, impartial and seen to be so.

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. The practical impact of this is that a disconnect occurs, for example, 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.

Please also refer to appendix ……

**[KK: Propose adding Emily's Compliance Findings here (from the Gap Analysis she added it to in the most recent draft]**

**c) ICANN Staff's Compliance Gaps**

1. **Communication**

* **The Compliance Team’s o**perating principles are generally good, but the use of jargon is out of place in high level principles.
* 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.
* 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**

* 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.
* 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.

1. **Investigating complaints of non-compliance**

* 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 some 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.
* 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.

1. **Other WHOIS Related work and efforts – Data Accuracy**

* 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 develop a methodology to measure overall accuracy, publish performance targets, and actively collaborate with registrars and registrants to improve data accuracy.
* 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 Reminder Policy is ineffective in achieving its goal of improving accuracy of data. Despite the dedication of considerable resources both by the Compliance Team and Registrars in sending out annual data reminders, the lack of follow-up renders the entire action ineffective. Simply put, no one knows what impact the policy has in improving the accuracy of WHOIS data.**
* 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.
* **It is unclear what the response of ICANN the Corporation has been to the Data Accuracy Study. It is noted that the study was undertaken on the iniative of the GNSO, but it is clearly relevant to the work of Compliance (as demonstrated by the Compliance Team’s inclusion of the study in their introduction of their work). If no follow up is done, 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.**

**Chapter 6**

**Internationalized Registration Data and the**

**Difficult Problem of Whois Translation**

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 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[[11]](#footnote-12) 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[[12]](#footnote-13). 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)[[13]](#footnote-14). The need for internationalized registration data has also been highlighted in the recent SSAC report SAC 051[[14]](#footnote-15). 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)[[15]](#footnote-16) 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[[16]](#footnote-17).

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[[17]](#footnote-18), 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).

**Chapter 7**

**Consumers of Whois Data and Consumer Trust**

**[Propose we move the Law Enforcement Questionnaire materials here, the Survey of Consumers, and much of the Comments from the Gap Analysis (from Consumers, namely, business, IP, noncommercial and individual consumers of Whois data]**

**I have sent suggestions to Peter, Lynn and Emily...**

**Chapter 8**

**Gap Analysis (content owner: Peter Nettlefold & Emily Taylor**

**[Compliance gaps]**

**Similarly, I have sent edits to Peter on this one, KK)**

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.[[18]](#footnote-19)

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.[[19]](#footnote-20)

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.[[20]](#footnote-21)

In their 2009 study, 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.[[21]](#footnote-22)

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 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[[22]](#footnote-23). [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.[[23]](#footnote-24)

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’*.*[[24]](#footnote-25)

[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[[25]](#footnote-26).

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 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.[[26]](#footnote-27)

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 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[[27]](#footnote-28). 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 [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.[[28]](#footnote-29)

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.

Throughout its work, the WHOIS Review Team was keen to compare gTLD WHOIS policy and its implementation with other examples of good practice in the domain name environment. A survey by CENTR (The Council of European National TLD Registries) of its membership, many of which operate under a data protection regime, indicates that 66% of the 21 registries surveyed allow the addresses of private individuals to be hidden from the public WHOIS service.  In a separate survey on release of "opted out" registrant data 14 out of 22 ccTLD’s (64%) noted they would provide data to Law Enforcement and a further 8 stated they provide information to law enforcement only with a warrant or court order.  Full details of the CENTR surveys and comments by individual ccTLDs are contained at Appendix [ ]. The WHOIS Review Team thanks those ccTLDs and CENTR for sharing this information.

The consensus procedure also appears to be consistent with **t**he 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.[[29]](#footnote-30) 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.

**(AJ) Please decide whether you wish to adopt these definitions or whether you would rather go for these instead:**

*Privacy Services* provide the Registrant's Name, but the Privacy Service's contact information. The Privacy Service passes on  non-spam messages to the Registrant, particularly legal notices, acting as a type of “registered agent.”

*Proxy Services* register the domain name and license it to another for use.

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.

Some 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 are uncontactable 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 untrusted parties. 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, TWI 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](#201106) (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](#201106) (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](#201106) (20110428-1).

Together these studies are 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’.[[30]](#footnote-31) 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]

KK: Propose moving IDN section to its own chapter, and it is inserted above as Chapter 6]

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 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[[31]](#footnote-32) 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[[32]](#footnote-33). 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)[[33]](#footnote-34). The need for internationalized registration data has also been highlighted in the recent SSAC report SAC 051[[34]](#footnote-35). 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)[[35]](#footnote-36) 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[[36]](#footnote-37).

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[[37]](#footnote-38), 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).

[KK end of proposed Move]

**[Propose moving this section, in full, and it's great, back into Compliance Chapter, now Chapter 5, which is now quite streamlined and short.]**

1. **Compliance Gaps**

**ET ADDED [NB THIS IS TEXT THAT HAS BEEN STABLE SINCE MdR with MINOR ADJUSTMENTS – REINTRODUCED FROM COMPLIANCE LETTER. NEW TEXT IS INCLUDED N BOLD]**

1. **Communication**

* **The Compliance Team’s o**perating principles are generally good, but the use of jargon is out of place in high level principles.
* 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.
* 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**

* 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.
* 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.

1. **Investigating complaints of non-compliance**

* 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 some 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.
* 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.

1. **Other WHOIS Related work and efforts – Data Accuracy**

* 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 develop a methodology to measure overall accuracy, publish performance targets, and actively collaborate with registrars and registrants to improve data accuracy.
* 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 Reminder Policy is ineffective in achieving its goal of improving accuracy of data. Despite the dedication of considerable resources both by the Compliance Team and Registrars in sending out annual data reminders, the lack of follow-up renders the entire action ineffective. Simply put, no one knows what impact the policy has in improving the accuracy of WHOIS data.**
* 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.
* It is unclear what the response of **ICANN the Corporation has been** to the Data Accuracy Study. **It is noted that the study was undertaken on the iniative of the GNSO, but it is clearly relevant to the work of Compliance (as demonstrated by the Compliance Team’s inclusion of the study in their introduction of their work). If no follow up is done, t**his 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.

**[End Proposed Move section]**

* **Conclusion**

**ET ADD**

**The WHOIS has been a source of long-running discussion at ICANN. This apparently simple look-up service raises issues of data accuracy, privacy, cost, policing and consumer trust. Each of the issues is important, and this is sometimes lost in the heat of the debate.**

**We have found little consensus on the issue. More concerning, we find little coordinated effort to achieve consensus in this important issue. Neither ICANN the corporation nor ICANN the community has seen the need to charge an individual or group as responsible for WHOIS. This we find to be a significant oversight, because without such coordinating effort, the small steps required for consensus may never be taken.**

**To help inform the debate, ICANN has adopted a recent trend of “the study” as a surrogate for action. Significant sums have been invested, and (From compliance letter)** the WHOIS Review Team would welcome a more joined up approach in future, which would view such studies as a resource for the benefit of the entire ICANN Community. Whilst it is laudable to adopt an evidence based approach, there must be tangible, measurable follow up in order to capitalize on the investment made in the reports.

*Lack of Documented policy*

One of our earliest findings has been our inability to find a clear, concise, well-communicated WHOIS Policy. In this case, the policy is divined from its implementation. As a result, what might have been simple has become complex, difficult to understand, or to identify the parties responsible for it.

*Effectiveness of consensus policies*

**The WHOIS Data Reminder Policy and its implementation we find to be ineffective in achieving the objective of improving data accuracy.**

***Internationalised Domain Names***

**Perhaps it should be no surprise that within this environment, policy and implementation have not kept pace with the real world. A significant example of this is Internationalised Domain Names (IDN), which have been available for registration at the second level for over a decade, and at the Top Level for more than a year, without a corresponding change to the policies relating to WHOIS. The NORC Study on Data Accuracy highlighted IDN contact data as a major cause of apparent inaccuracy, because the work to find a common format for presentation and transliteration of WHOIS contact data in IDNs has not yet been completed.**

***Data Accuracy***

**The NORC Study on Data Accuracy in 2009-2010 found that over 20% of gTLD WHOIS data was so inaccurate that it was impossible to reach the registrant in any way. In numbers, this translates to over 20,000,000 registrations in .com alone. Whilst the WHOIS Review Team in general would like to see a higher level of accuracy throughout the system, it is unacceptable to have such a high percentage with obviously inaccurate data. Those domain names should be subject to cancellation on the terms of the RAA, but the feedback which we received from many stakeholder groups was that they perceived that no one is doing anything.**

***Availability – proxy and privacy services***

The community has not handled the issue of privacy in a timely or effective manner.

As the community hesitateda 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.

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

**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

[

**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.

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.

**[KK Add: Chapter 9 ]**

**Recommendations**

**ET ADD (From compliance letter)**

With regard to the recent studies commissioned within the ICANN Community (no matter which entity within the Community commissioned the study) which are directly relevant to WHOIS policy or its implementation (eg the NORC 2009-10 Data Accuracy Study), we encourage the **Board** within 3 months of the publication of studies:

* To explore what opportunities are highlighted for operational improvements, and whether the studies highlight ineffective policy or implementation.
* Where such gaps are identified, the Board should take all necessary actions to ensure that corrective measures are taken, at whatever level in the organisation or community they exist, and set appropriate timeframes for reports to be made and action to be taken.

1. **Recommendations from our Brainstorming Session (Saturday afternoon in Dakar)**
2. 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 NORC Data Accuracy Study, 2010) by 50% within 12 months and by 50% again over the following 12 months. (SK) comment: this needs more discussion or detail how are we recommending ICANN do this?
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 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. 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. **IDN Recommendations**
3. 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**

(SK please delete the following language and insert the original language highlighted in yellow:

Definitions

***A proxy service provider*** *registers the domain name on the registrant’s behalf and then licenses the use of the domain name to the registrant. The contact information in a WHOIS directory for a domain name registered with a proxy service is that of the proxy service provider.*

From 2009 RAA 1.20 "Affiliated Registrar" is another ICANN accredited registrar that operates under a common controlling interest.

**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. a registrar is required to disclose their relationship with a Retail proxy service provider to ICANN.
2. A retail proxy service provider should follow best practice guidelines developed by the community.  These may include the following:
   1. standardized relay and reveal processes and timeframes;

establish a standardized process for requesting contact information for a proxy registration

24 hour  response to provide requested contact information when requested by Law Enforcement;

5 day business response when requested by a non LE third party

* 1. guidance on the appropriate level of publicly available information on the registrant;
  2. maintenance of a dedicated and available  abuse point of contact;
  3. public disclosure of contact details and the physical address of the retail proxy service provider; and
  4. validate registrant contact information.

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 encourage and incentivize registrars to interact with the retail service providers that adopt the best practices.
3. 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.
4. 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.
5. 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.

**(LD)’s recommendations on centralized WHOIS repository:**

Summary:

ICANN should set up and maintain a web interface to access all the WHOIS services in order to ease access to the WHOIS data.

Presumption:

The AoC 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."

Observation:

An User Insight Report came up with the following results:

* Almost nobody is aware of whois
* Almost nobody is able to query a whois server correctly
* Whois queries were done on websites which occur first in the search engine results. Usually those pages are overloaded with advertisments.

Detailed recommendation:

  ICANN should set up a dedicated, multilingual website to allow "unrestricted and public access to accurate and complete WHOIS information" even for those people which have problems with the plain WHOIS protocol.

The WHOIS information should be collected by following the thin WHOIS approach starting at whois.iana.org. The service should display the contractual relationships which are revealed by the WHOIS referals in a clear and understandable way. The results should be mark clearly the relevant information "including registrant, technical, billing, and administrative contact" data.

The server needs to be run by ICANN itself, because the "timely, unrestricted and public access" is usually rate limited, stripped or even blocked by the various WHOIS server administrators for uncontractual third party access. ICANN itself is the only party having the power to overcome those limits using its contratual compliance.

1. **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> (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> (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> (Draft Recommendations discussed in Dakar; V1; 24Oct2011)
4. Current IDN paper <https://community.icann.org/display/whoisreviewprivate/Internationalization+of+Domain+Name+Registration+Data>

1. http://www.icann.org/en/presentations/gnso-mar-28jun06.pdf [↑](#footnote-ref-2)
2. http://www.icann.org/en/committees/security/sac051.pdf [↑](#footnote-ref-3)
3. whois://whois.icann.org or http://whois.icann.org [↑](#footnote-ref-4)
4. 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-5)
5. 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-6)
6. 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-7)
7. 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-8)
8. For full comments, please see Appendixes – Public comments [↑](#footnote-ref-9)
9. Inter-Registrar Transfer Policy Part B – Recommendation #8 and #9 Part 2 – Staff Proposals, <http://www.icann.org/en/announcements/announcement-2-22nov11-en.htm> (deadline for comment Dec 31, 2011). [↑](#footnote-ref-10)
10. ICANN Compliance Team’s Operating Plan, item 1 <http://www.icann.org/en/compliance/>, accessed 7/7/11 [↑](#footnote-ref-11)
11. Available at <http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf>. [↑](#footnote-ref-12)
12. See [http://www.icann.org/en/minutes/resolutions-26jun09.htm#6](#6). [↑](#footnote-ref-13)
13. 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-14)
14. Availble at <http://www.icann.org/en/committees/security/sac051.pdf>. [↑](#footnote-ref-15)
15. See <http://www.icann.org/en/topics/idn/> for more details. [↑](#footnote-ref-16)
16. See <http://www.ietf.org/mail-archive/web/weirds/current/maillist.html> for archive of the discussion. [↑](#footnote-ref-17)
17. See WHOIS++ (RFC 1834), RWhois (RFC 2167), and CRISP (RFC 3707). [↑](#footnote-ref-18)
18. Time Warner Inc., *Comments of Time Warner Inc.*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.3 [↑](#footnote-ref-19)
19. GAC Principles Regarding gTLD WHOIS Services (28 March 2007), section 4.1 [↑](#footnote-ref-20)
20. Intellectual Property Constituency, *Comments of the Intellectual Property Constituency*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.5 [↑](#footnote-ref-21)
21. 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-22)
22. 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-23)
23. ICANN, *gTLD Applicant Guidebook* (30 May 2011) [↑](#footnote-ref-24)
24. Time Warner Inc., *Comments of Time Warner Inc.*, <http://forum.icann.org/lists/whoisrt-discussion-paper/> (23 July 2011), p.3 [↑](#footnote-ref-25)
25. 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-26)
26. 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-27)
27. [↑](#footnote-ref-28)
28. 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-29)
29. <http://blog.icann.org/2011/04/cylab-at-carnegie-mellon-university-selected-to-conduct-study-of-whois-misuse/> [↑](#footnote-ref-30)
30. The review team notes that this is consistent with ICANN-approved arrangements in place in the UK based Telnic. [↑](#footnote-ref-31)
31. Available at <http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf>. [↑](#footnote-ref-32)
32. See [http://www.icann.org/en/minutes/resolutions-26jun09.htm#6](#6). [↑](#footnote-ref-33)
33. 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-34)
34. Availble at <http://www.icann.org/en/committees/security/sac051.pdf>. [↑](#footnote-ref-35)
35. See <http://www.icann.org/en/topics/idn/> for more details. [↑](#footnote-ref-36)
36. See <http://www.ietf.org/mail-archive/web/weirds/current/maillist.html> for archive of the discussion. [↑](#footnote-ref-37)
37. See WHOIS++ (RFC 1834), RWhois (RFC 2167), and CRISP (RFC 3707). [↑](#footnote-ref-38)