SAC058
SSAC Report on Domain Name Registration Data Validation

A Report from the ICANN
Security and Stability Advisory Committee (SSAC)
27 March 2012

Preface

This is a report to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning the issue of domain name registration data quality. The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (*e.g.*, matters pertaining to the correct and reliable operation of the root name system), administrative matters (*e.g.*, matters pertaining to address allocation and Internet number assignment), and registration matters (*e.g.*, matters pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors, references to SSAC members' biographies, statements of interest, and SSAC members' objections to the findings or recommendations to this report are at end of this report.

Table of Contents

Executive Summary

Various studies that assessed the quality of domain name registration data have collectively shown that the accuracy of the data needs to be improved. In this report, the SSAC examines the feasibility and suitability of improving registration data accuracy through validation. Specifically, the SSAC:

- Proposes validation taxonomy for community consideration, and
- Explores the suitability and efficacy of various techniques of validating registration data elements in light of the taxonomy.

Finally, based on the taxonomy and suitability and feasibility of implementing validations, the SSAC makes the following recommendations for the ICANN community to consider.

Recommendation 1: The SSAC recommends that the ICANN community should consider adopting the terminology outlined in this report in documents and discussions.

Recommendation 2: As the ICANN community discusses validating contact information, the SSAC recommends that the following meta-questions regarding the costs and benefits of registration data validation should be answered:

- What data elements need to be added or validated to comply with requirements or expectations of different stakeholders?

- Is additional registration processing overhead and delay an acceptable cost for improving accuracy and quality of registration data?

- Is higher cost an acceptable outcome for improving accuracy and quality?

- Would accuracy improve if the registration process were to provide natural persons with privacy protection upon completion of multi-factored validation?

Recommendation 3: The SSAC recommends that the ICANN community should seek to identify validation techniques that can be automated and to develop policies that incent the development and deployment of those techniques. The use of automated techniques may necessitate an initial investment but the long-term improvement in the quality and accuracy of registration data will be substantial.

1. Introduction

The American National Dictionary for Information System defines data quality as "the correctness, timeliness, accuracy, completeness, relevance, and accessibility that make data appropriate for use."[1]

Various studies that assessed the quality of domain name registration data have collectively shown that the accuracy of the data needs to be improved[2]

To improve registration data accuracy, there needs to be 1) an incentive for the registrant to submit accurate data, or 2) efforts by registry / registrar to follow up and check the accuracy of the submitted data; or 3) both. This report focuses on addressing the first problem, the validation[3] of registration data. It synthesizes from past literature on reasons for registration data inaccuracy; proposes validation taxonomy for community consideration; explores the suitability and efficacy of various techniques of validating registration data elements in light of the taxonomy; and makes a series of recommendations.

The SSAC is a technical advisory committee. As such, in this report the SSAC attempts only to define the problem space and characterize the solution space. The SSAC makes no policy assertions in this report.

2. Accuracy of Registration Data

2.1 Why Accurate Registration Data is Important

In SAC003: *WHOIS Recommendation of the Security and Stability Advisory Committee*, the SSAC outlined two principal reasons to maintain accurate registration data: technical and legal.[4] The technical rationale is that if there are problems with or abuse originating from a resource (*e.g.*, a domain name, route, or Internet Protocol (IP) address), the registration data for the resource is the only source for finding the contact information of the responsible party. For some legal and other law-related purposes (e.g. serving court

[1] See American National Standards Committee (1984), American National Dictionary for Information Systems. McGraw-Hill School Education Group.

[2] For two examples see National Opinion Research Center (2010), Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information at http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf and U.S. Government Accountability Office (GAO) (2005), Internet Management: Prevalence of False Contact Information for Registered Domain Names (GAO publication No. GAO-06-165), Washington, DC at http://www.gao.gov/products/GAO-06-165.

[3] The word "verification", "validation" and "resolution" have been used interchangeably in the various literatures on this topic. For the purpose of this document, the SSAC will use the term "validation."

[4] See ICANN Security and Stability Advisory Committee (SSAC) (2003) WHOIS Recommendation of the Security and Stability Advisory Committee at http://www.icann.org/en/committees/security/sac003.pdf.

papers), the registration data may be the only source for finding the contact information for the responsible party.

In SAC 010: *Renewal Considerations for Domain Name Registrants*, the SSAC observed that registration data often contain "stale" contact information and that this problem can cause difficulties when registrants seek to renew a domain name or modify DNS information.[5] Stale information may prevent registrars from notifying a registrant that a domain registration is about to expire or that changes, possibly unauthorized, have been made to his domain registration. Failure to update information may result in domain hijacking or a dispute over the "ownership" of a domain.

It is important to note in understanding the scale of potential problems from inaccurate information that the difficulties do not arise only in criminal matters. The contexts also can include a simple contact issue, as described above with regard to domain renewals, civil and administrative law enforcement, private actions, and public needs to contact registrants that might arise, for example, when a consumer wants to reach an online seller.

2.2 Reasons for Registration Data Inaccuracy

Many reasons have been offered for the current extent of inaccurate registration data, including several from past SSAC advisories:

1. **Anti-abuse considerations.** Since current access to registration data is public and anonymous, some individuals and businesses submit incorrect information because they do not wish their contact information to be collected and used by miscreants as targets for spam and other attacks [6]

2. **Privacy considerations**. Some people intentionally submit false information because they do not wish to disclose personal contact information that can be accessed publicly and anonymously.[7]

---

[5] See ICANN Security and Stability Advisory Committee (SSAC) SAC010: SSAC Renewal Considerations for Domain Name Registrants (29 June 2006) at http://www.icann.org/en/groups/ssac/renewal-advisory-29jun06-en.pdf.

[6] See ICANN Security and Stability Advisory Committee (SSAC) SAC023: Is the WHOIS Service a Source for email Addresses for Spammers? (23 October 2007) at http://www.icann.org/en/committees/security/sac023.pdf.

[7] See Edelman, B. (2002) Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions" / "Domains For Sale" Cambridge, MA: Harvard University at http://cyber.law.harvard.edu/archived_content/people/edelman/invalid-whois/ and Internet Corporation for Assigned Names and Numbers (ICANN) *WHOIS Data Reminder Policy.* Marina Del Rey, CA: ICANN (2003) at http://www.icann.org/en/registrars/wdrp.htm.

3. **Stealth, intentional deception.** Miscreants intentionally provide false information to obfuscate identification by law enforcement or parties that investigate malicious use of domains.[8]

4. **Little or no corroboration of submitted data.** Current registration requirements take a minimalist approach to validation. Unless credit verification measures are stringently applied for all levels of payment, little or no additional proof of identity and verification of contact information is required when a user registers a domain name.

5. **User error.** Users may mistype when registering domain names. The current validation processes can overlook errors.

6. **User expectation mismatch.** Users may not understand the consequences of the registration data accuracy program and annual obligation to maintain accurate and complete registration data. They also may refuse to take time to check that their contact information is current, or reject the notion that they will forfeit a domain registration simply because some registration data are inaccurate.

As the ICANN community debates and evaluates proposals to improve the accuracy of the domain name registration data, it is important to consider whether these proposals address the underlying problems.

3. Taxonomy of Validation

Verification, validation and resolution have been used interchangeably in various literature on this topic. We choose "validation" to refer to the assessment of data as described by this document. Verification in this document refers to the process of validating. Resolution has an entirely different technical meaning that is out of scope for this document.

The SSAC asserts there are three types of validation for elements of the registration data.

1. **Syntactic Validation** refers to the assessment of data with the intent to ensure that they satisfy specified syntactic constraints, conform to specified data standards, and are transformed and formatted properly for their intended use. For example, if the data element is expected to be an email address is it formatted as an email address? In general, it is expected that syntactic validation checks would be entirely automated and could be executed inline with a registration process, follow up information reviews, and whenever registration data changes.

[8] See Edelman, B. (2002) Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions" / "Domains For Sale" Cambridge, MA: Harvard University at http://cyber.law.harvard.edu/archived_content/people/edelman/invalid-whois/

2. **Operational Validation** refers to the assessment of data for their intended use in their routine functions. Examples of operational validation include 1) checking that an email address or phone number can receive email or phone calls; 2) checking that a postal address can receive postal mail; 3) checking that the data entered are self-consistent, i.e. that all data are logically consistent with all other data. It is expected that many operational validation checks would be automated and some could be executed inline with a registration process.

3. **Identity validation** refers to the assessment that the data corresponds to the real world identity of the entity. It involves checking that a data item correctly represents the real world identity for the registrant. In general, identity validation checks are expected to require some manual intervention.

4. Implementing Validation

In this section the SSAC considers the feasibility of validation of four types of contact information elements. They are name, postal address, email address, and telephone and fax number.[9]

4.1 Validity Period

An essential characteristic of the validation of a data element is the length of time before the validation must be repeated. In addition, there is the question of whether or not the validation must be repeated if the registration data is transferred or otherwise modified in any way.

In the ICANN Registrar Accreditation Agreement (RAA), there is a contractual obligation that "The Registered Name Holder shall provide to Registrar accurate and reliable contact details and promptly correct and update them during the term of the Registered Name registration."[10] The WHOIS Data Reminder Policy, which is an ICANN Consensus Policy, states that at least annually, all registrars must present to the registrant the current WHOIS information, and remind the registrant that provision of false WHOIS information can be grounds for cancellation of their domain name registration, and that registrants must review their WHOIS data, and make any corrections.[11]

---

[9] The SSAC notes that X.509 certificates have been in use for over 20 years. A great deal of experience regarding the feasibility and applicability of validating contact information has been studied and implemented, most of which is valid in this context.

[10] See Internet Corporation for Assigned Names and Numbers (ICANN), (2009) *Registrar Accreditation Agreement.* Marina Del Rey, CA: ICANN at http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#2.

[11] See Internet Corporation for Assigned Names and Numbers (ICANN). (2003) *WHOIS Data Reminder Policy.* Marina Del Rey, CA: ICANN at http://www.icann.org/en/registrars/wdrp.htm.

There are no specific ICANN rules regarding the validation of changes to contact information or whether validation must be repeated when a domain name is transferred. Different contact information elements have different volatility characteristics, which suggests that different validity periods and revalidation requirements may be applicable.

Consider that phone numbers and email addresses tend to be volatile, in part because they are easy to change and usually fairly inexpensive to change. In contrast, physical locations and their related physical address tend to change less frequently and are usually expensive to change. Operational validation of phone numbers and email addresses can typically be automated. Operational validation of physical addresses is more variable, can only be partially automated in many parts of the world, and tends to be more expensive in part because of needing access to various private databases.

The SSAC notes that the actual cost of validation is dependent on many factors that need to be considered at the same time. Some of these factors are the cost of developing and deploying automation where applicable, the cost of a single validation, the cost of repeating the validation, and the cost of maintaining the information and infrastructure necessary to support the process of validation.

In addition, integrating a validity period and a corresponding revalidation upon change or transfer may require changes in the protocols used between the parties involved in the registration process, e.g., the addition of a validity period date or description to registration data elements, which may require a change or extension to EPP (Extensible Provisioning Protocol commonly used between registrars and registries) or the schemas it uses. It may also require changes to registration data service outputs, i.e. WHOIS. This will require further study.

4.2 Name

Regarding the validation of the name of registered domain holders, technical, administrative or billing contacts, the SSAC notes that:

- **Syntactic validation:** To be effective, the script (or writing system) used for a name element must be known. If it is, confirming that the syntax conforms to the script is possible and can be automated. However, the language of a name cannot be determined precisely as many languages (*e.g.* English, Spanish, German) shared the same script (*e.g.* Latin). The current WHOIS protocol (RFC 3912) has not been internationalized and has no mechanism for indicating the character set in use.[12]

[12] See Daigle, L., "WHOIS Protocol Specification," RCF 3912, September 2004. At https://tools.ietf.org/html/rfc3912.

- **Operational validation:** Due to the diversity of names in the world, it may not be possible to operationally verify a name automatically. Consider that real people are named after famous marks, nouns, and other well-known constructs. Creating exception lists for auditing purposes may be an acceptable method in this situation.

- **Identity Validation:** One of many ways to verify that registration data contact information corresponds to a real world entity is to require the submission of physical documentation issued by a government authority. Global identity validation without the physical presence of the real world entity is known to be an especially difficult problem.

4.3 Email Address

An email address is composed of a Left Hand Side (LHS) and Right Hand Side (RHS) separated by the at-symbol (@). The RHS is a domain name and the LHS is a local identifier used for routing purposes once the email is delivered to the Mail eXchanger (MX) server of the domain name.

Syntactic validation: RFC 5322 specifies syntax for a valid email address and RFCs 6530-33 further define syntax for a valid internationalized email address.[13] These checks can be automated.

Operational validation: To verify that an email address is operational, there are several checks that can be done. With respect to the RHS one could check:

- Does the domain name exist in the DNS?
- If it exists, is there an MX record or an A record for it in the DNS?
- If it exists, is there an email validation record for it in the DNS?[14]
- If there is an MX record or an A record, is there a valid SMTP endpoint reachable at the specified location?

With respect to the LHS one could check:

[13] See Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008; Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, February 2012; Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006; and Yang, A., Steele, S., and N. Freed, "Internationalized Email Headers", RFC 6532, February 2012.

[14] See Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", RFC 4406, April 2006 and Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

- Will the endpoint Simple Mail Transfer Protocol (SMTP) accept an email message for the recipient specified at the LHS?

Although these checks could be done automatically, the SSAC notes that the growth of bulk unsolicited emails (commonly called spam) has made the verification of deliverability of email more difficult. Historically, email systems would accept queries asking if a specific recipient was able to receive email and respond appropriately. Today this feature is routinely disabled for various reasons, including protecting privacy and to mitigate harvesting of email addresses.

A more effective verification technique is attempting to deliver an email message that requires explicit user action. In this case, the email address should not be considered valid until the user receives and performs some action described in the email, such as clicking on a web link or replying to the message in a specified way. The SSAC notes however sometimes anti-spam measures could still block these verification emails.

The SSAC notes that if such a verification technique is used, the timing of the verification email message will need to be carefully considered as to how it affects the overall registration process. Sending the verification email as an integral part of the registration process would alter the business process and may affect registration costs. Sending the verification email after registration would risk being ignored by the registrant or could introduce an attack vector. A miscreant, knowing that these verification emails will be sent, could initiate various types of man-in-the-middle attacks. Past security research has shown that such spear-phishing attacks are highly effective.

Identity validation: To verify that an email address is exclusively used by a particular registrant would require contacting the registrant using an out-of-band method, *i.e.*, contacting the registrant without using email. Using the postal information or the telephone information to contact the registrant are two possibilities.

4.4 Telephone Number

Syntactic Validation: E.164 is an International Telecommunications Union Telecommunications Standardization Sector (ITU-T) recommendation that defines the international public telecommunication numbering plan used in the Public Switch Telephone Network (PSTN) and some other data networks.[15] It also defines the format of telephone numbers. Automatic checks can be performed to determine if a phone number complies with the E.164 standard.

Operational Validation: E.164 formatted PSTN addresses (telephone numbers) can be verified by leveraging PSTN databases. The number can be validated up to a sub-address,

[15] See International Telecommunication Union, "E.164 : The international public telecommunication numbering plan," at: http://www.itu.int/rec/T-REC-E.164-201011-I/en.

which usually is all but the last four digits. Verifying whether or not an E.164 conformant phone number can be called requires attempting to connect to it using either the PSTN or the Signaling System No. 7 (SS7) network. Both methods may incur charges.

E.164 numbers are geographically constrained for land-line telephones, but with the advent of the cellular network and number portability the geographic nature of the PSTN has been decoupled and as such any geographic information leveraged from a E.164 number is becoming less valuable. Such geographic information is now, at best, constrained to political boundaries (i.e. countries). Number portability has also blurred the distinction to identifying landlines versus cellular numbers; at one time these were distinct but this is no longer guaranteed. Thus checking whether the telephone number is self-consistent with the postal information may not be a definitive indicator but may be useful as an exception that could be audited.

With the advent of Short Message Service (SMS) one could consider using SMS to verify a phone number; however, this only works for cellular numbers. Having a registrant call from a particular number may pose problems for those that use corporate direct inward dialing (DID) lines where outbound calls are automatically mapped to the main corporate number, frequently without the knowledge of the person making the call. Both may incur charges for either the sender or receiver or both.

Identity validation: To verify that a telephone number is used exclusively by a particular registrant would require contacting the registrant using an out-of-band method, *i.e.,* contacting the registrant without using the telephone number. Using the postal information or the email address to contact the registrant are two possibilities.

The SSAC also notes that identity validation is performed in other contexts, for example, in verifying whether or not the registrant of an E.164 Number Mapping (ENUM) domain name is identical to the assignee of the corresponding E.164 phone number. The applicability of this process and architecture (i.e. RFC 4725) to the identity validation of telephone numbers in this context is an area for further study.[16]

4.5 Postal Address

The Universal Postal Union (UPU) defines an interchange standard for the transmission of name and address data (S.53). The correlation of physical addresses with electronic address elements and communication of address data parsed into standard elements and element sub-types are among the use cases of S.53. The standard elements are defined in S.42, another UPU standard, which defines templates for address elements. These standards are not freely available but may be useful to inform the community regarding all postal address validation processes.

[16] See Mayrhofer, A. and B. Hoeneisen, "ENUM Validation Architecture", RFC 4725, November 2006.

Syntactic Validation: The EPP standard defines an opaque container and loose constraints that can support internationalized postal addresses.

Operational Validation: The postal address can be verified by leveraging postal databases. There are about 200 such databases in the world with about 20 (G20 major economies) being highly accurate.[17] These systems typically enable mapping the address to a latitude and longitude that are fairly accurate. The remainder, or about 180 nations, can be partitioned into two classes (B/C), which have less accuracy. This means that about 180 nations do not provide more than a possibly imprecise method for understanding if a city or geographic region exists.

Within the G20 major economies, about eight have highly accurate address information. While the information is available it is expensive and each country has a different procedure for normalizing an address, which must be done before it can be checked against a postal address database. In addition, existence in the address database does not guarantee that the physical address exists. For example, apartment numbers in the United State Postal Service address database are indicated as a range. As a result, an address may validate as accurate and complete when in fact it is undeliverable.

One way to verify a postal address with a high level of certainty is to attempt to deliver a postal message to it. One might consider validating it similar to how email address verification is done.

Identity validation: To verify that a postal address is exclusively used by a particular registrant would require contacting the registrant using an out-of-band method, *i.e.*, contacting the registrant without using the postal address. Using the telephone number or the email address to contact the registrant are two possibilities.

5. Findings

Finding 1: Data quality is relative to registrants and their purposes.[18]

The quality of data is relative to the purpose (or purposes) of the data. This is not to say that there are no objective aspects of data quality (such as accuracy and consistency), but even these must always be interpreted in terms of the purpose of the data.

Thus, a prerequisite for any effort to improve data quality should be to identify the potential providers (customers) of that data and understand the purposes and intended uses they have in mind. This is an inescapable first step in defining validity criteria for data, since such criteria are necessarily relative.

[17] See G20 Major Economies at http://en.wikipedia.org/wiki/G-20_major_economies.
[18] See Rothenberg, J., (1997) "A Discussion of Data Quality for Verification, Validation, and Certification (VV&C) of Data to be Used in Modeling", RAND Project Memorandum PM-709-DMSO, RAND at http://vva.msco.mil/Ref_Docs/DataQuality/DataQuality-pr.pdf.

In SAC055: *SSAC Comment on the WHOIS Review Team Final Repor*t, the SSAC asserted that the foundational problem facing all "WHOIS" discussions is to understand the purpose of domain name registration data.[19] To facilitate this discussion, in Appendix A the SSAC has outlined some stakeholders of the registration data along with the generally accepted purposes and use cases for registration data according to those stakeholders.

Finding 2: Certain verification measures can be automated, some with only a small amount of investment, and would improve the quality of registration data.

From a technical perspective, certain verification measures can be taken to reduce unintentional errors by registrants; for example, a formal data structure and strong typing of data (e.g., this field must be Arabic numbers only, this field must be alphabetical characters only) can reduce certain typographical errors. Enforcing mandatory submission of data for key data fields may reduce cases where users omit information.

The SSAC notes that accuracy is not directly related to format. Formatting is a way to improve syntactic correctness, not accuracy. For example, ensuring that a telephone number can be submitted using only Arabic numbers, no separators, assures that all numeric submissions are consistent and can be syntactically validated automatically. Similarly, creating a web form that recognizes how different countries compose telephone numbers accomplishes the same objective.

Finding 3: Different contact data elements have different validation cost structures.

The SSAC observes the following characteristics in terms of cost structure for validation.

- There is a large upfront cost in the beginning as nothing is validated. As registrants are validated the number of unverified registrants drops significantly, and thus costs for subsequent years might be more directly related to the validity periods, i.e., the frequency at which data must be revalidated.

- There are economies of scale for validation: costs of per contact data element validation drops as more contacts are validated.

- In EPP registries, registrars are free to create and manage multiple contact objects that refer to the same individual. Thus, the cost of validating the contact data associated with a domain name may be the cost of validating each contact object. However, from an operational cost and registrant experience perspective, validation of a registrant associated with multiple domains might not require each

[19] See ICANN Security and Stability Advisory Committee (SSAC) SAC055: SSAC Comment on the WHOIS Review Team Final Report (14 September 2012) at http://www.icann.org/en/groups/ssac/documents/sac-055-en.pdf.

domain's contact data elements to be re-validated if the registrant's contact data elements are the same for each domain name.

6. Recommendations

Recommendation 1: The SSAC recommends that the ICANN community should consider adopting the terminology outlined in this report in documents and discussions. In particular:

- **Syntactic Validation** - the assessment of data with the intent to ensure that they satisfy specified syntactic constraints, conform to specified data standards, and are transformed and formatted properly for their intended use.

- **Operational Validation** - the assessment of data for their intended use in their routine functions.

- **Identity Validation** - the assessment that the data corresponds to the real world identity of the entity.

Recommendation 2: As the ICANN community discusses validating contact information, the SSAC recommends that the following meta-questions regarding the costs and benefits of registration data validation should be answered:

- What data elements need to be added or validated to comply with requirements or expectations of different stakeholders?

- Is additional registration processing overhead and delay an acceptable cost for improving accuracy and quality of registration data?

- Is higher cost an acceptable outcome for improving accuracy and quality?

- Would accuracy improve if the registration process were to provide natural persons with privacy protection upon completion of multi-factored validation?

Recommendation 3: The SSAC recommends that the ICANN community should seek to identify validation techniques that can be automated and to develop policies that incent the development and deployment of those techniques. The use of automated techniques may necessitate an initial investment but the long-term improvement in the quality and accuracy of registration data will be substantial.

7. Acknowledgements, Statements of Interests, and Objections, and Withdrawals

In the interest of greater transparency, these sections provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent, or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

7.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this Report.

SSAC Members:

Greg Aaron
Jaap Akkerhuis
Jeff Bedser
Don Blumenthal
James Galvin
Rod Rasmussen
Rick Wesson

Staff:
Julie Hedlund
Barbara Roseman
Dave Piscitello
Steve Sheng (editor)

7.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/groups/ssac/biographies-01feb13-en.htm.

7.3 Objections and Withdrawals

There were no objections or withdrawals.

Appendix A: Use Cases for Domain Name Registration Data

In this appendix, the SSAC collected and summarized use cases for the domain name registration data provisioned through the WHOIS protocol. Various Internet stakeholder groups submitted these use cases. This is a starting point to inform the discussions on the purpose of domain name registration data, and is by no means complete.

Members of the Internet Service Providers Constituency[20] use the registration data to:

- To research and verify domain registrants that could vicariously cause liability for ISPs because of illegal, deceptive or infringing content;
- To prevent or detect sources of security attacks of their networks and servers;
- To identify sources of consumer fraud, spam and denial of service attacks and incidents;
- To effectuate Uniform Domain Name Dispute Resolution Policy (UDRP) proceedings; and
- To support technical operations of ISPs or network administrators.

Members of the **Business Constituency**[21] use the registration data to obtain registrant contact information for the following reasons:

- To verify the availability of a name they might wish to register;
- To thwart security attacks of their networks and servers;
- To validate the legitimacy of a website for transactions;
- To identity consumer fraud and cyber-scam incidents;
- To undertake routine reviews to protect their brands;
- To support UDRP and other infringement proceedings; and
- To combat spam.

Members of the **Intellectual Property Constituency**[22] use the registration data to:

- To facilitate commerce (e.g., domain name sales, transfers, and general portfolio management) ;
- To identify cybersquattters and others who infringe trademarks online;
- To investigate those conducting piracy, product counterfeiting, online fraud or

[20] See http://gnso.icann.org/en/issues/whois-privacy/Whois-tf3-preliminary.html#AppendixD

[21] The Business Constituency is a constituency representing customers of providers of connectivity, domain names, IP addresses, protocols and other services related to electronic commerce in its broad sense. The BC membership includes corporations, entrepreneurs, and associations.

[22] See http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CD8QFjAE&url=http%3A%2F%2Fforum.icann.org%2Flists%2Fwhois-rt-draft-final-report%2FpdfBnZfHBVSuN.pdf&ei=LoFXUI-vJKf8iQKP8YHgAw&usg=AFQjCNHqeAQgEWPDWQLA9Qoes_SHpGEESw&cad=rja

phishing schemes over the Internet (many of which involve some degree of trademark counterfeiting to give otherwise anonymous activity the cover of a brand's credibility);
- To prevent or limit damage to customers and business partners victimized by online frauds that are facilitated by trademark infringement and cybersquatting; and
- To assist law enforcement in their efforts to protect consumers against a wide range of criminal activity and online misconduct.

The **Intellectual Property Constituency**[23] uses the registration data in the following way:
- Registrant name – need for context, negotiation and legal action;
- Address – need for service of process;
- Email – need for quick communication;
- Phone no. – again for quick communication; and
- Fax no – less used, but sometimes useful.

[23] http://www.icann.org/en/news/presentations/mutimear-whois-workshop-24jun03-en.pdf