Registration Abuse Policies Working Group

Initial Report

Submitted [TBC]

[ROUGH DRAFT: IN PROCESS.
Version: 9 February 2010]

STATUS OF THIS DOCUMENT

This is the Initial Report of the Registration Abuse Policies Working Group (RAPWG), prepared by ICANN staff for submission to the GNSO Council on [TBC] and posted for public comment. A Final Report will be prepared following the closure of the public comment period.

1. Table of Contents

1. TABLE OF CONTENTS 2

2. EXECUTIVE SUMMARY 3

3. BACKGROUND, PROCESS, AND NEXT STEPS 14

4. DISCUSSION OF CHARTER AND SCOPE QUESTIONS 17

5. POTENTIAL REGISTRATION ABUSES EXPLORED 23

6. MALICIOUS USE OF DOMAIN NAMES 42

7. WHOIS ACCESS 64

8. UNIFORMITY OF CONTRACTS 74

9. META-ISSUES 90

10. CONCLUSIONS, RECOMMENDATIONS, & NEXT STEPS 96

ANNEX I – WORKING GROUP CHARTER 97

ANNEX II - THE WORKING GROUP 100

ANNEX III - RAPWG ATTENDANCE SHEET 1002

2. Executive Summary

2.1 Background

- On 25 September 2008, the GNSO Council adopted a motion requesting an issues report on registration abuse provisions in registry-registrar agreements. The issues report was submitted to the GNSO Council on 29 October 2008 and provides an overview of existing provisions in registry-registrar agreements relating to abuse and includes a number of recommended next steps. In December 2009, the GNSO Council agreed to charter a Working Group to investigate the open issues identified in Registration Abuse Policies report, before deciding on whether or not to initiate a Policy Development Process (PDP).
- A Registration Abuse Policies Working Group (RAPWG) was chartered in February 2009.
- The GNSO Council committed to not making a decision on whether or not to initiate a PDP on registration abuse policies until the RAPWG has presented its findings.

2.2 Next Steps

- Even though the RAPWG is not a Policy Development Process (PDP) Working Group, in the interest of transparency and participation it decided to follow the practice of PDP Working Groups by producing an Initial Report for community comment and consideration before finalizing the report and its recommendations for submission to the GNSO Council. The RAPWG will review the comments received and issue a Final Report following the closing of the public comment period.

2.3 Abuse Definition & Registration vs. Use

- The RAPWG developed a consensus definition of abuse, which served as a basis to further explore the scope and definition of registration abuse. This definition reads:

  Abuse is an action that:

  a. Causes actual and substantial harm, or is a material predicate of such harm, and

  b. Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.

- In discussing registration abuse vs. domain name use abuse, the RAPWG noted that registration abuses may occur at various points in a domain name's lifecycle. The RAPWG therefore found that making distinctions between pre-domain-creation, domain-creation, and post-creation abuses is sometimes not applicable or useful when considering whether an abuse is in-scope for policy-making.
- In contrast, domain name *use issues* concern what a registrant *does* with his or her domain name after the domain is created—the purpose the registrant puts the domain to, and/or the services that the registrant operates on it. These use issues are often independent of or do not involve any registration issues.
- Members of the RAPWG devoted significant discussion to the differences between registration issues and use issues and how they may intersect. The RAPWG also found that the distinctions can provide logical boundaries for policy-making as the Registrar Accreditation Agreement (RAA) and Registry Agreements may enable the Generic Names Supporting Organisation (GNS)) to develop consensus policies on the topic of registration abuse. In addition, the RAPWG agreed that understanding and differentiating between domain *registration* abuses and domain *use* abuses is essential in the ICANN policy context as failure to do so can lead to confusion.
- To facilitate its deliberations, the RAPWG developed a list of abuses and approached each proposed abuse on its list by determining what registration issue exists (if any), and considering if or how it has any inherent relation to a domain name or registration process.

2.4 Potential Registration Abuses Explored

- As instructed by the RAPWG Charter, which asked to create "an illustrative categorization of known abuses" and perform research "in order to understand what problems may exist in relation to registration abuse and their scope, and to fully appreciate the current practices of contracted parties", the RAPWG developed a list of abuses for further examination. In each case, the RAPWG considered the activity by applying the RAPWG's definition of abuse, and by discussing what scope and policy issues existed, especially whether registration issues were fundamentally involved. In some cases the RAPWG confirmed that abuse exists, and in some cases found that abuse does not exist or is out of scope for policy-making.

- Chapter 5 of this report discusses in further detail each abuse, including issue, definition, background and recommendations. The following abuses are covered in this chapter:
    - Cybersquatting
    - Front-running
    - Gripe sites; deceptive, and/or offensive domain names
    - Fake renewal notices
    - Name spinning
    - Pay-per-click
    - Traffic diversion
    - False affiliation
    - Domain kiting / tasting,

2.5 Malicious Use of Domain Names

- In addition to the specific abuses described in chapter 5, the RAPWG discussed some broader categories and issues such as malicious use of domain names (chapter 6).
- The WG discussed how these problems relate to the scope of the Working Group's activities as well as GNSO policy-making. In general, the RAPWG found that malicious uses of domain names have limited but notable intersections with registration issues.
- The RAPWG acknowledges that e-crime is an important issue of the ICANN community. The Internet community frequently voices concern to ICANN about malicious conduct and, in particular, the extent to which criminals take advantage of domain registration and name resolution services. Various parties—including companies, consumers, governments, and law enforcement—are asking ICANN and its contracted parties to monitor malicious conduct and, when appropriate, take reasonable steps to detect, block, and mitigate such conduct. The question is what ICANN can reasonably do within its mission and policy-making boundaries.
- Chapter 6 discusses in further detail issues such as intent, risk and indemnification; the Expedited Registry Security Request (ERSR), as well as some examples of malicious use such as spam, phishing, malware and use of stolen credentials.

2.6 Whois Access

- The RAPWG found that the basic accessibility of WHOIS has an inherent relationship to domain registration process abuses, and is a key issue related to the malicious use of domain names. It appears that WHOIS data is not always accessible on a guaranteed or enforceable basis, is not always provided by registrars in a reliable, consistent, or predictable fashion, and that users sometimes receive different WHOIS results depending on where or how they perform the lookup. These issues interfere with registration processes, registrant decision-making, and with the ability of parties across the Internet to solve a variety of problems. Further details can be found in chapter 7.

2.7 Uniformity of Contracts

- Three specific charter objectives of the RAPWG were to:
  - Understand if registration abuses are occurring that might be curtailed or better addressed if consistent registration abuse policies were established,
  - Determine if and how {registration} abuse is dealt with in those registries {and registrars} that do not have any specific {policies} in place, and
  - Identify how these registration abuse provisions are {...} implemented in practice or deemed effective in addressing registration abuse.
- The RAPWG formed a sub-team to fully appreciate the current state environment of ICANN-related contracts and agreements, and then discussed the findings in the larger RAPWG. Its findings are described in further detail in chapter 8.

2.8 Meta-Issues

- The RAPWG identified two registration abuse “meta-issues.” These meta-issues have a number of attributes in common:
  - They are being discussed in various Working Groups and Advisory Groups simultaneously.
  - Their scope spans a number of ICANN policies
  - Previous groups have discussed these issues without satisfactory resolution

- They are worthy of substantive discussion and action, but may not lend themselves to resolution through current policy processes

- The two meta issues discussed in chapter 9 are:
  - Uniformity of reporting – The RAPWG has identified the need for more uniformity in the mechanisms to initiate, track, and analyze policy-violation reports.
  - Collection and dissemination of best practices - The RAPWG has identified the need for and benefit of creating and disseminating "best practices" related to aspects of domain name registration and management, for the appropriate members of the ICANN community. Best practices should also be kept current and relevant. The question is how ICANN can support such efforts in a structured way.

2.9 Recommendations

- On the basis of its deliberations as outlined in this report, the RAPWG is putting forward the following recommendations for community discussion and feedback.

CYBERSQUATTING		
Recommendation #1	The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Report to investigate the current state of the UDRP, and consider revisions to address cybersquatting if appropriate. This effort should consider: • How the UDRP has addressed the problem of cybersquatting to date, and any insufficiencies/inequalities associated with the process. • Whether the definition of cybersquatting inherent within the existing UDRP language needs to be	**Unanimous consensus**

	reviewed or updated.	
Recommendation # 2 **View A**	The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Report to investigate the appropriateness and effectiveness of how any Rights Protection Mechanisms that are developed elsewhere in the community (e.g. the New gTLD program) can be applied to the problem of cybersquatting in the current gTLD space.	**Supported by 7 members of the RAPWG**
View B	The initiation of such a process is premature; the effectiveness and consequences of the Rights Protection Mechanisms proposed for the new TLDs is unknown. Discussion of RPMs should continue via the New TLD program. Experience with them should be gained before considering their appropriate relation (if any) to the existing TLD space.	**Supported by 6 members of the RAPWG**

FRONT RUNNING		
Recommendation #1	It is unclear to what extent front-running happens, and the RAPWG does not recommend policy development at this time. The RAPWG suggests that the Council monitor the issue and consider next steps if conditions warrant.	**Unanimous consensus**

GRIPE SITES; DECEPTIVE and/or OFFENSIVE DOMAIN NAMES		
Recommendation #1	Make no recommendation	**Rough Consensus**
Alternate view	**T**he URDP should be revisited to determine what substantive policy changes, if any, would be necessary to address any inconsistencies relating to decisions on "gripe" names and to provide for fast track substantive and procedural mechanisms in the event of the registration of deceptive domain names that mislead adults or children to objectionable sites.	**Supported by 4 members of the RAPWG**
Recommendation #2	Turn down a proposed recommendation that registries develop best practices to restrict the registration of offensive strings.	**Strong support**
Alternate view	Registries should consider developing internal best practice policies that would restrict the registration of offensive strings in order to mitigate the potential harm to consumers and children.	**Supported by 5 members of the RAPWG**

FAKE RENEWAL NOTICES		
Recommendation #1	The RAPWG recommends that the GNSO refer this issue to ICANN's Contractual Compliance department for possible enforcement action, including investigation of misuse of WHOIS data.	**Strong Consensus**

Alternate view	There does not seem to be any policy that Compliance could enforce	**Supported by 1 member of the RAPWG**
Recommendation #2	**The following recommendation is conditional.** The WG would like to learn the ICANN Compliance Department's opinions regarding Recommendation #1 above, and the WG will further discuss Recommendation 2 looking forward to the WG's Final Report. The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Report to investigate fake renewal notices.	**Unanimous consensus**

DOMAIN KITING / TASTING		
Recommendation #1	It is unclear to what extent domain kiting happens, and the RAPWG does not recommend policy development at this time. The RAPWG suggests that the Council monitor the issue (in conjunction with ongoing reviews of domain-tasting), and consider next steps if conditions warrant.	**Unanimous consensus**

MALICIOUS USE OF DOMAIN NAMES		
Recommendation #1	The RAPWG recommends the creation of non-binding best practices to help registrars and registries address the illicit use of domain names. This effort should be supported by ICANN resources, and should be created via a	**Strong consensus**

	community process such as a working or advisory group while also taking the need for security and trust into consideration. The effort should consider (but not be limited to) these subjects: • Practices for identifying stolen credentials • Practices for identifying and investigating common forms of malicious use (such as malware and phishing) • Creating anti-abuse terms of service for inclusion in Registrar-Registrant agreements, and for use by TLD operators. • Identifying compromised/hacked domains versus domain registered by abusers • Practices for suspending domain names • Account access security management • Security resources of use or interest to registrars and registries • Survey registrars and registries to determine practices being used, and their adoption rates.	
Alternate View	Pure uses of domain names are an area in which ICANN can impose mandatory practices	**Supported by 1 member of the**

	upon contracted parties.	**RAPWG**

WHOIS ACCESS		
Recommendation #1	The GNSO should determine what additional research and processes may be needed to ensure that WHOIS data is accessible in an appropriately reliable, enforceable, and consistent fashion. The GNSO Council should consider how such might be related to other WHOIS efforts, such as the upcoming review of WHOIS policy and implementation required by ICANN's new Affirmation of Commitments.	**Unanimous consensus**
Recommendation #2	The GNSO should request that the ICANN Compliance Department publish more data about WHOIS accessibility, on at least an annual basis. This data should include a) the number of registrars that show a pattern of unreasonable restriction of access to their port 43 WHOIS servers, and b) the results of an annual compliance audit of compliance with all contractual WHOIS access obligations.	**Unanimous consensus**

UNIFORMITY OF CONTRACTS		
Recommendation #1 **View A**	The RAPWG recommends the creation of an Issues Report to evaluate whether a minimum baseline of registration abuse provisions should be created for all in-scope ICANN	**Strong Support**

	agreements, and if created, how such language would be structured to address the most common forms of registration abuse.	
View B	Opposed to the recommendation for an Issues Report as expressed in view A	**Significant Opposition**

META ISSUE: UNIFORMITY OF REPORTING		
Recommendation #1	The RAPWG recommends that the GNSO, and the larger ICANN community in general, create and support uniform reporting processes.	**Unanimous consensus**

META ISSUE: COLLECTION AND DISSEMINATION OF BEST PRACTICES		
Recommendation #1	The RAPWG recommends that the GNSO, and the larger ICANN community in general, create and support structured, funded mechanisms for the collection and maintenance of best practices.	**Unanimous consensus**

2.10 Conclusions, Recommendations & Next Steps

- The RAPWG aims to complete this section of the report in the second phase of the WG process, following the review and analysis of the comments received during the public comment period.

3. Background, Process, and Next Steps

3.1 Background

- On 25 September 2008, the GNSO Council adopted a motion requesting an issues report on registration abuse provisions in registry-registrar agreements. The issues report was submitted to the GNSO Council on 29 October 2008 and provides an overview of existing provisions in registry-registrar agreements relating to abuse and includes a number of recommended next steps, namely for the GNSO Council to:
  - **Review and Evaluate Findings**
    A first step would be for the GNSO Council to review and evaluate these findings, taking into account that this report provides an overview of registration abuse provisions, but does not analyse how these provisions are implemented in practice and whether they are deemed effective in addressing registration abuse.
  - **Identify specific policy issues**
    Following the review and evaluation of the findings, the GNSO Council would need to determine whether there are specific policy issues regarding registration abuse. As part of this determination it would be helpful to define the specific type(s) of abuse of concern, especially distinguishing between registration abuse and other types of abuse if relevant.
  - **Need for further research**
    As part of the previous two steps, ICANN Staff would recommend that the GNSO Council determines where further research may be needed – e.g. is lack of uniformity a substantial problem, how effective are current registration abuse provisions in addressing abuse in practice, is an initial review or analysis of the UDRP required?'
- The GNSO Council voted on 18 December to form a drafting team to create a proposed charter for a working group charged with investigating the open issues identified in

Registration Abuse Policies report. The drafting team was formed and met for the first time on 9 January 2009. They finalized a charter (see Annex I), which was adopted by the GNSO Council on 19 February 2009, for a Registration Abuse Policies Working Group (RAPWG). The GNSO Council will not make a decision on whether or not to initiate a Policy Development Process (PDP) on registration abuse policies until the RAPWG has presented its findings.

3.2 Process

- The RAPWG started with discussing and developing a working definition of abuse, which has served as a basis to further explore the scope and definition of registration abuse.
- The RAPWG has been researching and discussing what "registration abuse" is, including:
  a. How 'registration' is defined. This term was not explicitly defined, and is essential for understanding the "registration" versus "use" issues that the charter and Issues Report call attention to.
  b. Which "aspects of the subject of registration abuse are within ICANN's mission to address and which are within the set of topics on which ICANN may establish policies that are binding on gTLD registry operators and ICANN-accredited registrars." As part of the RAPWG research, a presentation was provided by ICANN staff about policy-making scope issues and past PDPs.
- The RAPWG developed a list of potential abuses. The RAPWG discussed each of these proposed abuses, sometimes facilitated by the creation of sub-teams. The RAPWG developed a definition for each, considered whether they are abusive or not, determined if and how registration issues are implicated in them and whether regulation is within or outside of policy-making scope, and developed recommendations for further consideration. Further details can be found in the following chapter of this report.
- Several sub-tams were formed throughout this process to explore more complicated abuse types and other Registration Abuse topics identified in the charter. Sub-teams

focused on: Cybersquatting, Name Spinning, Malware/Botnet, Phishing/Malware and Uniformity of Contracts. Findings and recommendations that resulted from these efforts can be found in the chapters below.

3.3 Next Steps

- Even though the RAPWG is not a Policy Development Process (PDP) Working Group, in the interest of transparency and participation it decided to follow the practice of PDP Working Groups by producing an Initial Report for community comment and consideration before finalizing the report and its recommendations for submission to the GNSO Council. The RAPWG will review the comments received and issue a Final Report following the closing of the public comment period.

4. Discussion of Charter and Scope Questions

4.1 Abuse definition

The RAPWG developed a consensus definition of abuse, which served as a basis to further explore the scope and definition of registration abuse. This definition reads:

Abuse is an action that:

- *Causes actual and substantial harm, or is a material predicate of such harm, and*
- *Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.*

Note:

* The party or parties harmed, and the substance or severity of the abuse, should be identified and discussed in relation to a specific proposed abuse.
* The term "harm" is not intended to shield a party from fair market competition.
* A predicate is a related action or enabler. There must be a clear link between the predicate and the abuse, and justification enough to address the abuse by addressing the predicate (enabling action).
* The above definition of abuse is indebted to the definition of "misuse" in the document "Working Definitions for Key Terms that May be Used in Future WHOIS Studies" prepared by the GNSO Drafting Team[1] .
* *The WG achieved **unanimous consensus** on the above definition and notes, which should be taken together. In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RysG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual),*

[1] 18 February 2009, at [1] 18 February 2009, at http://gnso.icann.org/issues/whois/whois-working-definitions-study-terms-18feb09.pdf

Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.

4.2 Definitions of "registration" and "Use"

Registration issues are related to the core domain name-related activities performed by registrars and registries. These generally include but are not limited to:

- the allocation of registered names, and reserved names
- maintenance of and access to accurate and up-to-date information concerning domain name registrations – i.e. WHOIS information.
- the transfer, deletion, and reallocation of domain names.
- functional and performance specifications for the provision of Registry Services.
- The resolution of disputes regarding whether particular parties may register or maintain registration of particular domain names.

These are generally within the scope of GNSO policy-making. Many of the above are specifically listed in registration agreements as being subject to Consensus Policies, and the extant Consensus Policies have to do with these kinds of topics. Other potential outcomes of policy work are also possible, such as advice to ICANN on possible contract amendments, or the development of non-binding options such as codes of conduct or best practices.

Registration abuses are therefore abuses associated with the above kinds of activities or topics. ICANN has made consensus policies for several registration-related abuses. Examples[2] include:

- The AGP Limits Policy, instituted to curb abuse of the Add Grace Period—specifically the practice known as domain tasting.
- The WHOIS Data Reminder Policy, instituted to remind registrants that provision of false WHOIS information is abusive and can be grounds for cancellation of their domain name registration.

[2] http://www.icann.org/en/general/consensus-policies.htm

- The Inter-Registrar Transfer Policy, designed to guarantee that registrants can transfer names to the registrar of their choice, and to provide standardized requirements for the proper handling of transfer requests by registrars and registries.

Note that in this context, "registration" is not a synonym for the *creation* of a domain name. As per the lists above, registration abuses may occur at various points in a domain name's lifecycle. The RAPWG therefore found that making distinctions between pre-domain-creation, domain-creation, and post-creation abuses is sometimes not applicable or useful when considering whether an abuse is in-scope for policy-making.

In contrast, domain name *use issues* concern what a registrant *does* with his or her domain name after the domain is created—the purpose the registrant puts the domain to, and/or the services that the registrant operates on it. These use issues are often independent of or do not involve any registration issues.

A domain name can have nearly infinite uses. It can be used for various technical services, such as e-mail, a Web site, file transfers, and can support subdomains. And it can support all kinds of practical uses or purposes – speech and expression, e-commerce, social networking, education, entertainment, and so on. Some uses of domain names are generally agreed to be abusive or even criminal—such as phishing and malware distribution, which perpetrate theft and fraud. Other uses – such as adult pornography or political criticism – may be considered abusive or illegal in some jurisdictions but not generally. Domain names in sponsored TLDs may by design be restricted to certain uses or users.

Are uses of domain names subject to GNSO policy-making? In the Issues Report that led to the RAPWG, ICANN's General Counsel wrote: "Is the issue in scope of GNSO Policy Making? Section 4.2.3 of the RAA between ICANN and accredited registrars *provides for the establishment of new and revised consensus policies concerning the registration of domain names, including abuse in the registration of names, but policies involving the use of a domain name (unrelated to its registration) are outside the scope of policies that ICANN could enforce on registries and/or*

registrars. The use of domain names may be taken into account when establishing or changing registration policies. Thus, potential changes to existing contractual provisions related to abuse in the registration of names would be within scope of GNSO policy making. Consideration of new policies related to the use of a domain name unrelated to its registration would not be within scope." [3],[4] [Emphasis added].

Other sections of the RAA and Registry Agreements may enable the GNSO to develop consensus policies on the topic of registration abuse. For example, Section 4.2.1 of the RAA (as well as analogous sections of various registry agreements) authorizes development of consensus policies on topics where the uniform or coordinated resolution is reasonably necessary to facilitate the interoperability, technical reliability, or operational stability of registrars, registries, the DNS, or the Internet.[5] The Registry Agreements generally limit Consensus Policy-making to core registration issues.[6]

Careful consideration of these issues and limiting of scope seems to be consistent with ICANN's mission. In its 2002 "Working Paper on ICANN Mission and Core Values," the Committee on ICANN Evolution and Reform commented on the registration-versus-use issue. It said "Though

---

[3] "GNSO Issues Report on Registration Abuse Policies," 29 October 2008, pages 4-5. http://gnso.icann.org/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf

[4] See also http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm , paragraph 4.2. The new Registrar Accreditation Agreement (RAA) notes that a Consensus Policy may be established regarding the "resolution of disputes concerning the registration of Registered Names (as opposed to the use of such domain names), including where the policies take into account use of the domain names."

[5] Please also refer to the transcript of the 1 June 2009 RAP meeting, describing the presentation by Margie Milam on the scope of Consensus policies related to the topic of registration abuse, posted at http://gnso.icann.org/calendar/index.html#june

[6] Principles for allocation of registered names, prohibitions on warehousing of or speculation in domain names, reserved names, maintenance of and access to accurate and up-to-date WHOIS information; procedures to avoid disruptions of domain name registration due to suspension or termination of operations by a registry operator or a registrar, and domain name disputes.

some of ICANN's registry-level gTLD policies are non-technical in nature, all relate directly to ICANN's mission to coordinate the assignment of unique identifiers to ensure stable functioning of these systems. For example, the need for dispute resolution mechanisms in the gTLDs flows from the problem of unique assignment: it is the assigned domain name string itself that is at issue…. [RAPWG note: i.e. a registration issue is involved.] By contrast, disputes over the content of an e-mail message, ftp file, or web page bear no inherent relation to the assigned domain name, and therefore fall outside the scope of ICANN's policy-making scope. ICANN therefore does not base its policies on the content served by websites, contained in e-mail messages, or otherwise accessed by domain names."[7] ICANN's Core Values[8] also state that ICANN should respect the innovation and flow of information made possible by the Internet by limiting ICANN's activities to those matters within ICANN's mission, and "To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties"—perhaps such as courts, law enforcement, and contracted parties.

Members of the RAPWG devoted significant discussion to the differences between registration issues and use issues and how they may intersect. The RAPWG also found that the distinctions can provide logical boundaries for policy-making. For example, some members noted that ICANN is not in a position to create policies affecting speech or what kinds of e-commerce should be allowed via domain names, because those typically are uses of domain names and do not implicate registration issues. Others pointed out the difficulties of addressing criminal domain name use via ICANN policy and contractual compliance. (This issue is explored in additional depth in this Report's section about malicious uses of domain names.)

Understanding and differentiating between domain *registration* abuses and domain *use* abuses is essential in the ICANN policy context. Failure to do so can lead to confusion:

---

[7] http://www.icann.org/en/committees/evol-reform/working-paper-mission-06may02.htm

[8] http://www.icann.org/en/general/bylaws.htm#I

- In 2008, the GNSO initiated a PDP to examine fast-flux hosting; the concern was that fast-flux was a criminal abuse that leveraged the DNS. The Fast-Flux Working Group (FFWG) learned that fast-flux is actually a technical practice with both benign and malicious applications, and that most criminal fast-flux hosting did not involve any changes of registration records.[9] The FFWG determined that fast-flux was not always an abuse, and it found that illicit fast-flux was a domain use issue and did not generally involve registration issues. Some constituencies and observers noted that fast-flux was therefore outside of policy-making scope.[10] In the end, the FFWG did not recommend any new policies or any changes to existing policies.
- The "GNSO Issues Report on Registration Abuse Policies" was an initial look into the topic of registration abuse, and did not consistently and thoroughly delineate or define the registration versus use issues. It sometimes used the word "abuse" to refer to both registration and use problems interchangeably. At one point the Issues Report noted that "various registry operators have differing policies with respect to abusive registrations" while pointing to registry policies that have nothing to do with registration abuses.[11]

The RAPWG therefore approached each proposed abuse on its list by determining what registration issue exists (if any), and considering if or how it has any inherent relation to a domain name or registration process. Other questions that should be considered in evaluating potential abuses and related policies are if and how any policy decision might impact the use of domain names, and establishing whether and to what extent the use of domain names affects the stability and security of the DNS itself, and if so how.

---

[9] The DNS rotation took place at a level below the registries and registrars, and domain and nameserver records were usually not being updated on a rapid basis or at all.

[10] https://st.icann.org/data/workspaces/pdp-wg-ff/attachments/fast_flux_pdp_wg:20090807173836-0-13665/original/Fast%20Flux%20Final%20Report%20-%206%20August%202009%20-%20FINAL.pdf

[11] See "GNSO Issues Report on Registration Abuse Policies" Section 1.5 and Annex B. The .INFO Anti-Abuse Policy is strictly aimed at malicious *uses* of domains names, such as malware and child pornography.

5. Potential Registration Abuses Explored

Early in the RAPWG's existence, members were asked to propose potential abuses for examination. This was to fulfil the RAPWG Charter, which asked the RAPWG to create "an illustrative categorization of known abuses" and perform research "in order to understand what problems may exist in relation to registration abuse and their scope, and to fully appreciate the current practices of contracted parties." In each case, the RAPWG considered the activity by applying the RAPWG's definition of abuse, and by discussing what scope and policy issues existed, especially whether registration issues were fundamentally involved. In some cases the RAPWG confirmed that abuse exists, and in some cases found that abuse does not exist or is out of scope for policy-making.

5.1 Cybersquatting

5.1.1 Issue / Definition

Cybersquatting is the deliberate and bad-faith registration or use of a name that is a registered brand or mark of an unrelated entity, for the purpose of profiting (typically, though not exclusively, through pay-per-click advertisements). Cybersquatting is recognized as registration abuse in the ICANN community, and the UDRP was originally created to address this abuse. There was consensus in the RAPWG that provisions 4(a) and 4(b) of the UDRP are a sound definition of Cybersquatting.[12]

5.1.2 Background

As part of the RAPWG's work to catalog various types of abuse, Cybersquatting was targeted as an area for further work. Developing a universal, global, and technically operable definition for Cybersquatting has been challenging, particularly as the RAPWG sought to balance the needs

[12] http://www.icann.org/en/udrp/udrp-policy-24oct99.htm

and interests of all parties that can potentially be harmed by the practice. The RAPWG draws a distinction between competing but potentially legitimate claims and Cybersquatting, which denotes a bad-faith use of another party's mark. There was consensus in the RAPWG that provisions 4(a) and 4(b) of the UDRP are a sound definition of Cybersquatting. Several attempts to expand the definition beyond these by borrowing from other sources (e.g. the Anti-Cybersquatting Consumer Protection Act (ACPA)) have been challenging, and consensus on how to proceed ultimately broke down. There was minority interest in expanding the definition to include additional elements of bad faith intent, as denoted in the ACPA (i.e., 5(v) and 5(vi)). For further details, please see https://st.icann.org/reg-abuse-wg/index.cgi?cybersquatting.

The UDRP was specifically designed to address Cybersquatting. It is used to settle disputes between parties who have competing trademark claims as well as other cases in which the respondent may have no trademark claim at all or is acting in bad faith. Only disputes in which "the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights" are applicable for UDRP arbitration.[13] The ICANN Web site's UDRP page also notes: "Disputes alleged to arise from abusive registrations of domain names (for example, cybersquatting) may be addressed by expedited administrative proceedings that the holder of trademark rights initiates by filing a [UDRP] complaint with an approved dispute-resolution service provider." [14]

Notwithstanding its shortcomings, the UDRP has generally been considered a success. It has been used to settle thousands of cases, and WIPO has claimed that the UDRP has been a deterrent to undesirable registration behavior.[15] Since it went into effect in 1999, there have also been complaints about the UDRP. Some of these present policy and process issues. These criticisms have included: the following:

---

[13] Uniform Domain Name Dispute Resolution Policy, http://www.icann.org/en/udrp/udrp-policy-24oct99.htm

[14] http://www.icann.org/en/udrp/udrp.htm

[15] http://www.wipo.int/pressroom/en/html.jsp?file=/redocs/prdocs/en/2005/wipo_upd_2005_239.html

- Complainants can forum-shop in attempts to find arbitrators more likely to rule in the complainant's favor.
- Complainants have the ability to re-file a complaint for the same name against the same respondent – in effect re-trying the same case in hopes of achieving a different outcome.
- The UDRP requires the complainant prove that the domain name "has been registered and is being used in bad faith." However, many UDRP cases have been decided without the domain names having ever been used. Observers have noted that the usage requirement has sometimes been ignored in the UDRP "case law" that has developed over the years.
- The UDRP is too expensive and too time-consuming for some brand owners, who wish to pursue large numbers of potentially infringing domain names.
- The UDRP procedures lack some safeguards that are generally available in conventional legal proceedings, such as appeals.
- In a possibly related issue, ICANN apparently does not enter into contracts with its Approved UDRP Providers.[16] This may present a number of issues. For example, in the absence of such contracts, it is unclear whether ICANN has the ability to review or assure general uniformity or procedural compliance.
- One UDRP service provider, the Czech Arbitration Court, recently proposed changing some of its own supplemental rules in order to create an "expedited UDRP." Some community members asked whether the proposed scheme presented substantive issues that can and should only be dealt with in the main ICANN UDRP Rules.[17]

Some members of the RAPWG felt that the UDRP is a useful mechanism to counter some elements of cybersquatting, but were of the opinion that: "the scale of cybersquatting is overwhelming and the drain on cost and resources for brand-owners to respond in all instances by using only the UDRP as a remedy is prohibitive. In addition, there is insufficient up-front

[16] http://forum.icann.org/lists/cac-prop-supp-rules/msg00004.html

[17] http://forum.icann.org/lists/cac-prop-supp-rules/index.html

protection mechanisms to prevent registrants from initially registering infringing domains which are freely monetized from the date of registration, via PPC and other online advertising methods, thus earning revenue for the registrant. They can then simply wait until a UDRP action is commenced before they give up the domain, without penalty. The burden therefore rests with the trademark owner to monitor, investigate and pursue litigation in order to provide protection to Internet users. This burden often includes the registration and ongoing management of large domain name portfolios, consisting mainly of unwanted domains that benefit only the Registry, Registrar and ICANN parties. This approach is already a major concern for trademark owners, in terms of cost and resources, with the existing level of gTLDs and ccTLDs, let alone the anticipated growth of new gTLDs and IDNs."

Other members disagreed with those points, expressing the following opinions:

a) The URDP is the long-standing mechanism for addressing cybersquatting. A better first step would be to establish if or where the UDRP is ineffective, and make policy decisions based on facts and data. While some claim that “the scale of cybersquatting is overwhelming," the scale issue was not been quantified in or for the RAPWG, and an adequate factual basis was not provided by the IRT.

b) Those proposed rights-protection mechanisms upend several long-established legal principles. One is that the registrant is the party responsible for ensuring he or she is not infringing upon the rights of others. Another is that rights holders have the responsibility for protecting their intellectual property, and that shifting responsibility, cost, or liability for such to ICANN-contracted parties is unfair.

c) It is inadvisable to begin considering the imposition of those evolving rights protection mechanisms in the existing TLDs, when they are so controversial over in the new TLD discussion. There are many legal, business, and speech issues involved. The effectiveness of those proposed mechanisms is hypothetical, it is not known what impacts or unintended consequences they may have, and it is unknown if they can deliver the cost and process benefits their advocates promised or asked for. It is unknown what consequences those mechanisms

may have for speech and expression. Some parties have called for imposition of the trademark clearinghouse RPM during ongoing registry operations, which might effectively stop real-time, first-come registrations. This would be a major change to the industry.

5.1.3 Cybersquatting Recommendation

Recommendation #1:

The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Report to investigate the current state of the UDRP, and consider revisions to address cybersquatting if appropriate. This effort should consider:

- ***How the UDRP has addressed the problem of cybersquatting to date, and any insufficiencies/inequalities associated with the process.***
- ***Whether the definition of cybersquatting inherent within the existing UDRP language needs to be reviewed or updated.***

The Working Group had unanimous consensus for this recommendation. *In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.*

Recommendation #2:

The RAPWG was almost evenly split regarding a second recommendation. *The two opposing views are below, and the RAPWG will further consider these views after receiving public comment:*

Seven members supported **View A:** The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Report to investigate the appropriateness and effectiveness of how any Rights Protection Mechanisms that are developed elsewhere in the community (e.g. the New gTLD program) can be applied to the problem of cybersquatting in the current gTLD space.

In favour of View A (7): Cobb (CBUC), Felman (IPC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC).

Six members supported **View B:** The initiation of such a process is premature; the effectiveness and consequences of the Rights Protection Mechanisms proposed for the new TLDs is unknown. Discussion of RPMs should continue via the New TLD program. Experience with them should be gained before considering their appropriate relation (if any) to the existing TLD space.
In favour of View B (6): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Newman (RySG), O'Connor (CBUC), Young (RySG).

5.2 Front-Running

5.2.1 Issue / Definition

Front-running is when a party obtains some form of insider information regarding an Internet user's preference for registering a domain name and uses this opportunity to pre-emptively register that domain name. In this scenario, "insider information" is information gathered from the monitoring of one or more attempts by an Internet user to check the availability of a domain name.

5.2.2 Background

The definition above is taken from the SSAC paper "SAC 024: Report on Domain Name Front Running."[18] Specifically, the RAPWG examined these documents:

1. SAC 022, http://www.icann.org/en/committees/security/sac022.pdf
2. SAC 024, https://par.icann.org/files/paris/SSACReportonDomainNameFrontRunning_24Jun08.pdf
3. Benjamin Edelman, http://www.icann.org/en/compliance/edelman-frontrunning-study-16jun09-en.pdf

[18] http://www.icann.org/en/committees/security/sac024.pdf

The two reports by the SSAC contain a great deal of material. The RAPWG felt that a few key quotes for these documents are:

- "Checking the availability of a domain name can be a sensitive act which may disclose an interest in or a value ascribed to a domain name. SSAC suggests that any such domain name availability lookups should be performed with care. Our premise is that a registrant may ascribe a value to a domain name; that unintended or unauthorized disclosure, or disclosure of an availability check by a third party without notice may pose a security risk to the would-be registrant; and that availability checks may create opportunities for a party with access to availability check data to acquire a domain name at the expense of the party that performed an availability check, or to the benefit of the party that monitored the check." (SAC 022, page 2)
- "SSAC strongly contends that any agent who collects information about an Internet user's interest in a domain name and who discloses it in a public way violates a trust relationship. This violation is exacerbated when agents put themselves or third parties in an advantageous market position with respect to acquiring that domain name at the expense of its client." (SAC 024, page 12)
- "SSAC observes a deteriorating trust relationship between registrants and registrars and urge ICANN and the community to consider the implications of continued erosion and a loss of faith in the registration process." (SAC 024, page 12)

The RAPWG discussed issues such as theoretical vs. actual abuse; is domain speculation an abuse; expectations of trust; what is considered insider information; the interaction with the add-grace period and domain tasting; possible legitimate uses of pre-registration data; and, who is harmed by front-running. Commentary regarding these topics is summarized on the RAPWG wiki.[19] Highlights of the discussions included:

[19] https://st.icann.org/reg-abuse-wg/index.cgi?domain_front_running

- One well-known case of front-running is described in SAC 024. Otherwise, the RAPWG was unable to reference any other confirmed cases.[20] The WG members therefore wondered whether the practice exists or is widespread enough to merit further investigation or concern.
- The RAPWG members generally considered front-running an abuse, referencing the SSAC's concerns about registrant expectations and breach of trust. A member also offered that in a first-come-first-served environment, efforts to gain advantage or even game those processes should be considered abuse.
- A member noted that the harm is to people who are new to domains and not educated about how ordering takes place.
- The issue may involve registrars or registries only indirectly. A threat may come from third parties using monitoring to examine traffic and then front-run domains, perhaps even using spyware or malware. In such cases, it is unknown whether a registrar or registry would even be able to detect or do something about front-running. Some registrars have reportedly implemented SSL-protected search pages to help guard against intercepted availability check traffic.
- Members raised some issues regarding the definition of "insider information." For example, what information can registries or registrars collect about their customers, and that some uses may not be inappropriate or harmful. One member stated that traffic data regarding unregistered names (e.g. NX data) is by definition not registration data, while another was of the opinion that such is data that can be used to decide to register domains and is therefore registration data or at worst "lack-of-registration data, which is merely the negative of registration data."
- The new Add Grace Period Limits Policy effectively killed domain tasting, and may have an impact on front running. To be a profitable practice, front-running might require the registration of a fair number of domain names, which might now be prohibitive under the AGP Limits Policy.

---

[20] The Edelman study uncovered no additional evidence of the practice. The Edelman study's methodology has been called into question, and some members considered it inconclusive.

5.2.3 Recommendations

It is unclear to what extent front-running happens, and the RAPWG does not recommend policy development at this time. The RAPWG suggests that the Council monitor the issue and consider next steps if conditions warrant.

The WG achieved unanimous consensus for the above recommendation.

In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.

5.3 Gripe Sites; Deceptive, and/or Offensive Domain Names

5.3.1 Issue / Definition

The issue is whether the registration these kinds of domain names are simply a form of cybersquatting or whether the registration of such domain names should be addressed as a separate form of registration abuse, and whether a consistent policy framework addressing this category can or should be applied across all ICANN-accredited registries and registrars.

- Gripe/Complaint Sites a.k.a. "Sucks Sites": Web sites that complain about a company's or entity's products or services and uses a company's trademark in the domain name (e.g. companysucks.com).
- Pornographic/Offensive Sites: Web sites that contain adult or pornographic content and uses a brand holder's trademark in the domain name (e.g. brandporn.com).
- Offensive strings: Registration of stand-alone dirty words within a domain name (with or without brand names).
- Registration of deceptive domain names: Registration of domain names that direct unsuspecting consumers to obscenity or direct minors to harmful content—sometimes referred to as a form of "mousetrapping."

5.3.2 Background

The RAPWG discussed the issue of whether the registration of these types of domain names should be addressed as a unique category of registration, with discussions that centered on several different areas:

i. Gripe/Complaint Websites:

Several members pointed to the freedom of speech laws (not only in the U.S. but internationally) that govern gripe and complaint sites using a company's trademark in the domain name, and indicated that registration of these names should not be considered as a separate abuse category but rather should be considered as potential cases of cybersquatting, if anything. Other members also discussed the intrinsic value of gripe and complaint Web sites to companies and organizations that are seeking to understand the problems that customers may have with respect to their products or services. The WG noted that aggrieved parties could turn to the courts and the UDRP to remedy any claims they may have with respect to the use of trademarks in a domain name. There was some discussion that decisions have not been consistent with respect to gripe and complaint sites, although it is generally understood that that truthful statements in gripe and complaint sites are protected free speech. Examples include:

- http://decisions.courts.state.ny.us/fcas/fcas_docs/2005oct/30060065920045sciv.pdf. A U.S. court ruled that a disgruntled customer of an insurance firm cannot be sued for defamation over statements he made on his "gripe site" because those statements are protected free speech.
- http://www.acluva.org/docket/pleadings/lamparello_opinion.pdf - A U.S. Appeals Court found that a Web site using the domain name fallwell.com, set up to criticize evangelist Jerry Falwell, did not violate trademark laws. There was no likelihood of confusion, ruled the Court.
- http://www.wipo.int/amc/en/domains/decisions/html/2007/d2007-0731.html - Afigure behind controversial business schemes failed in his bid to gain control of the .COM Internet address consisting of his name. A site that criticizes his activities was allowed to keep the name.

- http://www.wipo.int/amc/en/domains/decisions/html/2005/d2005-0168.html - The domain name AirFranceSucks.com was transferred to Air France. But the airline's victory at arbitration was not without controversy: panelists disagreed about what the word 'sucks' really means to Internet users.
- http://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-1077.html- The Panel noted that that the domain name Radioshacksucks.com was not redirected to a "gripe" Web site, but was pointing to a Web site with various pay-per-click links mainly aimed at directing visitors to competing third party commercial Web sites. The Panel found for the Complainant and transferred the name.
- At least one article has criticized some of the current UDRP decisions in this area. That article can be found at: http://domainnamewire.com/2009/12/04/freedom-of-speech-a-concept-not-limited-to-yankees/

ii. Pornographic Websites/Registration of Offensive Strings:

There appears to be some distinction however between complaint and gripe sites and the registration of offensive strings, and whether these should be treated differently. The registration of complaint site names (a.k.a. "sucks sites") appears to have a direct impact on organizations and companies, while the registration of offensive words have a more direct impact on consumers. A domain name that contains a brand and an offensive word and also points to a Web site that contains pornographic content can tarnish the reputation and the image of a company's brand. In addition to court action, the UDRP is a tool that companies and organizations can turn to turn to remediate this problem because of the presence of the brand name. A recent article in Computerworld magazine[21] discusses the increase in cybersquatting abuse in general. The article points to the example of the Web site FreeLegoPorn.com that began publishing pornographic images created with Lego toys. The trademark owner Lego Juris

21 http://www.computerworld.com/s/article/print/9134605/Domain_name_wars_Rise_of_the_cybersquatters?taxonomyName=Networking+and+Internet&taxonomyId=16

AS filed a UDRP complaint with the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center, which ultimately ruled in its favor.

However, a domain name that is registered for the sole purpose of misleading a consumer can be extremely harmful. For example, the U.S. government enacted the Truth in Domain Names Act (18 USC Sec. 2252B), which makes it a crime to knowingly register a domain name with the intent to mislead a person into viewing obscene material. It also makes it a crime to register a domain name with the intent to deceive a minor into viewing harmful material. These domain names generally encompass typos (but not always) of recognizable names and trademarks as a means of confusing people into visiting objectionable Web sites. Moreover, a number of ccTLDs maintain policies governing the registration of objectionable words, with at least one ccTLD registry (.US) apparently preventing the registration of the "seven dirty words" as per a government policy. (The United States Federal Trade Commission also regulates the use of these seven words on broadcast television and radio stations in the U.S.)

The RAPWG discussed some of the practical business challenges that could be presented for a registry to adopt a policy that blacklists all names that also contain some form of prohibited word. For example, the RAPWG noted the difficulty in (i) trying to monitor the use of expletives in different languages, (ii) continuing to adapt to the evolution of obscenities in the vernacular of a specific language, and (iii) addressing "gaming" of the system in this area.

RAPWG members also pointed out that ccTLDs and gTLDs are not in equivalent positions in these matters. ccTLD operators are associated with certain countries, and are usually obligated to adhere to their governments' directives and laws, which reflect varying local standards of decency. In contrast, gTLDs are by definition global, and it would be difficult to determine baselines and balances for issues involving free speech and morals. Members commented that ICANN is not in a good position to enforce morals in relation to domain names. The issue was effectively settled in .COM/.NET/.ORG in 1999.

The RAPWG members generally agreed that gripe site and offensive domain names that use a brand owner's trademark are adequately addressed in the context of Cybersquatting for purposes of establishing consistent registration abuse policies in this area.

5.3.3 Recommendations

There was rough consensus to make no recommendation.
The majority of RAPWG members expressed that gripe site and offensive domain names that use trademarks are adequately addressed in the context of cybersquatting and the UDRP for purposes of establishing consistent registration abuse policies in this area, and that creating special procedures for special classes of domains, such as offendsive domain names, may present problems.
In favour (9): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Sutton (CBUC), Young (RySG).

Four (4) members supported this alternate view:
T*he URDP should be revisited to determine what substantive policy changes, if any, would be necessary to address any inconsistencies relating to decisions on "gripe" names and to provide for fast track substantive and procedural mechanisms in the event of the registration of deceptive domain names that mislead adults or children to objectionable sites.*
Supporting this alternate view (4): Cobb (CBUC), Felman (IPC), Rodenbaugh (CBUC), Shah (IPC). Rodenbaugh expressed a concurring view that "new TLD policy implementations, such as URS, may be applied to existing TLDs..and thus address the concern about offensive domain names."

There was strong support to turn down a proposed recommendation that registries develop best practices to restrict the registration of offensive strings. *A majority of the WG supported this view for the following reasons:*

- *ICANN is not a good forum to make recommendations regarding moral standards.*
- *"Potential harm to consumers" is a vague standard.*

- *The recommendation is problematic for global TLDs, and it was a matter closed in .COM/.NET/.ORG many years ago.*

In support (8): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Sutton (CBUC), Young (RySG).

Five (5) members supported an alternate view, that "Registries should consider developing internal best practice policies that would restrict the registration of offensive strings in order to mitigate the potential harm to consumers and children."
Supporting this alternate view (5): Cobb (CBUC), Felman (IPC), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC). Rodenbaugh expressed a concurring view that "best practices are not enough….other recommendations – for mandatory policy – are likely to better address the concern of offensive strings."

5.4 Fake Renewal Notices

5.4.1 Issue / Definition

Fake renewal notices are misleading correspondence sent to registrants from an individual or organization claiming to be or to represent the current registrar. These are sent for a variety of deceptive purposes. The desired action as a result of the deceptive notification is:

- Pay an unnecessary fee (fraud)
- Get a registrant to switch registrars unnecessarily ("slamming", or illegitimate market-based switching)
- Reveal credentials or provide authorization codes to facilitate theft of the domain

5.4.2 Background

What is the ICANN issue?

- Transfer issue (deceptive/fraudulent practices on the part of a registrar/reseller)
    - Pretending to be current registrar
    - Creating a fraudulent transfer event

- Domain hijacking issue (in the case of a non-registrar reseller)
- WHOIS abuse issue -- obtaining contact information through questionable means or in violation of RAA section 3.3.6.4.

What is ICANN's role?

- If the perpetrator is a registrar or reseller, ICANN policy applies through the RAA.
- If the perpetrator is not a registrar/reseller, ICANN's role is still applies, but it falls into the realm of IRTP, hijacking, or WHOIS abuse.

For a number of case studies, please see document at:
http://forum.icann.org/lists/gnso-rap-dt/msg00446.html

5.4.3 Recommendations

Recommendation #1:

The RAPWG recommends that the GNSO refer this issue to ICANN's Contractual Compliance department for possible enforcement action, including investigation of misuse of WHOIS data.

The WG achieved strong consensus on the above recommendation: In favour (12): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Shah (IPC), Sutton (CBUC), Young (RySG).

One member (Rodenbaugh) disagreed with the recommendation, stating that "there does not seem to be any policy that Compliance could enforce."

Recommendation #2:

The following recommendation is conditional. *The WG would like to learn the ICANN Compliance Department's opinions regarding Recommendation #1 above, and the WG will further discuss Recommendation 2 looking forward to the WG's Final Report.*

The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Report to investigate fake renewal notices.

The WG achieved unanimous consensus on the above recommendation. In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.

5.5 Name Spinning

5.5.1 Issue / Definition

This is the practice of using automated tools used to create permutations of a given domain name string. Registrars often use such tools to suggest alternate strings to potential registrants when the string that the person queriesthey is not available for registration. .

5.5.2 Background

- The main concern is that such tools may produce results that may infringe upon trademarked strings.
- There was agreement in the RAPWG that name spinning is a tool that can be used by people for both legitimate and illegitimate purposes. As such, name-spinning is not in and of itself abusive.
- As discussed in some other areas, a determination of whether or not a particular use of such software is dependent on the user's intent.
- Until a domain name is actually registered, the trademark infringement (and therefore any registration abuse) is purely hypothetical, and therefore not a subject for policy-making.
- As discussed in some other areas, a determination of whether or not a particular use of such software is dependent on the user's intent.
- Domain name registrations that infringe on trademarks may be addressed via the UDRP.

5.5.3 Recommendations

None.

5.6 Pay-per-Click

5.6.1 Issue / Definition

Pay per click (PPC) is an Internet advertising model used on Web sites, in which the advertiser pays the host only when their ad is clicked. The concern raised was use of a trademark in a domain name to draw traffic to a site containing paid placement advertising.

5.6.2 Background

The RAPWG had consensus that pay-per-click advertising is not in and of itself a registration abuse, and that bad-faith use of trademarks in domain names is a Cybersquatting issue that can be addressed under the UDRP. The abuse of a PPC system for illicit gain is most appropriately addressed by the operator of the PPC advertising network (e.g. Google Adsense).

5.6.3 Recommendations

None.

5.7 Traffic Diversion

5.7.1 Issue / Definition

Use of brand names in HTML visible text, hidden text, meta tags, or Web page title to manipulate search engine rankings and divert traffic.

5.7.2 Background

The RAPWG had consensus that this is a pure Web site use issue with no inherent relation to a domain name or registration process, and is therefore out of GNSO policy-making scope.

5.7.3 Recommendations

None.

5.8 False Affiliation

5.8.1 Issue / Definition

Web site that is falsely purporting to be an affiliate of a brand owner.

5.8.2 Background

The RAPWG had consensus that this is a pure Web site use issue with no inherent relation to a domain name or registration process, and is therefore out of GNSO policy-making scope.

5.8.3 Recommendations

None.

5.9 Domain Kiting / Tasting

5.9.1 Issue / Definition

Registrants may abuse the Add Grace Period through continual registration, deletion, and re-registration of the same names in order to avoid paying the registration fees. This practice is referred to as “domain kiting.” This term has been mistakenly used as being synonymous with domain tasting, but it refers to multiple and often consecutive tasting of the same domain name.

5.9.2 Background

Bob Parsons appears to have introduced the term “domain kiting” in a blog post in 2006. In the post he chose to call the activity “kiting”, but his definition described what later came to be

termed “domain tasting” (as The Public Interest Registry did in its letter to Steve Crocker on March 26, 2006). This confusion of terms carried forward for some time as can be seen in a MessageLabs report published several months later.

Eventually, the current definition of domain kiting (the serial re-registration of a domain to get a domain for free) solidified. Domain tasting is a different practice, in which a registrant measures the monetization potential of a domain during the Add Grace Period, and deletes it in AGP if the domain is not worth keeping.

ICANN staff looked into domain kiting (while developing the 2007 Issue Report on domain tasting) and could not find anything except anecdotal evidence of the activity. A RAPWG member performed an analysis of the .INFO registry in 2008 and again in December 2009, and did not find any examples of kiting. [1] However domain kiting was a factor in a broader complaint brought by Dell and Alienware against various registrars and individuals in 2007 [here's the link -- http://www.domainnamenews.com/images/dell_doc1.pdf]

5.9.3 Recommendations

It is unclear to what extent domain kiting happens, and the RAPWG does not recommend policy development at this time. The RAPWG suggests that the Council monitor the issue (in conjunction with ongoing reviews of domain-tasting), and consider next steps if conditions warrant.

The WG achieved unanimous consensus on the above recommendation. *In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O’Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.*

6. Malicious Use of Domain Names

The WG discussed how these problems relate to the scope of the Working Group's activities as well as GNSO policy-making. In general, the RAPWG found that malicious uses of domain names have limited but notable intersections with registration issues.

The RAPWG acknowledges that e-crime is an important issue of the ICANN community. The Internet community frequently voices concern to ICANN about malicious conduct and, in particular, the extent to which criminals take advantage of domain registration and name resolution services. Various parties—including companies, consumers, governments, and law enforcement—are asking ICANN and its contracted parties to monitor malicious conduct and, when appropriate, take reasonable steps to detect, block, and mitigate such conduct. The question is what ICANN can reasonably do within its mission and policy-making boundaries.

6.1 Issue / Definition

The RAPWG was asked by the GNSO Council to examine issues surrounding illicit uses of domain names, an outgrowth of learning done about that topic in the Fast-Flux Working Group (FFWG). Specifically, the GNSO Council resolved:

- "The Registration Abuse Policy Working Group (RAPWG) should examine whether existing policy may empower Registries and Registrars, including consideration for adequate indemnification, to mitigate illicit uses of Fast Flux," and
- "To encourage ongoing discussions within the community regarding the development of best practices and / or Internet industry solutions to identify and mitigate the illicit uses of Fast Flux."[22]

[22] http://gnso.icann.org/meetings/minutes-03sep09.htm

Malicious or illicit behavior may be mitigated by stopping the domain name from resolving. This can be accomplished by the sponsoring registrar or registry by: applying an EPP Hold status; by removing or changing the nameservers delegated to the domain; or by deleting the domain name. Some malicious behaviors may be stopped by the hosting provider, and that may be the most appropriate action depending upon the specific case. (For example, hosting providers can take down individual phishing pages while the rest of the Web site continues to resolve.) But in the ICANN context, stopping resolution of the domain is the relevant issue, since that is what registrars and registries have the technical ability to make happen.

This issue is common to many types of abusive or malicious behavior – not only illicit fast-flux, but also spamming, malware distribution, online child pornography, phishing, botnet command-and-control, 419 scams, and others. Some specifics related to some common malicious abuses are noted below.

The RAPWG also discussed how the basic accessibility of WHOIS, the accuracy of contact data, and the use of proxy contact services are registration issues related to the malicious use of domain names.

6.2 Background

ICANN possesses a limited technical coordination function for the DNS. The Internet is a huge and sprawling environment that crosses international borders. It is decentralized by design, and involves millions of parties all exercising ownership of or control over various assets and infrastructure. These parties include network and telecom operators, ISPs, RIRs, registrants, registrars, registry operators, corporations and organizations, governments, the root operators, and more. The Internet and its users also depend upon hardware and software vendors, such as the creators of operating systems and Web browsers. All of these parties are vulnerable to and are often leveraged by criminals. As a result, no one party -- and no one type of entity -- has the power to solve the problem of e-crime alone. Indeed, security experts agree that e-crime cannot

be solved – it can only be fought, and hopefully contained, just like offline crime. In the end, all responsible parties have a role to play. Collaboration, data sharing, and education are effective and important tools for dealing with Internet security problems.

Law enforcement becomes involved in only a tiny percentage of e-crime incidents, due to the limited resources available, the large number of incidents, and the difficulties of investigating and prosecuting across national borders and jurisdictions. Instead, the great bulk of abusive or criminal behavior is dealt with via terms of service and contractual rights. The standard mitigation model on the Internet is that malicious behavior is reported to the service provider(s) who may have the right and ability to do something about it. Malicious domain name use is reported to the relevant hosting provider and/or to the sponsoring registrar (and occasionally to the registry operator). The registrar is the ICANN-related party with the direct relationship with—and a direct contract with—the registrant. The registrar (and/or registry) may determine if the use violates its legal terms of service, and decides whether or not to take any action.

Registrars always include language in their registrar-registrant contracts that allows the registrar to suspend or cancel a domain name. The language and terms vary among registrars, and the RAPWG examined this in its explorations of contract uniformity. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if payment fails. Some registrar-registrant agreements are broader and allow the registrar to suspend a domain at any time for any reason, or for no reason. It appears that registrars are empowered to mitigate abusive uses of domains if they so choose, and indeed registrars use that freedom to suspend gTLD domains as a matter of daily business.

Some registrars may have terms that address specific domain name uses or abuses. For example, the RAPWG saw how GoDaddy's Universal Terms of Service contains a fairly unique prohibition against use of domain names for "activities associated with the sale or distribution of prescription medication without a valid prescription."[23] Some RAPWG members commented

[23] http://www.godaddy.com/gdshop/agreements.asp

that such contractual variances are a way that registrars differentiate themselves in the market, and they can help registrars adhere to the laws of the jurisdictions in which they are incorporated or operate.

Some gTLD and ccTLD registry operators also have anti-abuse policies or provisions. Neustar's .BIZ contract with ICANN require that "The registered domain name will be used primarily for bona fide business or commercial purposes," and Neustar has relied on that requirement to suspended domains being used for phishing and malware distribution. Anti-abuse policies have also been instituted at the initiative of registry operators. For example, both The Public Interest Registry (.ORG) and Afilias (.INFO) instituted policies under their existing rights in their ICANN-registry and RRA contracts.[24],[25] The resulting anti-abuse policies include lists of prohibited abuses and reiterate the registry's right to suspend domain names. To create these anti-abuse policies, the registry operators relied upon contract provisions that allow the registry operator to "establish operational standards, policies, procedures, and practices for the Registry TLD", in a non-arbitrary manner and applicable to all registrars, and consistent with ICANN's standards, policies, procedures, and practices and the registry's Agreement with ICANN. Most ICANN-registry contracts contain provisions such as the ones relied upon by the .INFO and .ORG registries.

So, it appears that all registrars and most, if not all registries are already empowered to develop anti-abuse policies and mitigate malicious uses if they wish to do so. In addition, they may use the Expedited Registry Security Request (ERSR, discussed below) to address threats to the DNS or their TLDs.

---

[24] See: http://www.pir.org/index.php?db=content/Website&tbl=About_Us&id=14 and section 3.5.2 of the .ORG Registry-Registrar Agreement (RRA) at http://www.icann.org/en/tlds/agreements/org/appendix-08-08dec06.htm

[25] See http://www.info.info/info/abusive_use_policy and section 3.5.2 of the .INFO Registry-Registrar Agreement ("RRA") at http://www.icann.org/en/tlds/agreements/info/appendix-08-08dec06.htm

Some malicious uses of domain names involve legitimate domain name registrations that are compromised or infected by criminals and then used to perpetrate crimes such as phishing and malware. The RAPWG notes that any policy or recommendations must not adversely impact innocent parties, including the registrant and the registrar.

RAPWG members also noted that malicious use of domain names varies significantly by TLD, and some gTLDs have low-to-nonexistent problems. Many factors may explain this, including: eligibility or locus requirements; general availability; price; the registrars the TLD is available through and whether any of those registrars maintains less-than adequate defences or response capabilities; and the general whims of e-criminals. This raises the question of whether "one-size-fits-all" policies are relevant or needed. A WG member suggested that verification of users might be a potential approach to consider suitable for policy development, while others felt that required pre-screening of registrants raises many operational and economic issues.

It was pointed out that as a business practice, some registrars suspend or delete domain registrations that have not been used for phishing, malware, etc. when they discover that the registrant is using at least some of their domains for malicious purposes. In these cases, the registrant has broken the terms of service agreement.

It was suggested that injecting uniform requirements can sometimes be counterproductive – it can inject limitations into a situation where flexibility is often required, and might tie the hands of registries and registrars by reducing or limiting their ability to effectively respond. It was suggested that best practices or minimum standards could be explored. The importance of due process was also noted.

6.3 Intent, Risk, and Indemnification

The decision to suspend a domain name is up to the discretion of the registrar or registry operator, as per their terms of service. Suspending domain names involves risk. Registrars and registry operators especially wish to avoid suspending the domain names of innocent parties (a

"false-positive"). A mistake can take an innocent registrant's Web site and e-mail offline and potentially cause significant economic damage and other problems for the registrant. In turn, the registrar or registry operator may face legal action, and may further face customer service and public relations problems.

The RAPWG's members also discussed the issue of registration intent. It was agreed that assessing what a domain name will be used for at the time of its registration requires speculation about future intent, which can never be accurate 100% of the time. Some members suggested that if one was able to determine at the time of registration that a domain name will be used for an abusive activity, it might then be considered registration abuse. Some stated that it is not possible to reliably determine at the time of registration whether a domain will be used for phishing, spam or malware. Members provided examples of when it has been possible to predict intent to a high degree of confidence, such as in certain cases of ongoing criminal behavior. Such cases seem somewhat rare, the particulars can vary greatly between cases and over time, and they usually involve small numbers of gTLD domains – perhaps dozen to hundreds over time.[26] So for these reasons, even if such cases were determined to be registration abuse, there were doubts that they would be good candidates for ICANN policy-making.

Diligent registrars and registries have procedures for investigating abuse claims. These involve performing diligence and documenting problems as a way to protect registrants and minimize false-positives, to avoid risk, or to balance risk with the benefits of stopping malicious behavior. Some registrars and registries may avoid risk by declining to suspend domains at all, or only in the most pressing circumstances. Some may see domain name use as an issue they should not

[26] An example are the domains registered by the "Rock Phish" and "Avalanche" phishing operations. These gTLD and ccTLD domains were registered regularly, in batches, and contained characteristic string patterns. The case of Conficker was unusual in that it involved thousands of *unregistered* gTLD domain strings over time; see the commentary of Conficker and the Expedited Registry Security Request Process (ERSR) elsewhere in this paper.

make judgments about at all. As far as is known, there are no registrars or registry operators that trust heuristics or abuse blacklists in order to automatically suspend abusive domain names. Apparently all require the decisions to be made by an authorized person. Often this function resides with an attorney, a compliance officer, or a specially trained analyst.

WHOIS data is an integral part of the investigation process used by registrars, registry operators, law enforcement, and many other parties affected by malicious use of domains. The RAPWG discussed how the basic accessibility of WHOIS, the accuracy of contact data, and the use of proxy contact services are registration issues related to the malicious use of domain names. Accessibility of WHOIS data is discussed elsewhere in this paper, and upcoming GNSO studies will investigate how the contact accuracy and proxy issues are related to e-crime.

The Fast-Flux Working Group also discussed the issues of false-positives and intent. The FFWG examined case studies that show that fast-flux detection systems create false-positives, and that it is not always possible to determine the intent that some fast-flux domains are being used for. There was discussion of how detection systems would need to yield an "acceptably low" level of false-positives, but no agreement about what that level would be. Also, "In order to constrain the working definition of fast flux to lie within the scope of ICANN to address, the FFWG also tentatively agreed to limit the definition to the operation of the DNS and its registration system, specifically excluding the question of what constitutes criminal intent."[27]

Along with the provisions that allow them to suspend domains names, registrar and registry contracts include indemnification language. Current ICANN-registry and registry-registrar contracts –and virtually all registrar-registrant agreements—obligate registrants to abide by ICANN, registry, and registrar policies, and require registrants to indemnify and hold harmless

[27] "Final Report of the GNSO Fast Flux Hosting Working Group", page 26: http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf

registrars and registries for enforcing those policies.[28] This language is designed to protect the registrar or registry from claims and damages brought by the registrant.

An issue raised in the RAPWG is that indemnification language may not always an effective or practical protection. Despite indemnification language, gTLD registries and registrars have been sued by registrants for enforcing their terms of service.[29], [30], [31] Such legal proceedings can have

---

[28] For example, the .COM Registry-Registrar contract that is part of VeriSign's contract with ICANN says: "2.14. Indemnification Required of Registered Name Holders. In its registration agreement with each Registered Name Holder, Registrar shall require each Registered Name holder to indemnify, defend and hold harmless VNDS, and its directors, officers, employees, agents, and affiliates from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses arising out of or relating to the Registered Name holder's domain name registration." http://www.icann.org/en/tlds/agreements/verisign/appendix-08-01oct08.pdf

[29] In *Davies v. Afilias Ltd*., 293 F.Supp.2d 1265 (M.D. Fla. 2003), a registry operator was sued in a U.S. district court for locking Sunrise domains that the registrant did not have a right to possess, even though the registrant was bound to relevant terms and conditions and had indemnified the registry operator. In the course of the action, it was claimed that defendant Afilias incurred approximately US$100,000 in damages as a result of responding to the action. The court found that: "Plaintiff did not follow these rules, but rather subverted the process by attempting to register domain names for his own use before the names were offered on any basis to the general public, Defendant's 'interference' by locking the domain names was, as a matter of law, justified....summary judgment in Defendant's favor is appropriate." http://scholar.google.com/scholar_case?case=10308248522650356354&q=%22293+F.+Supp.+2d+1265%22&hl=en&as_sdt=2002

[30] See *Stephen Weingrad and Weingrad & Weingrad, P.C. vs. Telepathy, Inc,, Network Solutions, Inc., and Namebay S.A.M.* (05 Civ. 2024 (MBM), United States District Court for the Southern District of New York; 2005 U.S. Dist. LEXIS 26952). In this case, a registrar was sued after performing standard renewal and redistribution operations. Registrar Network Solutions notified registrant Weingrad of the upcoming expiration of his domain name. Weingrad failed to renew and the domain expired. When offered, Weingrad then declined to pay Network Solutions a standard redemption fee to redeem the name. The domain eventually became available, and was registered by another registrar. Weingrad then sued Network Solutions. The case was dismissed, and the court noted that Weingrad was bound by the

significant costs in money and resources, even though the registry or registrar was within its legal rights and may have thought that it had exercised good faith. And as referenced above, registrars have suspended domain names within their rights and then encountered customer and public relations problems, which have costs of their own. Indemnification language in ICANN contracts may fall short of being a true legal "safe harbor," which reduces or eliminates a party's liability under the law.

The domain-takedown and indemnification issue may come down to this: If a registrar or registry chooses to suspend a domain for malicious use, it is deciding to assume the risk and bear responsibility for possible consequences. But ICANN apparently does not have the power to require registries or registrars to suspend domain names for use issues, and if it did, then provisions to fully protect the contracted party from exposure to harm incurred by implementing ICANN-required mitigation procedures must be considered.

6.4 The Expedited Registry Security Request (ERSR)

The RAPWG discussed the new ERSR, which offers a flexible, contract-related response mechanism for registries to respond to significant malicious threats to the DNS itself or a TLD's operations.

Registration Agreement between him and Network Solutions. Network Solutions believed that it had acted within its Registration Agreement, and within ICANN policies. However, Network Solutions incurred over US$80,000 in legal fees defending itself.

[31] There are many examples of how registrars have encountered difficulties after suspending domain names as per legal requirements and/or the registrar's terms of service. A few include:

- http://www.nytimes.com/2008/03/04/us/04bar.html?_r=3&scp=1&sq=liptak&st=nyt&oref=slogin&oref=slogin
- http://en.wikipedia.org/wiki/Network_Solutions#Fitna_controversy
- http://en.wikipedia.org/wiki/Godaddy#Suspension_of_Seclists.org
  http://en.wikipedia.org/wiki/Godaddy#Deletion_of_FamilyAlbum.com

The Expedited Registry Security Request (ERSR)[32] was developed to "provide a process for gTLD registries who inform ICANN of a present or imminent security incident (hereinafter referred to as “Incident”) to their TLD and/or the DNS to request a contractual waiver for actions it might take or has taken to mitigate or eliminate an Incident. A contractual waiver is an exemption from compliance with a specific provision of the Registry Agreement for the time period necessary to respond to the Incident. The ERSR has been designed to allow operational security to be maintained around an Incident while keeping relevant parties (e.g., ICANN, other affected providers, etc.) informed as appropriate."

The ERSR was a result of learning from the Conficker problem, and was published for pubic comment in September 2009. The ERSR was included in the Draft Applicant Guidebook, draft 3 (DAG3) so as to be made available in new TLDs that may be introduced in the future.

The ERSR framework allows flexibility, which will be necessary for responding to the unknown and possibly novel threats to the DNS or TLDs that may arise in the future. It also allows registries to propose operational solutions that may be suited to the situation at hand, and to the registry's technical and operational capabilities. For example, in the case of another Conficker, registries could be allowed to perform relevant domain name blocking and/or registration themselves, or could accommodate arrangements in which a trusted party would register relevant domain names and would receive fee relief from ICANN and the registry. The ERSR also provides for expedited action, and process that involves legal and security experts at ICANN and the registry or registries involved.

[32] http://www.icann.org/en/registries/ersr/

6.5 Other Notes

Registrars are often viewed by the public as the key to successfully resolving malicious conduct because the registrars directly interact with those registrants who misuse domain names, and because registrars have freedom to set their terms of service.

- It has been observed that registrars' responses and defensive mechanisms vary widely in effectiveness and timeliness, and that some registrars are much less inclined to address e-crime than others.
- Registrars are the parties that generally possess the most information that can be used to assess the trustworthiness of a registration and a registrant and can link it to malicious behavior. These include credit-card data (criminals often use stolen credentials; see below), the true registrant's identity (when protected by a proxy contact or privacy service), the IP of the registrant, and what domains that registrant has registered in other TLDs.
- RAPWG members observed that malicious use of domain names varies significantly by sponsoring registrar. [33]
- Members also discussed apparent recurrent abuse by resellers, which goes back to how registrars deal with their various agents, how those agents are bound to ICANN policies, and how registrars are held accountable for the actions of their resellers.

Some members of the Internet security community are convinced that a small number of domain name registrars knowingly tolerate malicious abuse, or are actively involved in it. Such cases need the attention of ICANN and its compliance department. A key question is what tools are needed and are appropriate to deal with this worst-case behavior.

Given the above, the logical question is whether there are any registration-related policies that can be used to positively affect such problems.

[33] For example, see http://rss.uribl.com/nic/

6.6 Examples of Malicious Uses

Phishing

Phishing is a Web site fraudulently presenting itself as a trusted brand in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords). The goal of phishing is usually the theft of funds or other valuable assets. The great majority of domains used for phishing are compromised or hacked by phishers, and the registrants are not responsible for the phishing. Such cases are not registered for bad purposes and therefore present cases where there is no inherent registration issue, and where mitigation must be handled carefully.

RAPWG members Rod Rasmussen and Greg Aaron publish semi-annual Global Phishing Surveys via the Anti-Phishing Working Group.[34] Findings from these reports include these relevant to registration and use issues:

- About 81% of domains used for phishing are compromised or hacked by phishers, and the registrants are not responsible for the phishing. These domains should therefore not be suspended, and mitigation must usually be performed by the hosting provider. "Malicious" domain registrations totalled about 5,591 domain names in all gTLDs and ccTLDs worldwide in the first six months of 2009. This was about 18.5% of the domain names involved in phishing.
- Only about 3.5% of all domain names that were used for phishing contain a brand name or variation thereof, designed to fool visitors. Placing brand names or variations thereof in the domain name itself is not a favored tactic of phishers, since brand owners are

[34] The last three reports were: First Half 2009: http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf, Second Half 2008: http://www.apwg.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf , First Half 2008: http://www.apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf

proactively scanning Internet zone files for such names. Instead, phishers usually place brand names in subdirectories or on subdomains in an attempt to fool Internet users. Most maliciously registered domains were random strings, such as "hodfw42hj.com.es", which offered nothing to confuse a potential victim.

- Phishers are increasingly using subdomain services to host and manage their phishing sites. These services are below the level provided by registries and registrars, and use of subdomains is not subject to policies maintained by ICANN. Phishers use such services almost as often as they register domain names. Such attacks even account for the majority of phishing attacks in certain large TLDs. This trend shows phishers migrating to services that cannot be taken down by registrars or registry operators.
- Phishing (and phishing using maliciously registered domains) varies greatly by TLD. Many factors may explain this, including general availability or nature of the TLD, price, the registrars the TLD is available through, and locus or eligibility requirements.

The RAPWG had consensus that phishing is generally a domain name use issue. Those cases that involve misleading use of brand names in the domain string may be treated as cases of cybersquatting.

Spam

Spam is generally defined as bulk unsolicited e-mail. Spam may be sent from domains, and spam is used to advertise Web sites.

Statistics published by various service providers show that spam levels vary significantly by TLD and by registrar.[35]

The RAPWG had consensus that spam is generally a domain name use issue. Those cases that involve misleading use of brand names in the domain string may be treated as cases of cybersquatting.

[35] For example: http://rss.uribl.com/tlds/ and http://rss.uribl.com/nic/

Malware / Botnet Command-and-Control

Malware authors sometimes use domain names as a way to control and update botnets. Botnets are composed of thousands to millions of infected computers under the common control of a criminal. Botnets can be used to perpetrate many kinds of malicious activity, including distributed denial-of-service attacks (DDoS), spam, and fast-flux hosting of phishing sites.

Relevant malware (including that associated with Srizbi, Torpig, and Conficker) on these infected machines attempts to contact domains included on some sort of pre-determined list or generated via an algorithm. If the botnet's master has deposited instructions at one of these valid domains, the botnet nodes will download those instructions and carry out the specified malicious activity, or update themselves with improved code.

It is notable that especially in the case of Conficker, these lists were not domain names that had been created – the great majority of the domains strings had not yet been created as domain names. They were essentially domains that might be registered at some point in the future by the criminal in question. Further, some of the valid domains may already be registered to innocent parties by coincidence.

If the relevant domain name list or domain-generation algorithm is known, white-hat parties (such as security researchers, registries, and registrars) can register and/or monitor the relevant domains. In the case of Conficker, white-hat parties registered the domain names that could have been used for command-and-control, successfully disrupted the botnet, and prevented much of it from being updated or controlled. These parties also sinkholed traffic to those domains (directed traffic to nameservers the researchers controlled). This allowed them to identify the IPs of infected computers, thus estimating the size of the botnet and enabling mitigation and cleanup efforts.

There are several ways in which malware authors and botnet "herders" utilize domain names they control or plan to control at some point in conjunction with their schemes. The most common and well understood is using websites under domains they control to distribute new malware infections to victims. This is often done via social engineering, where the malware is disguised as something else. More and more, we are seeing so-called "drive-by" infections, where a malware author simply gets a victim to visit their site via a browser that is not fully patched or is vulnerable due to a "zero-day exploit". Malware authors are also using domain names to facilitate communication with infected machines and/or to actually control large botnets. Many different malware families use pre-defined "rendezvous" domain names that are hard coded into an initial downloaded piece of malcode. These rendezvous domains will provide further instructions using some sort of communications method, that is often, but not necessarily web-based, to relay further instructions or to provide more malware to download to the infected machine. Typically, the malware author will need to register such domains prior to deployment of their code in the wild. Other, more sophisticated malware programs (e.g. Conficker, Srizbi, Torpig), use a pre-defined algorithm to get updates from domains based on the current time and perhaps other conditions. This allows malware authors to pick and choose when and what domains to register in order to provide more instructions or control their botnets.

- Descriptions of Conficker can be found at the Conficker Working Group (http://www.confickerworkinggroup.org) and on Wikipedia: http://en.wikipedia.org/wiki/Conficker
- Srizbi info is also at Wikipedia: http://en.wikipedia.org/wiki/Srizbi_botnet plus a write-up on the domain calculator it uses at ThreatExpert.com: http://blog.threatexpert.com/2008/11/srizbis-domain-calculator.html.
- A relevant research paper is: "Your Botnet is My Botnet: Analysis of a Botnet Takeover" by researchers at the University of California, Santa Barbara: http://www.cs.ucsb.edu/%7Eseclab/projects/torpig/torpig.pdf.

  Section 3 of this paper contains a very useful description of how the Torpig bot is controlled via domain names. The Conficker botnet uses a similar means. As the Santa

> Barbara authors note, "The use of domain flux in botnets has important consequences in the arms race between botmasters and defenders. From the attacker's point of view, domain flux is yet another technique to potentially improve the resilience of the botnet against take-down attempts. More precisely, in the event that the current rendezvous point is taken down, the botmasters simply have to register the next domain in the domain list to regain control of their botnet. On the contrary, to the defender's advantage, domain flux opens up the possibility of sinkholing (or "hijacking") a botnet such as Torpig." The Conficker bot is protected by sophisticated encryption, and its nodes will only download instructions from a domain that provides an authenticated response.

Newer variants of Conficker generate 50,000 potentially viable domains per day, spread across more than 100 TLDs. Registering all the domains generated by Conficker at market prices would therefore carry an enormous cost. (The Santa Barbara team estimated the cost at between $91.3 million and $182.5 million per year.)

Some registries blocked the viable Conficker domains. Those registries refused all attempts to create the relevant domains, thereby keeping them out of the hands of all parties for a certain period of time. Some registry operators were able to accomplish blocking, while others were not able to do so due to technical or policy reasons.

It is generally agreed by the members of the Conficker Working Group[36] that:

1) Fighting Conficker by acquiring and/or blocking domains was a success in many ways and was worth attempting. The effort prevented many nodes from being updated or controlled, and many nodes were identified and removed from the botnet.
2) The counter-measure of acquiring and/or blocking domains is probably not scalable in the long term. It is expected that criminals may expand the numbers of domains their malware

[36] http://www.confickerworkinggroup.org

algorithms use. The blocking efforts also depend upon the flawless and continued participation of all relevant TLD registry operators.

6.7 Use of Stolen Credentials

6.7.1 Issue / Definition

Criminals often use stolen credentials—such as stolen credit card numbers—to register domain names for malicious purposes. Is this a registration issue, and what if any solutions can be pursued through ICANN?

6.7.2 Background

For the purposes of examining registration abuse and the "use of stolen credentials", there are three usages that seem to apply:

1. "Identity credentials" – Credentials that establish identity (e.g. personal identification cards, stored personal information)
2. "Access credentials" – Credentials that control access to computer systems (e.g. username and password, digital certificates)
3. "Financial credentials" – Credentials that provide access to financial accounts (e.g. credit and debit cards).

Some blending of usages would apply in some cases as well. For example, the use of a stolen e-mail account to establish identity or the authority to modify access to financial credentials crosses multiple definitions.

Given the disparate nature of the uses and protections against abuse the types of credentials identified each have, it would seem prudent to examine them individually. Some commonalities may present themselves to allow for unified approaches.

Identity Credentials

In general, stolen identity credentials allow a miscreant to assume or impinge the identity of another in order to perpetuate one of their own schemes. This can manifest itself in the use of purloined personal information to make a domain registration appear to be legitimate (e.g. false WHOIS) or in allowing a perpetrator to assume control over access or financial credentials. The latter case can be explored in-depth in examining those other two credential types, but the former case is worth considering further.

1. Fraudsters use misappropriated identities of the actual individuals or institutions targeted by a particular scheme in conjunction with a domain registration. The fraudster wishes to make the domain name appear to be associated with the actual victim in order to make their scheme more viable to other victims, and/or their application for the domain legitimate.
2. Miscreants use identities of random, but real individuals/organizations in conjunction with a domain registration, unrelated to the actual fraud scheme. Use of real data may allow the miscreant to fool anti-fraud measures put in-place by the registrar. Victims of the actual scheme may be put at ease by the appearance of "real" verifiable domain ownership information in WHOIS, or they may make complaints against innocent parties. The stolen identity data may well cause delays in authorities investigating the scheme, as innocent parties are scrutinized. The person who is "spoofed" in this instance may be the registrant for other domains, which may also allow the registration to get past anti-fraud measures, especially if the registrar being used is the same.
3. The miscreant uses stolen identities in conjunction with stolen financial credentials to bolster their fraud efforts when registering a domain. Including the stolen access information in WHOIS and/or account information that matches stolen credit card data can help avoiding anti-fraud systems, as well as all the benefits mentioned above.

Access Credentials

A miscreant can do quite a bit of damage with stolen access credentials. Outside of reselling those credentials, the real value of stolen access credentials lies in what is possible to do with the systems to which those credentials provide access. Two possible attacks seem to be meaningful within the confines of "domain registration abuse" examined here. First are direct attacks against registrar/reseller systems using stolen access credentials for that service. Second, a perpetrator could launch an indirect attack via access credentials to other accounts.

1. A miscreant with direct access to a domain management account can make new domain registrations using funds or "credits" that account may have with the reseller or registrar. Obviously domains can be taken over, deleted, or otherwise sabotaged from such a compromised account, but those scenarios are likely outside the scope of "registration abuses". Further, a miscreant may be able to gain access to credit card information that is stored in such an account, or affect purchases with that card that directly benefit that criminal. Again, this is outside scope, as this is more of a theft problem than a domain registration issue, but it is likely a concern that could come up in discussions of this topic.
2. If a fraudster has access to an account that is used to verify identity or confirm change requests, like an e-mail account, they can either attempt to gain access/control over a domain management account, or use a domain registration verification process to register domains using someone else's account/identity. Some domain resellers may use legacy models based on the original e-mail based registration and modification system, which would allow for fraudulent domain registrations based on e-mail confirmations.
3. If a criminal has access via stolen credentials (or simply hacking) into a computer/server that is part of some automated domain registration system, they can subvert that system. With such control, new domains can be registered using the victim's automated access to registrar systems. Of course hijacking, sabotage, and other acts can be perpetuated as well, just as if the miscreant had access to an account with the registrar/reseller.

Financial Credentials

Abuses perpetrated with stolen financial credentials are fairly straightforward. The criminal can utilize those credentials to fraudulently register domains and other related resources. This is quite common practice with criminals today, with most of the domains registered in this manner being used to perpetuate other crime, fraud, and abuse. Such credentials include credit cards, debit cards, on-line banking, alternate payment systems (e.g. PayPal), ACH systems, and other various means for affecting payments for domain name transactions.

An interesting aspect for domain name registration via stolen financial credentials versus other types of fraud done via stolen financial credentials is the need to establish domain ownership information (whois and/or account) and domain deployment characteristics (nameservers) at the time of registration. This allows for some unique techniques to expose fraudulent registrations via stolen financial credentials.

Observed abuses

Use of stolen financial credentials would seem, at first glance, to be the primary abuse seen today. Thousands of domains are registered daily using such credentials to perpetuate all sorts of criminal and abusive schemes. However, there has been a shift of late in the way criminals are amassing infrastructure resources, with more emphasis being placed on obtaining access credentials to infrastructure elements. Some level of stolen identity credential abuse co-exists with these other abuses as well, so all three areas deem at least some consideration.

Roles for policy and other industry-wide approaches

These three types of uses of stolen credentials present different opportunities for mitigation efforts, both at the individual registrar/reseller level and across the industry. Some registrars and resellers see fairly frequent abuse, especially of stolen financial credentials, while others do not. There are opportunities for dissemination of best practices, plus potential for “minimum standards” for dealing with various types of abuse in this arena. Further, given the unique nature of domain names requiring access to a shared data system (the zone files) with detailed

ownership/contact data in order to function and be in compliance, there may be ways to share information about fraudulent activities occurring at some registrars/resellers to curb those abuses across the industry. No formal system or policy for the latter currently exists.

Free-market forces have largely determined how different registrars and their resellers respond to these issues. There is a strong argument for allowing competition to dictate many of these responses, as there is continuous innovation in these areas, and many market participants compete on these features. And there is a strong argument that is an apparent free-market failure, in which registrars/resellers who appear to be fairly weak in practices to prevent such fraudulent registrations are generally not being penalized. The large numbers of fraudulent domains obtained through the methods discussed previously with infrequent sanctions evidences this. So the question becomes one of balance, as is often the case in such industry issues.

Complicating these issues are the large number of business models currently employed by domain registration companies. “Retail” registrars who sell direct to individuals and businesses will most often process transactions with credit cards or alternate payment services. There are many other models, including large “corporate” registrars that establish credit accounts, multi-level resellers, internal operations that register names on their own accounts, and more. This makes it more difficult to find solutions that effectively cover all vendors well. Perhaps concentrating on the areas that appear to have the highest incident of abuses would be prudent.

6.7.3 Recommendations Regarding Malicious Use of Domain Names

The RAPWG recommends the creation of non-binding best practices to help registrars and registries address the illicit use of domain names. This effort should be supported by ICANN resources, and should be created via a community process such as a working or advisory group

while also taking the need for security and trust into consideration. The effort should consider (but not be limited to) these subjects:

- ***Practices for identifying stolen credentials***
- ***Practices for identifying and investigating common forms of malicious use (such as malware and phishing)***
- ***Creating anti-abuse terms of service for inclusion in Registrar-Registrant agreements, and for use by TLD operators.***
- ***Identifying compromised/hacked domains versus domain registered by abusers***
- ***Practices for suspending domain names***
- ***Account access security management***
- ***Security resources of use or interest to registrars and registries***
- ***Survey registrars and registries to determine practices being used, and their adoption rates.***

The WG achieved strong consensus on the above recommendation*. In favour (12): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Shah (IPC), Sutton (CBUC), Young (RySG).*

Alternate view: One member (Rodenbaugh) expressed a belief that pure uses of domain names are an area in which ICANN can impose mandatory practices upon contracted parties.

7. WHOIS Access

7.1 Issue / Definition

The RAPWG found that the basic accessibility of WHOIS has an inherent relationship to domain registration process abuses, and is a key issue related to the malicious use of domain names. It appears that WHOIS data is not always accessible on a guaranteed or enforceable basis, is not always provided by registrars in a reliable, consistent, or predictable fashion, and that users sometimes receive different WHOIS results depending on where or how they perform the lookup. These issues interfere with registration processes, registrant decision-making, and with the ability of parties across the Internet to solve a variety of problems.

WHOIS is an area within GNSO policy-making scope and has had a long history of discussion. Below, the RAPWG comments on the basic availability of and access to WHOIS data, and not the accuracy of contact data or the use of proxy contact services. To avoid duplication of effort and charter scope problems, the RAPWG decided to identify when WHOIS is seen to be a contributing factor in other problems, and not to discuss WHOIS issues for which the GNSO has already commissioned studies. (Those are: WHOIS contact data accuracy, the use of proxy contact and privacy services, implications of non-ASCII registration data in WHOIS records, and technical requirements for the WHOIS service itself – including potential replacements. For background, please see: http://gnso.icann.org/issues/whois/)

WHOIS data availability problems have been discussed in other GNSO working groups, for example:

- The Post-Expiration Domain Name Recovery Working Group (PEDNR-WG) discussed how access to WHOIS data is essential for parties to determine if contact data has been updated upon the expiration of a domain name, and to check domain name expiration

dates. A majority of the registrars polled may make substantial updates to WHOIS data upon expiration.[37]

- The Inter-Registrar Transfer Policy Part A PDP Working Group (IRTP-WG)[38] noted in its final report that gaining registrars sometimes have difficulty accessing WHOIS data, and therefore Administrative Contact e-mail addresses.
- The Fast-Flux PDP Working Group (FFWG) discussed how responders must access WHOIS data when mitigating illicit uses of domain names.

Published WHOIS data for domain names involved in malicious conduct is an irreplaceable part of the investigation and mitigation processes used by registrars, registry operators, registrants, security companies, brand owners, victims, and law enforcement.

- The national law enforcement agencies of the United States, the United Kingdom, Australia, Canada, and New Zealand have recommended that "ICANN should require Registrars to have a Service Level Agreement for their Port 43 servers." These authorities consider that this is required in order "to aid the prevention and disruption of efforts to exploit domain registration procedures by criminal groups for criminal purposes."[39]

---

[37] "Draft Initial Report on the Post-Expiration Domain Name Recovery Policy Development Process": https://st.icann.org/data/workspaces/post-expiration-dn-recovery-wg/attachments/post_expiration_domain_name_recovery_wg:20100112125658-0-27743/original/Draft%20Initial%20Report%20-%20PEDNR%20PDP%20-%2012%20January%202010.doc

[38] "Draft Final Report on the Inter-Registrar Transfers Policy - Part A Policy Development Process": https://st.icann.org/data/workspaces/irtp_jun08_pdp-wg/attachments/irtp_part_a_pdp_wg_pdp_jun08:20090318145458-1-14319/original/Draft%20Final%20Report%20-%20IRTP%20Part%20A%20-%2018%20March%202009.doc%20%5BCompatibility%20Mode%5D.pdf

[39] "Law Enforcement Recommended RAA Amendments and ICANN Due Diligence", November 2009, https://st.icann.org/raa-related/index.cgi/LawEnforcementRAArecommendations%20(2).doc?action=attachments_download;page_name=05_january_2010;id=20091118185109-0-21002

- The Anti-Phishing Working Group's DNS Policy Committee has stated that published WHOIS is "an invaluable resource, in fact, without which most of the cited cases would not have been successful. For cases in which legitimate machines or services have been hacked or defrauded, published domain name WHOIS information is an important tool used to quickly locate and communicate with site owners and service providers. For cases where domain names are fraudulently registered, the published domain name WHOIS information can often be tied to other bogus registrations or proven false to allow for quick shutdown."[40]

7.2 Background

ICANN's current registry contracts require registry operators to adhere to port 43 WHOIS Service Level Agreements (SLAs). These SLAs require that port 43 WHOIS service be highly accessible and fast. For example, the .ORG contract requires that WHOIS service be functional at least 99.31% of the time per month (with exceptions for scheduled maintenance), and that responses be provided in less than 800 milliseconds. Failure of registries to meet these SLAs have been very rare according to monthly registry reports.[41]

The majority of gTLD registries are "thick" registries, in which all authoritative WHOIS data—including contact data—is maintained at the registry. The .COM and .NET registries are "thin," and contact data is located only at each domain name's sponsoring registrar. Registrars are therefore responsible for providing WHOIS service for .COM/.NET names so that contact data may be retrieved. The .COM/.NET registry contains approximately 85% of the gTLD domains in existence,[42] so registrar WHOIS accessibility is very important. When displaying WHOIS data for

[40] "Issues in Using DNS Whois Data for Phishing Site Take Down," http://www.antiphishing.org/reports/APWG_MemoOnDomainWhoisTake-Downs.pdf

[41] http://www.icann.org/en/tlds/monthly-reports/

[42] "VeriSign Domain Name Industry Brief," September 2009, http://www.verisign.com/domain-name-services/domain-information-center/domain-name-resources/domain-name-report-dec09.pdf

thick TLD domains names—especially on their Web sites—registrars often query the registry's WHOIS, and display that output to users.

The Registrar Accreditation Agreements (RAAs)[43] require that registrars provide:

- port 43 WHOIS access
- a Web-based WHOIS
- a listed set of information (WHOIS data fields), including:
    - identity of the registrar
    - domain name's expiration date
    - nameservers associated to the domain; and
    - specified fields of data for the Registrant Contact, Administrative Contact, and Technical Contact.

There are no service levels (SLAs) in the Registrar Accreditation Agreements (RAAs). A registrar-provided WHOIS service is not required to be online for any particular amount of time, nor provided with any particular response speed.

Port 43 is designed for use with automated and machine queries. It can also be queried manually by users who know how to perform telnet sessions and the "whois" command in Linux/Unix/macosx shell. The percentage of Internet users who are technically fluent enough to perform these types of queries (or even know about port 43 at all) is small. Thus, it is required that registrars have a Web-based WHOIS query on their sites.

A sub-team of RAPWG members performed some basic research by querying the Web-based and port 43 servers of 50 registrars. This set included the top 20 registrars by gTLD market share, 15 randomly-chosen mid-sized registrars, and 15 randomly-chosen small registrars. When a registrar's site was in a language other than English, the assistance of a native speaker was

[43] http://www.icann.org/en/registrars/agreements.html

obtained. In addition to manual checks, automated queries of port 43 were performed to test availability over time.

The sub-team members found WHOIS accessibility situations with 19 of the 50 registrars sampled. Four registrars may have been in violation of their contractual WHOIS access requirements:

- Two did not provide a functional Web-based WHOIS.
- One registrar's WHOIS listed a sponsoring registrar different from that provided by the .COM/.NET registry WHOIS. The registrar's port 43 server provided an expiration date different from that listed in the registry. The registrar's Web WHOIS provided two different expiration dates for the same domain name.
- One registrar did not identify the sponsoring registrar of its domains. The registrar does not operate its port 43 server on the domain indicated by the .COM/.NET registry WHOIS; the registrar's WHOIS service is evidently subcontracted to a second registrar on that registrar's domain; and the sponsoring registrar's Web WHOIS is provided on a third domain not branded as the sponsoring registrar.

In addition, one registrar provided facially invalid registrant contact data for its own .COM name -- including a registrant contact e-mail address on the domain "icann.org". This appears to be a violation of the RAA.

Fifteen other registrars presented these situations:

- Three registrars had port 43 servers that did not return replies for a notable number of queries. One was offline/nonresponsive 21% of the time, one was offline/nonresponsive 20% of the time, and one was offline/nonresponsive 14% of the time. (Based on 100 queries per registrar, spread out over several weeks).
- Ten provided different WHOIS data on their port 43 servers than they did via their Web WHOIS.
    - Four provided only thin contact data via their Web WHOIS, while providing thick contact data only on port 43.

  - In two cases, registrars provided two different expiration dates for each domain name via the Web WHOISes. One of the two expiration dates did not match the expiration date provided by the .COM/.NET registry.
  - Two sometimes provided full contact data on their Port 43 servers, and sometimes provided just Registrant contact data (and no Admin or Tech contact data) on their port 43 servers. It is unknown if this was due to a rate-limiting activity.
  - One registrar did not provide registrant contact data via port 43, and did not provide Admin or Tech contact data via its Web WHOIS.
  - One registrar provided a required data field (Tech and Admin contact phone numbers) on port 43 but not via its Web WHOIS.
- Four cut off telnet sessions to port 43 very quickly--effectively disallowing manual queries via that method.

These results indicate that:

1. Some registrars appear to be in violation of their contractual WHOIS accessibility obligations;
2. Users are occasionally unable to obtain contact data due to WHOIS availability problems.
3. Registrars occasionally provide registration data that differs from that provided by the registry.
4. Users are sometimes given different registration data depending on the method they use to access the sponsoring registrar's WHOIS.
5. Users are sometimes given different registration data depending upon who they are; perhaps depending upon whether they are being rate-limited.

These issues were distributed across a notable number of registrars, with different sizes, business models, and locations around the world.

The reasons why registrars provide different data on port 43 versus their Web sites requires further investigation. Some might be attempts to prevent automated data mining by spammers, competitors, and other parties. The RAPWG notes that reasonable rate-limiting WHOIS can be a valid, prudent practice – for example it can prevent spammers from mining WHOIS information[44], and can prevent WHOIS servers from being overwhelmed by excessive queries. During Web-based WHOIS sampling, the RAPWG members observed that only some registrars employ CAPCHAs on their Web-based WHOIS services as a protection against automated queries.

In addition to the research conducted by working-group members, the RAPWG requested information from the ICANN Compliance Department about how it monitors registrar WHOIS access. The ICANN Compliance Department noted: "ICANN has developed a Whois server audit tool which monitors access to registrars' Whois servers over a Port 43 connection. The script developed for this task retrieves data for 4 registered domain names for each accredited registrar…. The purpose of the audit is to flag Whois servers that are down for an amount of time that is suspect and probably not just a manifestation of periodic server maintenance or scheduled update. … What is the "reasonable amount of time" for a server to be down? Probably no more than an hour or so per day, although these are ICANN internal, 'soft metrics', not agreed-upon timeframes with registrars. The script records the results and flags registrars that prevent access to data on registered names. Transient network problems are less of a concern, so ICANN focuses on long-term behavior, i.e., registrars which ICANN is unable to communicate with for several days in a row. ….ICANN also reaches out to registrars that provide access to data on registered names but provide 'thin', not 'thick', Whois data. The former does not provide details on the registered name holder and additional contacts, which is required by the RAA."[45]

---

[44] See: "SAC 023: Is the WHOIS Service a Source for Email Addresses for Spammers?": http://www.icann.org/en/committees/security/sac023.pdf

[45] http://forum.icann.org/lists/gnso-rap-dt/msg00454.html

Over the last three years, ICANN's Compliance Department has sent seven escalated compliance notices (e.g. notices of breach, termination, or RAA non-renewal) to seven registrars for failure to comply with WHOIS access requirements of the Registrar Accreditation Agreement:

- One registrar did not have its contract renewed solely for failure to provide WHOIS access. (South America Domains dba NameFrog.com, which had less than 300 gTLD names under sponsorship at the time.)
- The other six registrars were cited for both WHOIS access breaches AND at least one other contract violation, such as failure to pay ICANN fees, failure to escrow data, and/or failure to respond to WHOIS accuracy complaints.

ICANN's Compliance Department is in contact with registrars to resolve issues before escalated compliance notices become necessary. The Compliance staff noted to the RAPWG that "some registrars block incoming WHOIS queries traffic by IP address, and Compliance works with the registrars to get them unblocked when there may be a misunderstanding." and, "Aside from metrics on informal outreach to resolve blocked Whois servers and incomplete, or 'thin', Whois data with registrars, which have been more than two dozen in the past 6-8 months, Compliance could provide bi-weekly statistics to the WG from here on out on the number of registrars that showed a pattern of restricting access to their Whois server over a Port 43 connection. These statistics have not been published before."

So, it appears that some contractual violations are cured in an amicable manner, and that public breach letters have apparently been used as a tool of last resort. It is unknown how many WHOIS accessibility issues have been discovered but not resolved.

The last time that ICANN published WHOIS access compliance data was 2007.[46] That year, ICANN's Compliance Department examined every ICANN-Accredited Registrar's Web site, and did not examine port 43 access. [47]

---

[46] http://forum.icann.org/lists/gnso-rap-dt/msg00454.html

[47] http://www.icann.org/en/compliance/reports/contractual-compliance-audit-report-18oct07.pdf

The Compliance Department numbers indicate that WHOIS access problems are found regularly. Above and beyond those, the RAPWG research indicates that a notable percentage of registrars might not make WHOIS data available in a reliable, consistent, or predictable fashion.

7.3 Recommendations

Recommendation 1:

The GNSO should determine what additional research and processes may be needed to ensure that WHOIS data is accessible in an appropriately reliable, enforceable, and consistent fashion.
The GNSO Council should consider how such might be related to other WHOIS efforts, such as the upcoming review of WHOIS policy and implementation required by ICANN's new Affirmation of Commitments. The Affirmation of Commitments says: "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 [30 September 2009] 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."[48]

The WG achieved unanimous consensus on the above recommendation*. In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.*

[48] http://www.icann.org/en/announcements/announcement-30sep09-en.htm

Recommendation 2.

The GNSO should request that the ICANN Compliance Department publish more data about WHOIS accessibility, on at least an annual basis. This data should include a) the number of registrars that show a pattern of unreasonable restriction of access to their port 43 WHOIS servers, and b) the results of an annual compliance audit of compliance with all contractual WHOIS access obligations.

The WG achieved unanimous consensus on the above recommendation. *In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.*

8. Uniformity of Contracts

8.1 Issue / Definition

Three specific charter objectives of the RAPWG were to:

- Understand if registration abuses are occurring that might be curtailed or better addressed if consistent registration abuse policies were established,
- Determine if and how {registration} abuse is dealt with in those registries {and registrars} that do not have any specific {policies} in place, and
- Identify how these registration abuse provisions are {...} implemented in practice or deemed effective in addressing registration abuse.

The RAPWG formed a sub-team to fully appreciate the current state environment of ICANN-related contracts and agreements, and then discussed the findings in the larger RAPWG.

8.2 Background

The Sub-Team was tasked with the specific topic of contract uniformity relative to abuse as defined by the larger Working Group, and presented its research to the larger WG. The sub-team's membership, meeting schedule, and meeting minutes are found on the RAPWG web site.

8.2.1 ICANN Agreement Landscape:

The following diagram is meant to define scope and visually represent the relationships between parties and the contracts that bind them. Additionally, nested relationships between the agreements themselves are depicted.

Market Participants:

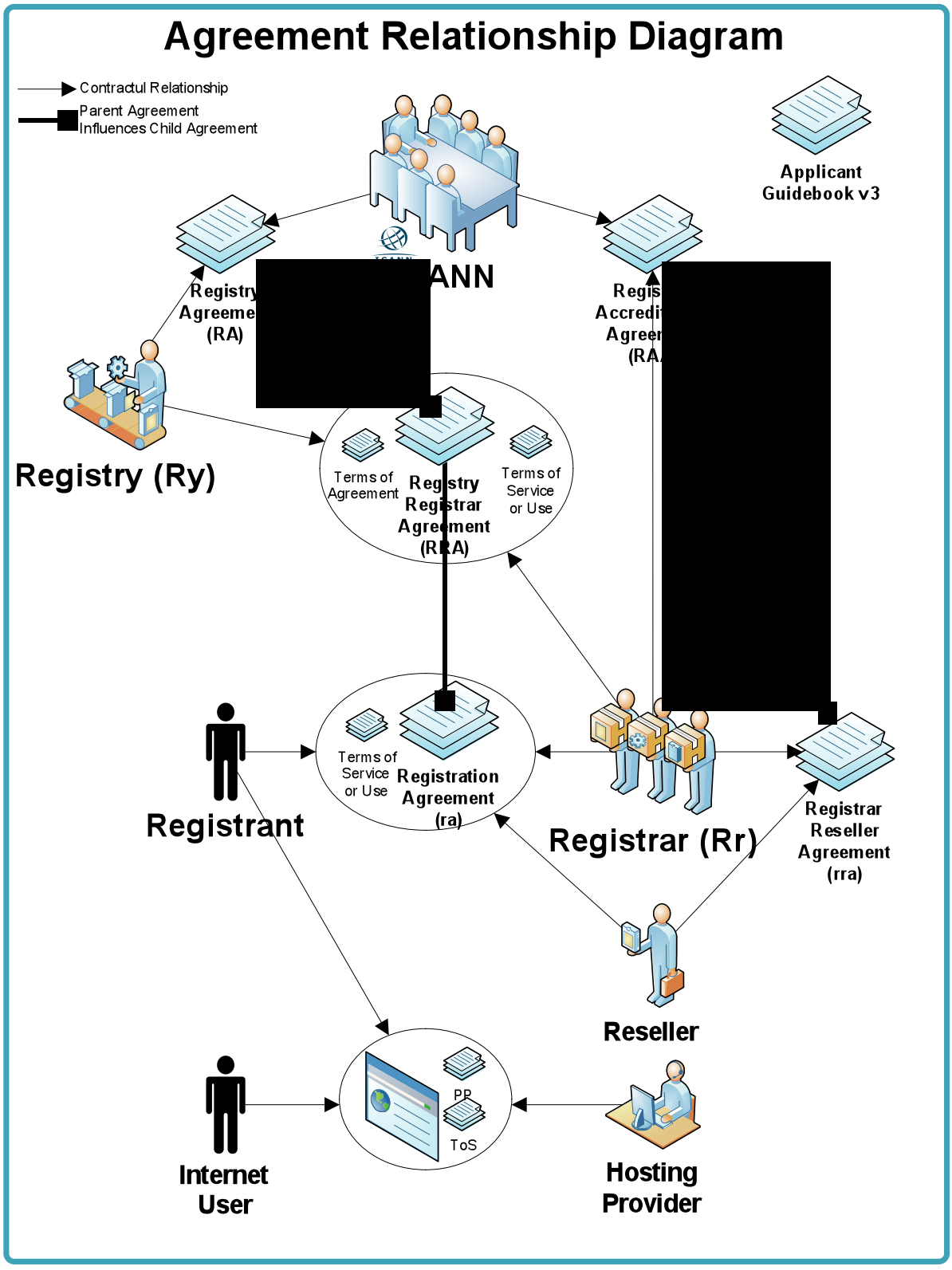
- ICANN
- Registry (Ry)
- Registrar (Rr)

- Registrant
- Hosting Provider
- Internet User

Agreements:

- Registry Agreement (RA)
- Registry Registrar Agreement (RRA)
- Registrar Accreditation Agreement (RAA)
- Registration Agreement (ra)
- Registrar Reseller Agreement (rra)**
- Terms of Service**
- Terms of Use**
- Terms of Agreement**

**Agreements typically not in scope of primary dispersion research


Agreement Relationship Diagram
Contractul Relationship
Parent Agreement
Influences Child Agreement
Applicant Guidebook v3
ANN
Registry Agreeme (RA)
Regis Accredi Agreer (RA
Registry (Ry)
Terms of Agreement
Registry Registrar Agreement (RRA)
Terms of Service or Use
Terms of Service or Use
Registration Agreement (ra)
Registrant
Registrar (Rr)
Registrar Reseller Agreement (rra)
Reseller
PP
ToS
Internet User
Hosting Provider

8.2.2 Dispersion Research

Registry Agreement (RA) Dispersion:

Refer to the GNSO Issues Report on Registration Abuse Policies

Section 4 - Provisions in Registry Agreements relating to abuse

Pages 11 - 29

http://gnso.icann.org/files/gnso/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf

Registry Registrar Agreement (RRA) Dispersion:

Refer to the GNSO Issues Report on Registration Abuse Policies

Section 4 - Provisions in Registry Agreements relating to abuse

Pages 11 - 29

http://gnso.icann.org/files/gnso/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf

RRA Templates are contained within the RA and hence the analysis is combined with appendix 1.

Registrar Accreditation Agreement (RAA) Dispersion:

Because the RAA is template driven, a quick inventory of Registration Abuse Types (as defined by the RAPWG) was conducted within the RAA template instead of a formal dispersion study. Two RAAs exist. A version from May 2001 existed until the most recent May 2009 version was released. With over 80+% adoption rates by Registrars to the May 2009 version, it was the only RAA reviewed for dispersion.

http://www.icann.org/en/registrars/agreements.html

The May 2009 RAA does contain provisions that align with abuse types defined by the Working Group. These include WhoIS, UDRP, and Privacy language. However, the latest RAA does not contain any language relative to take-down, conduct & use, abuse definitions, and indemnification to protect parties from taking action against abuse.

In parallel to the RAPWG, a Working Group to enhance the RAA is underway. It is the UoC's intent to share any recommendations that appear to align with RAA WG actions. Based on the latest presentations from ICANN Seoul, WG members have already identified gaps around Malicious Conduct, Cybersquating, Privacy/Proxy Services, and complete information disclosure with Affiliates & Resellers.

Registration Agreement (ra) Dispersion:

Refer to the GNSO Issues Report on Registration Abuse Policies
Section 5 - Provisions in Registration Agreements relating to abuse
Pages 30 - 37
http://gnso.icann.org/files/gnso/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf

Registration Agreement (ra) Dispersion Study

An evaluation of publicly available online agreements (Domain Registration Agreement, Universal Terms of Service, etc..), from a representative sample of registrars was performed to determine the degree of variation among agreement provisions relative to abuse. This evaluation, essentially, is an inventory of sections within the registration agreement. It attempts to quantify "current state" for the purpose of providing a visual representation of dispersion.

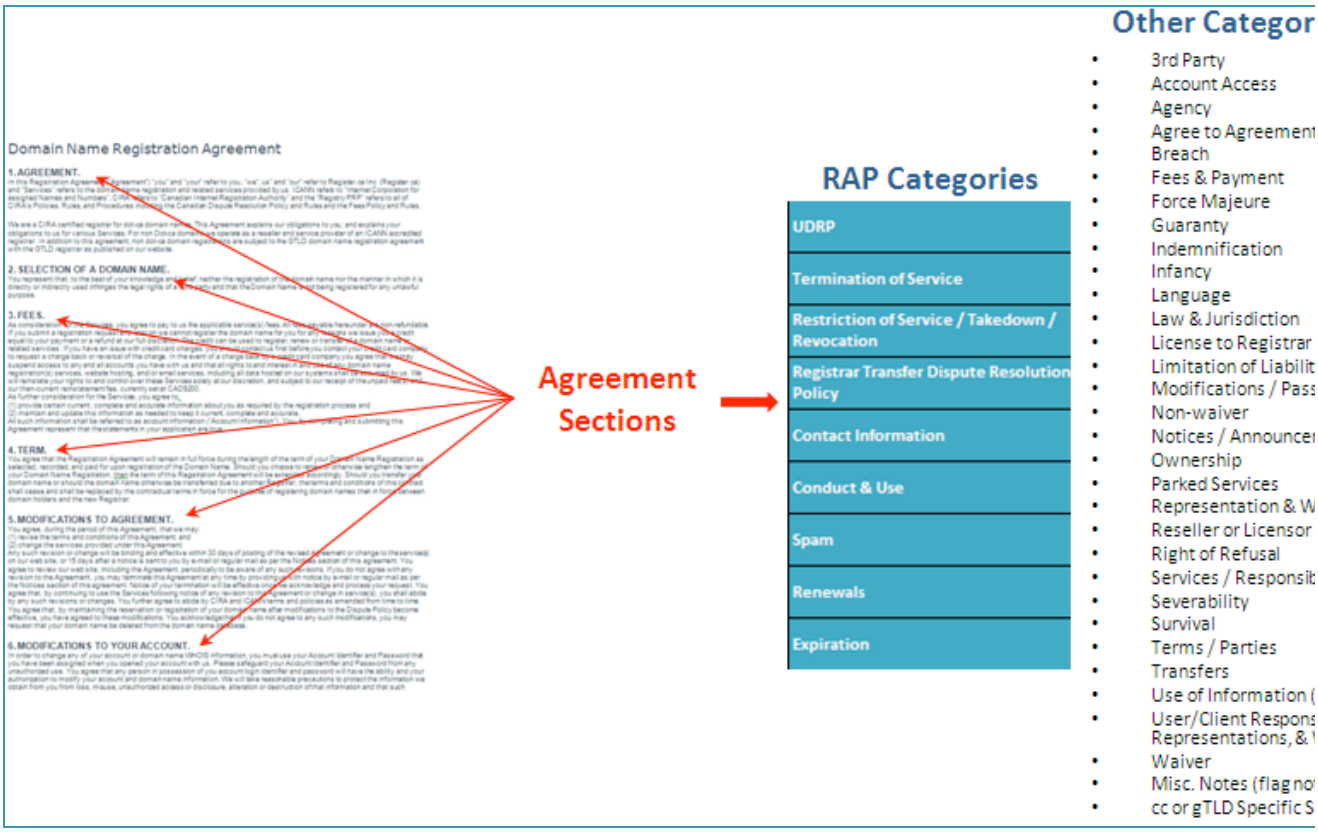
By review of the various registration agreements, sections began to naturally form in to forty or so categories in which the registration agreements could be inventoried. For each of the 22 Registrars, from the representative pool, an Excel spreadsheet was used to track the binary

existence of each agreement category. If a category was found, the spreadsheet would be incremented accordingly, and if the section was relevant to abuse, the corresponding agreement language was pasted in to the spreadsheet. If no section was found, the category requirement was not met, nor was it incremented.

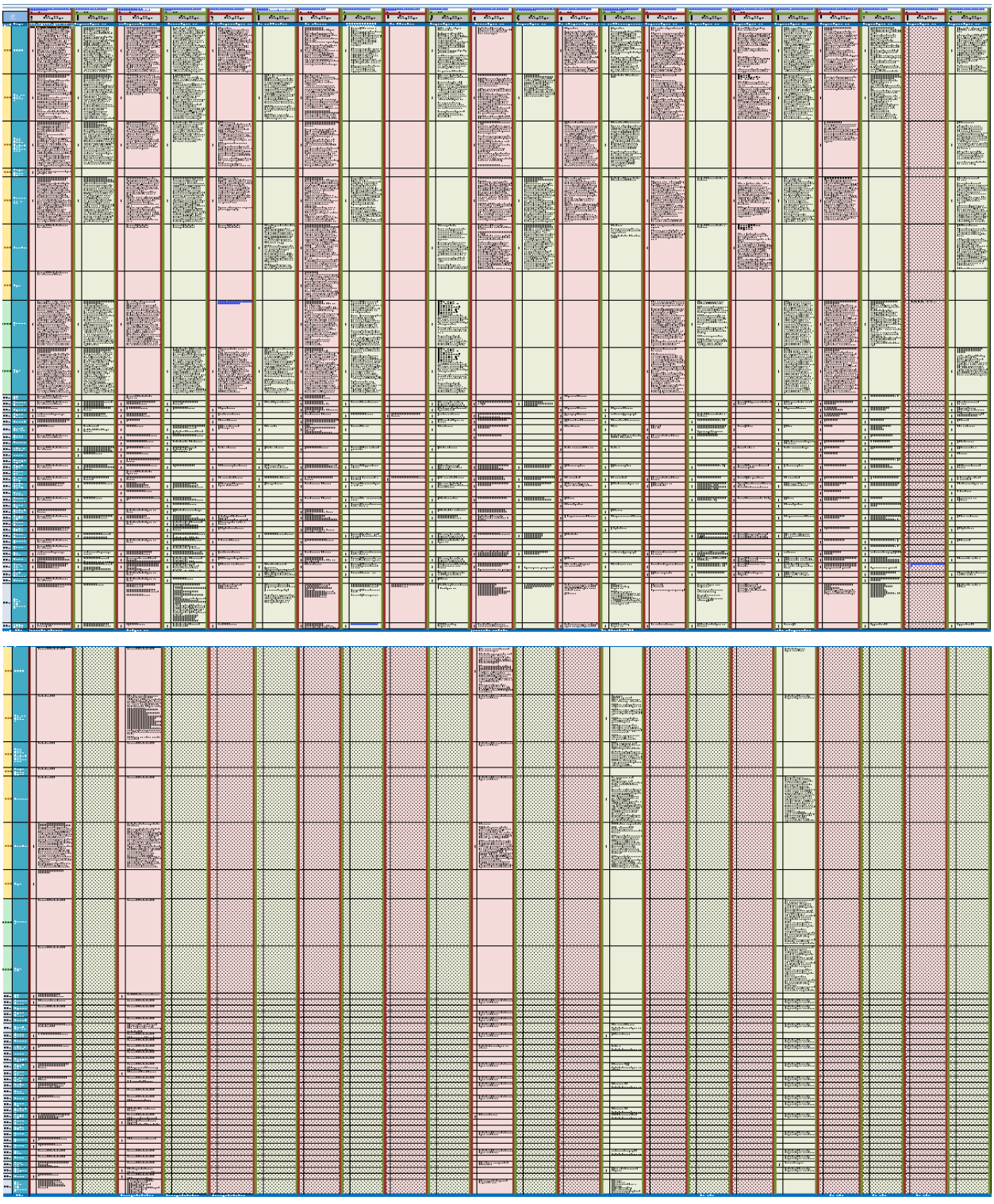
It should be noted, that this was not a compliance exercise, and as such, all results shared are anonymous. The representative sample of registrars is based on % market share of held registrations per webhosting.info as of June 2009. Within that sample, a general guiding principle for selection of the 22 registrars was the top, middle, and bottom market participants. This sample of 22 Registrars makes up approximately 59% of total market share. Additionally, the sample also attempts to gain representation across varying countries.

The actual spreadsheet and presentation reports can be found at the UoC Wiki Attachments section:
https://st.icann.org/reg-abuse-wg/index.cgi?uniformity_sub_team
RAPWG-UofC_Dispersion_Matrix_09152009.xls
RAPWG-UofC_Report_09152009.pdf

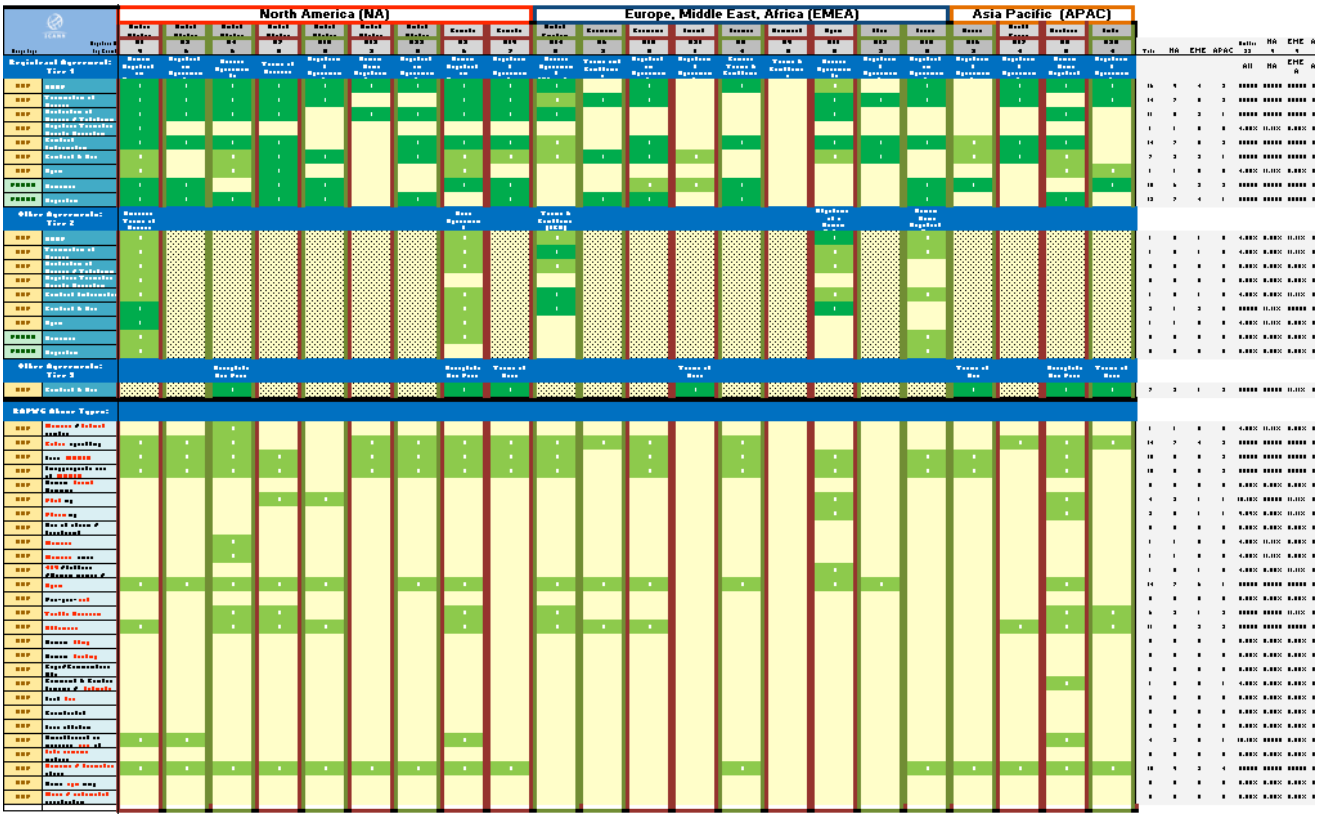
The diagram here shows a screen shot of a Registration Agreement (ra) on the left. Each red arrow points to a defined section within the agreement. On the right side of the diagram are the categories that formed from the inventory. Those labelled in the blue boxes pertain to the abuse types within scope of the RAPWG.



This screen shot represents the entire spreadsheet used to inventory Registration Agreement sections across the 22 Registrars. The zoom here is at 10%. This screen shot also includes those categories not relevant to abuse, and as such will not show pasted language from the agreement:



This screen shot represents a summary view of the previous spreadsheet. The legend is listed below, but basically the variance between the green and yellow coloring depicts the dispersion found within agreements relative to abuse. The gray section to the right provides "hit rate" percentages of agreement sections by region and overall. Please refer the UoC Wiki for the actual reports to zoom in and gain a clearer understanding.



Legend:

1 — Agreement met category requirement by formal section definition

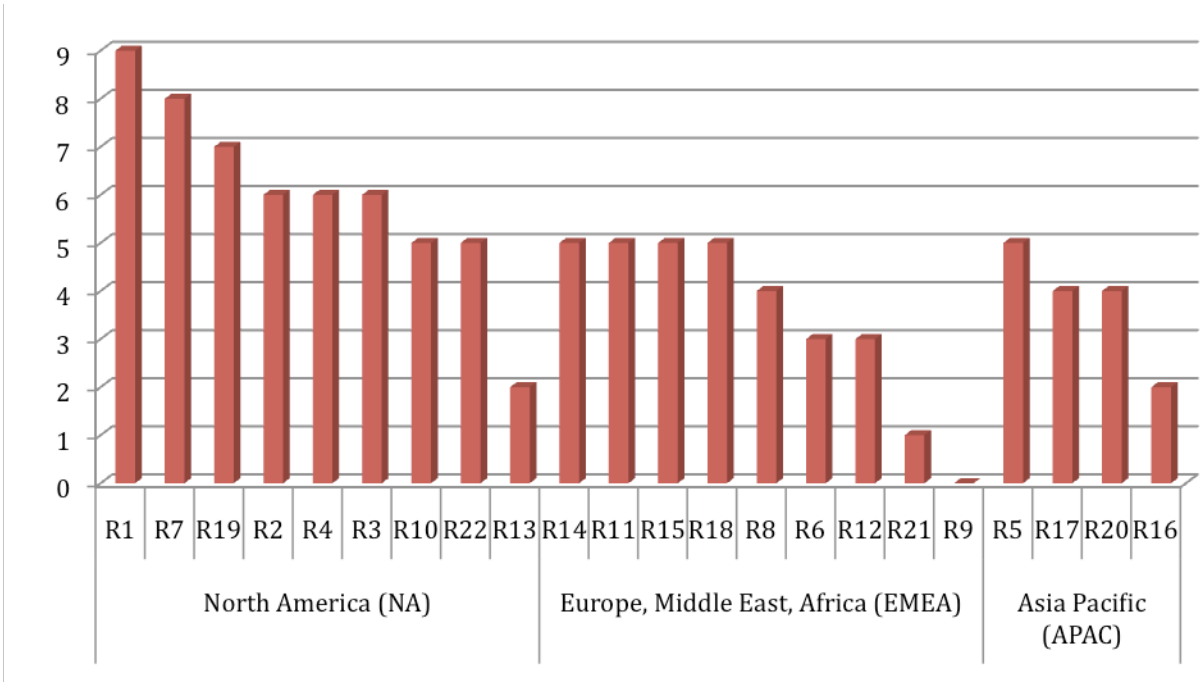
0 — Category requirement flagged via separate agreement

Formal section definition of category not found within agreement

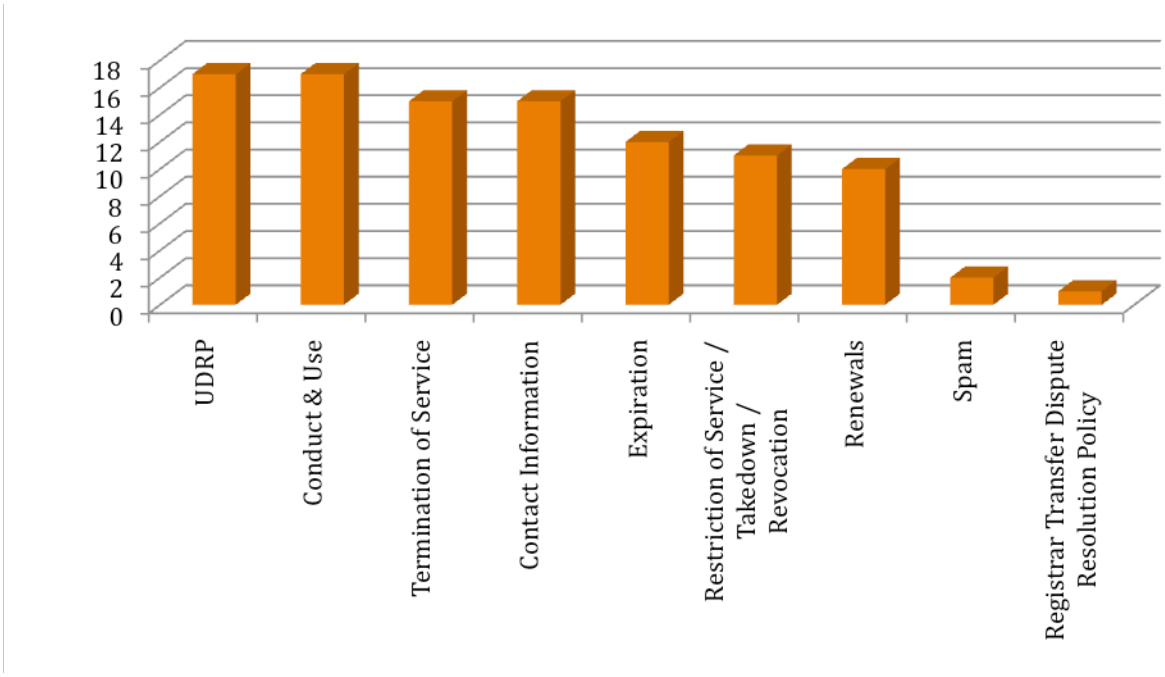
Tier 2 or 3 Agreement not found or not in scope

The chart below provides a different view at the dispersion across Registration Agreements. The Y Axis represents the number of categories where the agreement satisfied the formal section

definition requirements while the X Axis represents registrars by region, sorted highest to least (left to right).



This chart represents categories with the greatest achievement of section definition.



8.2.3 Dispersion & Consistency

The UoC sub-team believed that uniformity does not exist among "RA, RRA, RAA and ra" agreements relative to abuse provisions. The sub-team was of the belief that increased uniformity is important for the marketplace and helps promote equal competition, and that while perfect uniformity is not realistic, it should be striven for when and where feasible.

At the same time, the team also recognized that lack of uniformity complicates efforts to mitigate abusive uses of domains, but is not a predicate for abuse that we see today, and that if policies are consistent, then greater responsibility to enforce the policy consistently falls upon ICANN.

8.2.4 Registration Abuse Provision Baseline

- The sub-team agreed that if any sort of uniformity in agreements is to be implemented, a minimal baseline of provision or language would be the best method to accommodate the various business models.
- The sub-team thought that a lowest common denominator (minimum requirement) approach with abuse provisions is best and allows market participants to not be constrained by exceeding minimums in efforts to promote differentiation within the competitive landscape.
    - The sub-team recognized the spectrum of abuse provisions can range from:
        - General language with broad powers to act against all kinds of abuse, or
        - Specific language which can be limiting; and may not be adaptive to changing conditions
    - Finding the right balance of language that provides adequate authority to respond to abuse with adequate protection from lawsuits is required.

- A "One size fits all" kind of provision that can anticipate future or unknown abuses was the sub-team's desire, but equally recognize the existence of varying models prevent this notion.

- The sub-team thought that any provision baseline should be clearly communicated and shared with market participants and that high degrees of transparency is required where participants choose to exceed any baselines or minimums that are established.
- The sub-team agreed that outcomes from any future and not-yet-determined registration abuse policies PDP will be long coming and that in the meantime it would be a useful thing for ICANN, Registries, and Registrars to develop abuse provisions and/or continue to enhance abuse provisions for their agreements with continued voluntary, proactive enforcement as necessary. Additionally, the sub-team agreed that the investigation and deployment of best practices would be a great interim step until such a PDP is complete.

8.2.5 Sub-Team Conclusions & Guiding Principles

Over the course of UoC sub-team meetings and research findings, reoccurring themes developed with consistent agreement leading to sub-team consensus and defined boundaries for recommendations that the sub-team created.

8.2.6 RAPWG Discussion of Sub-Team Work

The members of the sub-team reported their results to the whole RAPWG team for review. When the wider RAPWG discussed the sub-team's analysis, there was not agreement about the sub-team's findings and recommendations.

Some RAPWG members believed that uniformity already exists in the important and relevant ways. Observations included:

- Registries, registrars, and registrants are required to follow Consensus Policies. So, if there is a registration abuse, ICANN can make consensus policy about that abuse, and

the resulting policy will be applied to all contracted parties. The Consensus Policy process is a mechanism specifically designed to create uniformity where it is needed, and it guarantees uniformity.

- All registrars are bound to a uniform RAA. While two version of the RAA currently exist, the great majority of the registered gTLD domains are now covered under the new (2009) RAA, and the old RAA (2001) is being phased out in a planned fashion.
- Language in the RAA requires registrars and registrants to adhere to all ICANN policies.
- Some amount of non-uniformity is necessary. For example, sTLDs may require language in their contracts to define their unique sponsorship and eligibility needs.
- Uniformity for the sake of uniformity does not necessarily solve any problem.

The sub-team advocated the exploration of "general language with broad powers to act against all kinds of abuse," and provisions "that can anticipate future or unknown abuses." Some RAPWG members expressed concern that these ideas might not be desirable or realistic. They might be a solution in search of an undefined problem, and might not include adequate consideration of who is being harmed, how, and to what extent. The RAPWG did agree in its definitional work that "The party or parties harmed, and the substance or severity of the abuse, should be identified and discussed in relation to a specific proposed abuse." Members expressed that it is difficult to anticipate future or unknown abuses, and raised the issue that general and/or pre-emptive policies may create collateral damage and harm registrants or other parties in unexpected fashions. In general, the RAPWG discussed how in the past consensus policy-making efforts, specific registration abuses were verified and understood, and then specific policies and procedures were designed to address them.

Some members were of the opinion that the sub-team did not always distinguish adequately in its contracts analysis between registration abuse provisions and provisions designed to address malicious uses of domains. This distinction can be critical for policy-making.

Regarding uniformity of registrar-registrant agreements and TLD-specific terms of service: Registrars do have the right to set their terms of service as long as they are consistent with

ICANN requirements. Similarly, many registries have the contractual right to institute policies and procedures for their own TLDs, and it was unclear to some RAPWG members whether ABPs would alter those existing contractual rights. As per the exploration of malicious use above, ICANN does not appear to have the ability to force registrars and registries to implement domain suspensions for malicious use alone.

There was some disagreement with the sub-team's statement that "uniformity is important for the marketplace and helps promote equal competition;" RAPWG members commented that contractual variances in registrar-registrant agreements are a way that registrars differentiate themselves in the market, and can help registrars adhere to the laws of the jurisdictions in which they are incorporated or operate.

8.3 Recommendations

There was strong support for but significant opposition for the following recommendation. *The two opposing views are below, and the RAPWG will further consider these views after receiving public comment:*

Eight (8) members supported this recommendation:

The RAPWG recommends the creation of an Issues Report to evaluate whether a minimum baseline of registration abuse provisions should be created for all in-scope ICANN agreements, and if created, how such language would be structured to address the most common forms of registration abuse.

The members who support the recommendation stared the following reasons: "The analysis conducted by the ICANN staff Issue Report and this Working Group concludes that significant variance (or "lack of uniformity") within contracts does exist, especially with respect to abuse definitions, abuse types, and indemnification to mitigate abuse. Existing agreement provisions, in varying forms, do generally cover suspension of domain names or indemnify select parties, but they do NOT specifically address abuse as defined by this working group. By such regards, this is partly the very condition in which the Registration Abuse pre-PDP was formed.

The recommendation does not reduce or remove the rights of market participants to create and manage their own policies, nor does it reduce any competitive advantages that may exist today. Rather, the establishment of minimum Registration Abuse baselines, if any are determined by such a PDP, will begin to introduce predictability in a rather chaotic world. More importantly, minimum standards will enable market participants to better mitigate or eliminate registration abuse in a more coordinated and unified manner by raising the bar in a method where ALL equally participate in the mitigation or elimination of abuse."

In favour (8): Cobb (CBUC), Felman (IPC), , O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC).

Five (5) members opposed the recommendation for an Issues Report, *for the following reasons:*

- *All registries, registrars, and registrants are already contractually obligated to abide by ICANN policies, notably existing or new Consensus Policies.*
- *In those cases where ICANN has defined a registration abuse policy, the abuse definitions and the policies have been clearly and consistently expressed.*
- *The Consensus Policy process is a mechanism specifically designed to create uniformity where it is needed. If there is a registration abuse that needs to be addressed, it should be specifically identified, and a specific Consensus Policy crafted to deal with it.*
- *Consensus Policies or contractual provisions should be created only after the abuse's scope and impact are understood. The proponents of the PDP advocate for general and/or pre-emptive policies, and those can create collateral damage and harm registrants and other parties in unexpected fashions.*
- *Uniformity for the sake of uniformity is NOT a solution to any identified problem. The supporters of an Issues Report did not identify why "a minimum baseline of registration abuse provisions" is needed, or whether such might better curtail or address any problem, as the RAPWG's Charter required. It is unclear what purpose might be served by continuing down that proposed path.*

- *It may not be desirable or possible to create a baseline applicable to diverse entities. Some amount of non-uniformity is necessary.*
- *The recommendation could reduce or remove the rights of market participants to create and manage their own policies. Contracted parties already have, and should continue to have, some rights to create their own policies as long as they do not conflict with ICANN policies.*
- *It seems that the proposed PDP could explore not only the creation of registration abuse policies, but also policies to regulate how registrars and registries address the malicious use of domains names. That would be overbroad and inappropriate, as the use of domain names unrelated to registration issues is out of ICANN and GSNO scope for reasons detailed in depth elsewhere in this paper.*

In opposition (5): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Newman (RySG), Young (RySG).

9. Meta-Issues

The RAPWG identified registration abuse "meta-issues." These meta-issues have a number of attributes in common:

- They are being discussed in various Working Groups and Advisory Groups simultaneously.
- Their scope spans a number of ICANN policies
- Previous groups have discussed these issues without satisfactory resolution
- They are worthy of substantive discussion and action, but may not lend themselves to resolution through current policy processes

9.1 Meta-issue : Uniformity of Reporting

This working group has identified the need for more uniformity in the mechanisms to initiate, track, and analyze policy-violation reports. The IRTP Working Group identified a similar need during its review of compliance reports in that arena. This issue is much broader than registration abuse, is being discussed by a number of working and advisory groups simultaneously, and will require more than simple uniformity of contracts to address.

9.1.1 The Problem

The processes by which a person experiencing a problem learns about their options to resolve that problem, or learns which remedies are covered by ICANN policy and which are not, is sometimes difficult. As a result:

- End-users and registrants find it confusing and difficult to identify the most appropriate problem-reporting venue or action to take when they experience problems.

- Registrars and registries are frustrated if their customers file complaints in error, in the wrong place, or without first seeking help from the most relevant provider.
- Working and advisory groups find their work hampered by the lack of reliable (rather than anecdotal) data upon which to base policy decisions.

In addition, the process of reporting a perceived policy violation could be used to educate people on the limits of ICANN policies and available options if their issue is not covered by policy.

The RAPWG suggests, as a starting point for discussion, that every abuse policy should have:

- **Reporting**: a mechanism whereby violations of the policy can be reported by those who are impacted
- **Notification:** standards as to how contracted parties make visible:
    - where to report policy violations,
    - "plain language" definitions of what constitutes a "reportable" problem,
    - "just in time education" describing reporting or action options that are available when the person's problem falls outside ICANN policy.
- **Tracking**: transparent processes to collect, analyze, and publish summaries of valid policy-violation reports, the root-causes of the problems and their final disposition
- **Compliance:** processes to provide due process, and sanctions that will be applied, in the case of policy violations.

If the GNSO creates a subsequent effort to address this issue, it might consider the following tentative list of goals:

- Providing "just in time" education and knowledge to people wanting to report problems
- Making it easier to submit a valid complaint
- Reduce the number of erroneous complaints
- Improving understanding of the limits of ICANN policies and other options to pursue if the issue is not covered by policy

- Improving the effectiveness of policy-compliance activities
- Improving the data available for GNSO (working-group) and ICANN (advisory-group) policy-making
- Improving the data available for compliance activities
- Answering the question "which comes first, policy-process or definitive data describing the problem?" along with suggestions as to how data can be gathered when it hasn't yet been included in the reporting process.

9.1.2 Recommendation

The RAPWG recommends that the GNSO, and the larger ICANN community in general, create and support uniform reporting processes.

The WG achieved unanimous consensus on the above recommendation. *In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.*

9.2 Meta-issue: Collection and Dissemination of Best Practices

The RAPWG has identified the need for and benefit of creating and disseminating "best practices" related to aspects of domain name registration and management, for the appropriate members of the ICANN community. Best practices should also be kept current and relevant. The question is how ICANN can support such efforts in a structured way.

This recommendation is a "meta-issue" because it is much broader than registration abuse, is being discussed by a number of working and advisory groups simultaneously, and has potential impact for almost any current and future working or advisory group.

9.2.1 Definition of "Best Practices"

From Wikipedia (http://en.wikipedia.org/wiki/Best_practices):

> *A best practice is a technique, method, process, activity, incentive, or reward that is believed to be more effective at delivering a particular outcome than any other technique, method, process, etc. when applied to a particular condition or circumstance. The idea is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. Best practices can also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people.*
>
> *A given best practice is only applicable to particular condition or circumstance and may have to be modified or adapted for similar circumstances. In addition, a "best" practice can evolve to become better as improvements are discovered.*

The members of the RAPWG discussed that "best practices" should be considered non-binding by definition, and should therefore not have an implication of finality, obedience, or universality. This distinguishes them from binding requirements such as Consensus Policies and contractual obligations, which are considered final and require compliance, and are created via other processes at ICANN. Best practices may often be a good alternative when binding requirements are not applicable or appropriate. (In a parallel example, IETF Best Practices or "best current practice RFCs" are recommendations only, and the IETF chose not to make them Internet Standards for a reason.) Best practices are also flexible, can be updated as needed, and can be adopted and adapted by various users according to their varying needs. As has been noted in this paper, that is helpful because industry parties often face very different problems, to different degrees, etc.

9.2.2 Background

A number of working and advisory groups are coming up with many good ideas for addressing a wide variety of problems in the industry. The group's participants often label these ideas as "best practices". However, many of these ideas do not lend themselves well to crafting as policy, for policies are often narrow in scope, limited in the time they could be effective, or difficult to capture as policy concepts or contract terms. This is particularly true in the areas surrounding malicious use. Yet all industry participants could benefit greatly by adopting many of these best practices. Unfortunately, no formal mechanisms for collecting such practices, keeping them updated, or disseminating them to all relevant industry participants exists today within the ICANN community. Thus, much of the good work done in these groups is not captured effectively if it is not included in their policy-making outcomes.

Best practices in the field of anti-abuse or security often lose their effectiveness in a relatively short amount of time. This does not lend well to formal policy, but sharing effective techniques with peers in the field can still be very beneficial.

Best practices in the field of anti-abuse or security are often very sensitive, and industry participants would not always like some of them made public so that bad actors can learn from them and adapt new tactics. How can sensitive best practices be safely disseminated to industry participants? How can the veracity of all industry participants be assured as well?

If the GNSO creates a subsequent effort to address this issue, it might consider the following tentative list of goals:

- Creating mechanisms within the ICANN community to support the creation and maintenance of best practices efforts in a structured way.
- Creating multiple channels (some private or secure) for dissemination of best practices to all relevant community members.
- Incorporating the gathering and recommendation of best practices into the processes used by various policy and advisory working groups.

- Instituting practices to measure and incentivize adoption of best practices across the industry.
- Launching regular review processes where universal best practices might be incorporated into more formal policies, when appropriate.

9.2.3 Recommendation

The RAPWG recommends that the GNSO, and the larger ICANN community in general, create and support structured, funded mechanisms for the collection and maintenance of best practices.

The WG achieved unanimous consensus on the above recommendation. *In favour (13): Aaron (RySG), Amadoz (RySG), Bladel (RrSG), Cobb (CBUC), Felman (IPC), Newman (RySG), O'Connor (CBUC), Queern (CBUC), Rasmussen (Individual), Rodenbaugh (CBUC), Shah (IPC), Sutton (CBUC), Young (RySG). Against, or alternate views: none.*

10. Conclusions, Recommendations, & Next Steps

The RAPWG aims to complete this section of the report in the second phase of the WG process, following the review and analysis of the comments received during the public comment period.

Annex I – Working Group Charter

Whereas GNSO Council Resolution (20081218-3) dated December 18, 2008 called for the creation of a drafting team "to create a proposed charter for a working group to investigate the open issues documented in the issues report on Registrations[sic] Abuse Policy".

Whereas a drafting team has formed and its members have discussed and reviewed the open issues documented in the issues report.

Whereas it is the view of the drafting Team that the objective of the Working Group should be to gather facts, define terms, provide the appropriate focus and definition of the policy issue(s), if any, to be addressed, in order to enable the GNSO Council to make an informed decision as to whether to launch PDP on registration abuse.
Whereas the drafting team recommends that the GNSO Council charter a Working Group to (i) further define and research the issues outlined in the Registration Abuse Policies Issues Report; and (ii) take the steps outlined below. The Working Group should complete its work before a decision is taken by the GNSO Council on whether to launch a PDP.

The GNSO Council RESOLVES: To form a Working Group of interested stakeholders and Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, to further define and research the issues outlined in the Registration Abuse Policies Issues Report; and take the steps outlined in the Charter. The Working Group should address the issues outlined in the Charter and report back to the GNSO Council within 90 days following the end of the ICANN meeting in Mexico City.

CHARTER

Scope and definition of registration abuse – the Working Group should define domain name

registration abuse, as distinct from abuse arising solely from use of a domain name while it is registered. The Working Group should also identify which aspects of the subject of registration abuse are within ICANN's mission to address and which are within the set of topics on which ICANN may establish policies that are binding on gTLD registry operators and ICANN-accredited registrars. This task should include an illustrative categorization of known abuses.

Additional research and identifying concrete policy issues – The issues report outlines a number of areas where additional research would be needed in order to understand what problems may exist in relation to registration abuse and their scope, and to fully appreciate the current practices of contracted parties, including research to:

- 'Understand if registration abuses are occurring that might be curtailed or better addressed if consistent registration abuse policies were established'
- 'Determine if and how [registration] abuse is dealt with in those registries [and registrars] that do not have any specific [policies] in place'
- 'Identify how these registration abuse provisions are [...] implemented in practice or deemed effective in addressing registration abuse'.

In addition, additional research should be conducted to include the practices of relevant entities other than the contracted parties, such as abusers, registrants, law enforcement, service providers, and so on.

The Working Group should determine how this research can be conducted in a timely and efficient manner -- by the Working Group itself via a Request for Information (RFI), by obtaining expert advice, and/or by exploring other options.

Based on the additional research and information, the Working Group should identify and recommend specific policy issues and processes for further consideration by the GNSO Council.

SSAC Participation and Collaboration: The Working Group should (i) consider inviting a representative from the Security and Stability Advisory Committee (SSAC) to participate in the

Working Group; (ii) consider in further detail the SSAC's invitation to the GNSO Council to participate in a collaborative effort on abuse contacts; and (iii) make a recommendation to the Council about this invitation.

Workshop at ICANN meeting in Mexico City on Registration Abuse Policies - In order to get broad input on and understanding of the specific nature of concerns from community stakeholders, the drafting team proposes to organize a workshop on registration abuse policies in conjunction with the ICANN meeting in Mexico City. The Working Group should review and take into account the discussions and recommendations, if any, from this workshop in its deliberations.

The working group established by this motion will work according to the process defined in Working Group Processes.

Annex II - The Working Group

Following the adoption of the charter by the GNSO Council, a call for volunteers was launched. The following individuals are part of the RAP WG; all have submitted Statements of Interest (see https://st.icann.org/reg-abuse-wg/index.cgi?statements_of_interest):

Name	Affiliation[49]
Greg Aaron (Chair)	RySG
Mike Rodenbaugh (Council Liaison)	CBUC
James Bladel	RrSG
Olga Cavalli	NCA
Zahid Jamil	CBUC
Beau Brendler	ALAC
Jeff Neuman	RySG
Nacho Amadoz	RySG
Philip Corwin	CBUC
Martin Sutton	CBUC
Richard Tindal	RrSG
Greg Ogorek	CBUC
Faisal Shah	IPC
Roland Perry	Individual
Paul Stahura	RrSG
Jaime Echeverry Gomez	RrSG
Li Guanghao	Individual
Mike O'Connor	CBUC
Gretchen Olive	RrSG
Berry Cobb	CBUC
Jeff Eckhaus	RrSG
Robert Hutchinson	CBUC
Andy Steingruebl	Individual

[49] RySG = Registry Stakeholder Group, RrSG = Registrar Stakeholder Group, CBUC = Commercial and Business Users Constituency, NCA = Nominating Committee Appointee, ALAC = At Large Advisory Committee, IPC = Intellectual Property Constituency, SSAC = Security and Stability Advisory Committee, NCUC = Non-Commercial Users Constituency

Jeremy Hitchcock	SSAC
Patrick Kane	RySG
George Kirikos [resigned from the WG on [22 October 2009]	CBUC
Michael Young	RySG
Rod Rasmussen	Individual
Edward Nunes	NCUC
Frederick Felman	IPC
Evan Leibovitch [resigned from the WG on 21 January 2010	ALAC
Caleb Queern	CBUC
Avri Doria (as former GNSO Chair)	NCUC
Chuck Gomes (GNSO Chair)	RySG

For attendance sheet, see Annex III.

ANNEX III - RAP WG Attendance Sheet

Participants		9,01	16,01	30,01	18,02	16.03 DT to WG	30,03	13,04	27,04	11,05	1,06	15,06	6,07	20,07	3,08	17,08	31,08	14,09	28,09	12,10	9,11	23,11	30,11	7,12	14,12	21,12	4,01	11,01	18,01	25.01.10	01.02.10	8,02	Total Calls Attended
Beau Brendler	ALAC					0			1					1																				***2***
Evan Leibovitch	ALAC												1	0																				***1***
Roland Perry	Individual						1	1	1	1	1	1	1	0	1	1		0	1	1	1													***12***
Rod Rasmussen	Individual							1	0	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	***23***
Greg Ogorek	Individual					1		1	1	1			1						1		1						1						***8***
Andy Steingruebl	Individual						1				1			1																			***3***
Guanghaoi Li	Individual						0	0	0	1																							***1***
Olga Cavalli	NCA		1	0	0	0	0																										***1***
Sub-Total…	**Others**	**0**	**1**	**0**	**0**	**1**	**2**	**3**	**3**	**4**	**2**	**2**	**4**	**3**	**2**	**2**	**1**	**1**	**3**	**2**	**3**	**1**	**1**	**1**	**1**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**51**
Caleb Queern	CBUC															1					1				1								***3***
Mike Rodenbaugh	CBUC	1	1	0	1	1	1	1	1	1	1		1	1	1																		***12***
Berry Cobb	CBUC						1	1	1		1	1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1	1	1	1	1	***24***
George Kirikos	CBUC						1	1	1	0	1	1	1	1	1	1	1	1	1	1													***13***
Mike O'Connor	CBUC					1	0	1	1	1		1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	***23***
Martin Sutton	CBUC					1	1		1	0	1	1	1	1		1		1	1	1	1			1	1	1	1	0	1	0	1	1	***19***

Philip Corwin	CBUC					1	1	1	1	0	1	0	1	1			1	1	0	1					1	1	0	1					***13***
Robert Hutchinson	CBUC									1			1				1	1	1	1		1		1	1		1	1		1			***12***
Zahid Jamil	CBUC			0	1																												***1***
Sub-Total…	**Business**	**1**	**1**	**0**	**2**	**4**	**5**	**5**	**6**	**3**	**5**	**4**	**7**	**6**	**4**	**5**	**5**	**6**	**5**	**4**	**3**	**3**	**2**	**4**	**6**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**120**
Faisal Shah	IPC					1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	***25***
Gretchen Olive	IPC					1	1		1	0	1			1																			***5***
Kristina Rosette	IPC	1		1	0	1																											***3***
Frederic Felman	IPC											1	1	1	0				0		0									1	1	1	***6***
Sub-Total…	**IPC**	**1**	**0**	**1**	**0**	**3**	**2**	**1**	**2**	**1**	**2**	**2**	**2**	**3**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**2**	**2**	**2**	**39**
	ISPC																																***0***
	NCUC																																***0***
James Bladel	Registrar	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	***30***
Richard Tindal	Registrar					1	1	1	1		1		1				1	1															***8***
Jeremy Hitchcock	Registrar						1	0	0		1			1																			***3***
Sub-Total…	**Registrars**	**1**	**0**	**1**	**1**	**2**	**3**	**2**	**2**	**1**	**3**	**1**	**2**	**2**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**41**
		1																															
Greg Aaron	Registries	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	***31***
Nacho Amadoz	Registries					1	0		1	1	1	1	1	0																			***6***
Jeff Neuman	Registries						1						1		1	0	1	1	0														***5***
Michael Young	Registries						1				1		1						1												1	1	***4***

Patrick Kane	Registries						1																									***1***
Sub-Total…	**Registries**	**1**	**1**	**1**	**1**	**2**	**4**	**1**	**2**	**2**	**3**	**2**	**4**	**1**	**2**	**1**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**47**
Total Participants		**4**	**3**	**3**	**4**	**12**	**16**	**12**	**15**	**11**	**15**	**11**	**19**	**15**	**10**	**10**	**11**	**12**	**12**	**9**	**8**	**7**	**6**	**8**	**10**	**8**	**8**	**8**	**7**	**8**	**9**	**9**	**298**
TOTAL RAP Calls		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	***31***
Geof Bickers	Staff						1	1																								***2***
Liz Gasster	Staff	1	1	0	0						1				0																	***3***
William McKelligott	Staff																								1							***1***
Margie Milam	Staff			1		1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	***26***
Marika Konings	Staff	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	***27***
Glen de Saint Gery	Staff	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	1	0	1	1	1	***25***
Sub-Total…	**Staff**	**2**	**3**	**3**	**2**	**3**	**4**	**3**	**3**	**2**	**4**	**2**	**3**	**3**	**2**	**3**	**3**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**4**	**1**	**2**	**3**	**1**	**3**	**3**	**3**	**84**
BLANK = absent, no apologies, no attendance																																
1 = attendance																																
0 = absent apologies																																
Resignations and No Attendance (Data Excluded																																
Edward Nunes	NCUC																															***0***
Jon Nevett	Registrar						0																									***0***

Paul Stahura	Registrar								0																					***0***