Registration Abuse Policies Working Group

Initial Report

Submitted [TBC]

[ROUGH DRAFT: IN PROCESS. Version: 27 January 2010]

Marika Konings 14/1/10 10:19
Deleted: 11

- 20/1/10 09:01
Deleted: 14

Marika.Konings 27/1/10 10:33
Deleted: 6

- 20/1/10 09:01
Deleted: 14

Marika.Konings 27/1/10 10:33
Deleted: 20

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

2. Executive Summary

- TBC

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 to specifically deep dive on abuse types and other RAP topics. Such sub-teams were: Cybersquatting, Uniformity of Contracts, Front-Running,

Marika Konings 14/1/10 10:29
Deleted: PDP

- 19/1/10 13:38
Deleted: (see chapter (TBC) for further details).

- 20/1/10 11:50
Deleted: '

- 20/1/10 11:50
Deleted:

- 19/1/10 13:44
Deleted: is

- 19/1/10 13:44
Deleted: '

- 19/1/10 13:44
Deleted: '

- 19/1/10 13:44
Deleted: '

- 19/1/10 13:44
Deleted: '

- 19/1/10 13:44
Deleted: '

- 19/1/10 13:44
Deleted: '.

Mike O'Connor 22/1/10 10:48
Deleted: ,

Mike O'Connor 22/1/10 10:48
Deleted: have been discussed

- 19/1/10 13:44
Deleted: , which were categorized in pre-registration abuse, registration abuse, post-registration abuse, domain name use abuse and tools that have the ability to facilitate abuse, but also have legitimate purposes.

- 19/1/10 13:44
Deleted: has

- 19/1/10 13:45
Deleted: were actually

- 20/1/10 11:50
Deleted: whether

- 19/1/10 13:43
Deleted: they seemed

Mike O'Connor 22/1/10 10:49
Deleted: some

etc. The Uniformity of Contracts sub-team was formed in order to research whether registration abuses are occurring that might be curtailed or better addressed if consistent policies / contract language were established, The findings and recommendations that resulted from this effort can be found in the "uniformity of Contracts" chapter.

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.

Marika.Konings 27/1/10 11:33
Deleted: A

Mike O'Connor 22/1/10 10:52
Deleted: I

- 19/1/10 13:46
Deleted: address the questions in the charter related to further

- 19/1/10 13:46
Deleted: such as

Mike O'Connor 22/1/10 10:51
Deleted: registration abuse

Mike O'Connor 22/1/10 10:51
Deleted: policies

Mike O'Connor 22/1/10 10:52
Deleted: a Uniformity of Contracts sub-team was formed

- 19/1/10 13:45
Deleted: in chapter [TBC].

- 19/1/10 13:46
Deleted: C

Mike O'Connor 22/1/10 10:53
Deleted: Following the closing of the public comment period

- 19/1/10 13:46
Deleted: decide how the report will need to be updated

Mike O'Connor 22/1/10 10:54
Deleted: then

4. Discussion of Charter and Scope Questions

4.1 Abuse definition

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

- 19/1/10 10:59
Deleted: has

- 19/1/10 10:59
Deleted: has

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.

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.

* 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] .

- 25/1/10 13:16
Deleted:

- 25/1/10 13:16
Deleted: s

- 19/1/10 11:02
Deleted: <#>This is a working definition as per group consensus on April 27, 2009 and will be re-visited should the WG find it inadequate after examining some specific examples.

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

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

- 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.

- 19/1/10 13:47
Deleted: redistribution

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.
- 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.

- 20/1/10 11:52
Deleted: identified and

- 19/1/10 13:47
Deleted: notably

- 19/1/10 13:48
Deleted: of excessive

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-

- 19/1/10 13:49
Deleted: synonymous

- 19/1/10 13:49
Deleted: with the

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

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.

- 20/1/10 11:54
Deleted: solely

- 19/1/10 13:49
Deleted: runs

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.

- 19/1/10 13:50
Deleted: subdomains

- 19/1/10 13:50
Deleted: others

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 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

- 20/1/10 11:58
Deleted: Other potential outcomes of policy work are also possible, such as development of best practices, advice to ICANN on possible contract amendments, or development of codes of conduct.

- 20/1/10 12:13
Deleted: This

- 20/1/10 12:13
Deleted: approach

[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.

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:

- 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

- 19/1/10 15:13
Deleted: and

margie.milam 12/1/10 10:47
Deleted: regulate

- 19/1/10 10:05
Deleted: consensus

- 20/1/10 12:14
Deleted: that

- 20/1/10 12:09
Deleted: .

margie.milam 12/1/10 10:49
Deleted: regulating

- 19/1/10 10:06
Deleted: was

Marika.Konings 27/1/10 10:41
Formatted: Font:10 pt

Marika.Konings 27/1/10 10:41
Formatted: Font:Calibri

Marika.Konings 27/1/10 10:41
Formatted: Font:10 pt

Marika.Konings 27/1/10 10:41
Formatted: Font:Calibri

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

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

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]

- 19/1/10 13:52
Deleted: always do an adequate job of delineating

- 19/1/10 13:52
Deleted: and

- 19/1/10 13:52
Deleted: ing

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.

- 20/1/10 12:15
Deleted: if any

- 19/1/10 13:53
Deleted: a

- 19/1/10 15:14
Deleted: basic

[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.

- 19/1/10 10:06
Deleted: if

[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.

- 19/1/10 11:06
Deleted: p

Marika Konings 14/1/10 14:08
Deleted: fulfill

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]

Faisal Shah 24/1/10 12:25
Deleted: an

Faisal Shah 24/1/10 12:27
Deleted: c

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

Faisal Shah 24/1/10 12:28
Deleted: c

Faisal Shah 24/1/10 12:28
Deleted: c

[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.

Faisal Shah 24/1/10 12:28
Deleted: c

Faisal Shah 24/1/10 12:29
Deleted: c

Faisal Shah 24/1/10 12:29
Deleted: c

- 20/1/10 12:15
Deleted: is

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]

Faisal Shah 24/1/10 12:35
Deleted: The UDRP

Faisal Shah 24/1/10 12:32
Deleted:

Faisal Shah 24/1/10 12:35
Deleted: , and was also specifically designed to address cybersquatting and other cases in which the respondent may have no trademark claim or may be acting in bad faith.

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:

Faisal Shah 26/1/10 14:02
Deleted: T

Mike O'Connor 22/1/10 11:57
Deleted: story

- 19/1/10 13:55
Deleted: has acted as a

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

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

Faisal Shah 24/1/10 12:38
Deleted: F

Faisal Shah 24/1/10 12:38
Deleted: ping

Faisal Shah 24/1/10 12:39
Deleted: by complainants,

Faisal Shah 24/1/10 12:42
Deleted: may not be clear what ability, if any,

Marika.Konings 27/1/10 10:45
Formatted: Font:10 pt

Marika.Konings 27/1/10 10:45
Formatted: Font:Calibri

Marika.Konings 27/1/10 10:45
Formatted: Font:10 pt

Marika.Konings 27/1/10 10:45
Formatted: Font:Calibri

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.

[VERSION 19 Jan. by Martin Sutton:] The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Reportissues 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 withwhere the process.UDRP may be insufficient to curb cybersquatting
- Whether the definition of cybersquatting inherent within the existing UDRP language needs to be reviewed or updated. ;

View B:

Recommendation #2:

View A: The RAPWGRAP WG further 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 new gTLD program) can be applied to the problem of cybersquattingCybersquatting in the current gTLD space.

View B: The initiation of such a process is premature; the effectiveness and consequences of RPMs proposed for the new TLDs is unknown. Discussion of Rights Protection Mechanisms 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.

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

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

- 19/1/10 10:07
Deleted: <#>The RAP WG recognises that the UDRP is regarded a useful mechanism to counter some elements of cybersquatting, particularly where both parties can evidence prior rights and a judgement is required to resolve a complaint. However, the scale of cybersquatting is overwhelming and the drain on cost and resources for brand-owners to respond in all instances by using UDRP is prohibitive. Some of the key issues raised were:

Marika Konings 14/1/10 19:34
Deleted: If the UDRP requires revision to make it more effective as an anti-Cybersquatting mechanism, it should be revised as part of a subsequent PDP to update the policy.
Efforts at establishing Rights Protection Mechanisms elsewhere in the community (e.g., the New gTLD program) should be monitored for their applicability to the problem of Cybersquatting.
This issue, upon first inspection, seems to be relatively straightforward. It is only through discussion with diverse stakeholders do the complexities emerge. Therefore, we recommend that the RAPWG, and any subsequent PDP WGs, be wary of any proposed "silver bullet" solutions.

Unknown
Field Code Changed

Marika.Konings 27/1/10 10:47
Formatted: Font:10 pt

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

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:

- 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

- 26/1/10 10:16
Deleted: M

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

[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.

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.

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.

- 19/1/10 14:04
Deleted: is

- 26/1/10 10:16
Deleted: --

- 26/1/10 10:13
Deleted: <#>Better education of all parties involved in the domain name registration process (SAC 024 Recommendation #1, #2, #3, #4, #5).

Marika.Konings 27/1/10 10:49
Deleted: <#>More study

Marika.Konings 27/1/10 10:49
Deleted: <#>, with the goal of determining whether this abuse is actually occurring, or simply has the potential to occur.

- 26/1/10 10:13
Deleted: <#>Better disclosure by registry operators as to their privacy policy and how they use information, including availability checks and DNS traffic for unregistered domain names (extending point above which applied only to registrars).
<#>Requiring registry operators to produce and publish lists of all registered domain names with expiry dates, lists of post expiration domain names (with expected deletion date, etc.), and daily diffs, so that availability checks can be performed locally by registrars, registrants, and 3rd parties, thereby enabling greater privacy.
<#>Prohibiting registrars and/or registry operators from using/disclosing availability checks (including DNS traffic to unregistered domains), and/or creating "Chinese Walls" between different TLDs managed by a registry operator. Alternatively, creating rules as to how those availability checks can be used (e.g. instead of being able to use/sell real-time results, one might permit 1 hour old results to be sold, to permit novel idea creators sufficient time to complete registrations within an hour).

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

- 20/1/10 13:27
Deleted: Pornographic,

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:

- 19/1/10 11:15
Deleted: With respect to the registration of domain names regarding gripe and complaint,

- 19/1/10 11:15
Deleted: t

- 19/1/10 11:15
Deleted: However, there

- 19/1/10 11:15
Deleted: with respect to the fact

- 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 (Domain-name wars-Rise of the Cybersquatters) discusses the increase in Cbersquatting 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 AS filed a UDRP complaint with the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center, which ultimately ruled in its favor. That article can be found at: http://www.computerworld.com/s/article/print/9134605/Domain_name_wars_Rise_of_the_cybersquatters?taxonomyName=Networking+and+Internet&taxonomyId=16

- 19/1/10 14:08
Deleted: and dirty

- 19/1/10 14:08
Deleted: and dirty

- 19/1/10 11:17
Deleted: A recent article (part of which is set forth below) discussed this issue and the increase in cybersquatting abuse in general: "(Computerworld)

Faisal Shah 24/1/10 15:45
Deleted: For example, when the Web site FreeLegoPorn.com began publishing pornographic images created with Lego toys, trademark owner Lego Juris AS filed a UDRP complaint with the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center, which 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

Mike O'Connor 22/1/10 11:50
Deleted: regulate

- 19/1/10 15:15
Deleted: dirty

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.)

- 19/1/10 11:17
Deleted: tn

- 19/1/10 14:08
Deleted: ”

- 19/1/10 14:09
Deleted: .

- 19/1/10 11:17
Deleted: FTC

- 19/1/10 14:08
Deleted: dirty

- 19/1/10 14:09
Deleted: TV

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.

- 26/1/10 10:54
Deleted: expletive or dirty

- 19/1/10 14:10
Deleted: dirty words

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.

- 19/1/10 14:10
Deleted: mores

- 19/1/10 14:11
Deleted: and

- 19/1/10 14:11
Deleted: use

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.

Faisal Shah 24/1/10 19:02
Deleted: c

5.3.3 Recommendations

Recommendation 1:

- View A: The 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

- 19/1/10 11:19
Deleted: That gripe site and offensive site domain names should be addressed in the context of cybersquatting for purposes of establishing consistent registration abuse policies in this area, and

- 19/1/10 11:19
Deleted: however

of the registration of deceptive domain names that mislead adults or children to objectionable sites.

View B: Make no recommendation. There should not be a PDP to examine the UDRP for carve-outs or exceptions for "gripe" sites, or for fast track substantive and procedural mechanisms to address the registration of deceptive domain names that mislead adults or children to objectionable sites. Gripe site and offensive domain names are adequately addressed in the context of cybersquatting and the UDRP for purposes of establishing consistent registration abuse policies in this area. Creating special procedures for special classes of domains may present problems.

- Recommendation 2: Registries should also 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.

Faisal Shah 24/1/10 15:46
Deleted: , especially minors.

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

- 19/1/10 11:21
Deleted: <#>Cause illegitimate market-based switching between registrars (deceptive advertising)

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)

- 19/1/10 11:23
Formatted: Bullets and Numbering

- 19/1/10 11:23
Deleted: <#>Transfer issue (deceptive/fraudulent practices on the part of a registrar/reseller)?

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.

- 19/1/10 11:24
Formatted: Bullets and Numbering

- 19/1/10 11:24
Deleted: <#>If the perpetrator is a registrar or reseller, ICANN policy applies through the RAA

For a number of case studies, please see [complete with link to wiki].

5.4.3 Recommendations

- Refer to RAA working group (for additional enforcement tools)
- Refer to WHOIS working groups (to clarify the sanctions for unauthorized use)
- Refer to IRTP working group (for inclusion in the "urgent return" discussion)
- Refer to PEDNR working group (for inclusion in the hijacking/return topic)

Recommended -- Keep in proposed RAP PDP (reducing the risk of overlaps or gaps in the review/analysis)

Recommended – Refer to ICANN Contract Compliance for possible enforcement action.

Marika.Konings 27/1/10 11:18
Deleted:

- 19/1/10 11:24
Deleted: <#>Refer to RAA working group (for additional enforcement tools)?
Refer to WHOIS working groups (to clarify the sanctions for unauthorized use)?
Refer to IRTP working group (for inclusion in the "urgent return" discussion)?
Refer to PEDNR working group (for inclusion in the hijacking/return topic)?
Recommended -- Keep in proposed RAP PDP (reducing the risk of overlaps or gaps in the review/analysis)?
Recommended – Refer to ICANN Contract Compliance for possible enforcement action

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.

- 19/1/10 11:26
Deleted: permutations

- 26/1/10 11:49
Deleted: y

- 26/1/10 11:49
Deleted: query

5.5.2 Background

- The main concern Is that such tools may produce results that may infringe upon trademarked strings.

Faisal Shah 24/1/10 17:57
Deleted: seemed to be that

- There was agreement in the RAPWG that 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.

Faisal Shah 24/1/10 17:59
Deleted: Infringing d

- 19/1/10 11:26
Deleted: [Notes from conference call – further editing required]

- 19/1/10 11:27
Formatted: Highlight

- 19/1/10 11:27
Formatted: Highlight

- 19/1/10 11:26
Formatted: Not Highlight

- 19/1/10 11:26
Deleted: TBD

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.

- 19/1/10 11:27
Deleted: s

- 19/1/10 11:27
Deleted: ir

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

Faisal Shah 24/1/10 18:02
Deleted: c

Faisal Shah 24/1/10 18:02
Deleted: is covered

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 for continual registration, deletion, and re-registration of the same names in order to avoid paying the registration fees. This practice is sometimes 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. ICANN staff has received anecdotal reports that this type of activity is occurring, but does not currently have data to demonstrate definitively that domain kiting occurs or to what extent.

- 19/1/10 11:28
Deleted: also

The anecdotal reports received by the ICANN staff would indicate that:

a. Very few registrants engage in kiting;

b. Those registrars who facilitate kiting are discovered and warned by the registry to cease the behaviour;

c. Kiting practices cannot enable a registrant to “keep” a single domain name. Any name is available to be taken in the drop pool by another registrant. The activity is only practicable if attempting to maintain a number of names – some would be lost at each drop.

- 19/1/10 11:28
Deleted: 1.

- 19/1/10 11:28
Deleted: 2.

- 19/1/10 11:28
Deleted: 3.

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.

- 19/1/10 11:28
Deleted: [include link]

- 19/1/10 11:29
Deleted: PIR

- 19/1/10 11:29
Deleted: their

- 19/1/10 11:29
Deleted: 26th

Eventually, the current definition of domain kiting (the serial re-registration of a domain to get a domain for free) solidified, but it is not clear whether it was based on any actual activity or whether it was simply a matter of repurposing an already confused definition to cover a possible abuse scenario.

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. [21]

- 19/1/10 11:32
Deleted: A 2008 study by Affilias [need sources on this if we include it] using .info registry data supported this (negative) finding.

5.9.3 Recommendations

- Refine the definitions of tasting and kiting based on the discussion and defined boundary conditions above.
- Incorporate these definitions in any review or refinement of excess-delete policy and data collection or data reporting efforts.
- Alert ICANN staff to the possibility of kiting as a possible abuse of the add-grace period.
- Check with other working groups (e.g. domain tasting) to determine if follow-on studies have useful definitions and data.
- Conduct broader research (at the registry level) to determine to what extent domain kiting is a problem.

- 19/1/10 11:34
Deleted: <#>Possible clarifications

[21] http://forum.icann.org/lists/gnso-rap-dt/msg00425.html

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.

- 19/1/10 14:20
Deleted: these attacks

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.

- 19/1/10 14:21
Deleted: Web

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.

- 19/1/10 14:22
Deleted: specific

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

- 19/1/10 14:26
Deleted: While

- 19/1/10 14:27
Deleted: , t

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.

Faisal Shah 24/1/10 18:08
Deleted: o

- 19/1/10 11:43
Deleted: registries with such contractual provisions are already empowered to

[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 mightmay 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 defenses 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.

- 19/1/10 14:30
Deleted: be threatened with

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 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

- 19/1/10 14:30
Deleted: R

- 19/1/10 14:30
Deleted: often

[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.

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.

- 19/1/10 14:31
Deleted: an experienced

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 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.

[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

[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

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

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

- 19/1/10 10:09
Deleted: ***Examples to come.***

[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 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.

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.

- 19/1/10 14:32
Deleted: time

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.

- 19/1/10 14:33
Deleted: would need to

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.

[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.

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.

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

- 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.

- 19/1/10 10:32
Deleted: u

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

6.6 Examples of Malicious Uses

- 19/1/10 11:56
Deleted: <#>RECOMMENDATIONS

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

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.

- 19/1/10 11:56
Deleted: <#>Issue / Definition

RAPWG members Rod Rasmussen and Greg Aaron publish semi-annual Global Phishing Surveys via the Anti-Phishing Working Group.[35] 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 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.

[35] 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

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.

Mike O'Connor 22/1/10 11:51
Deleted: regulated

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.[36]

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.

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

Malware / Botnet Command-and-Control

- 19/1/10 14:36
Deleted: and

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.

- 19/1/10 11:59
Deleted: <#>Background

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.

- 19/1/10 14:37
Deleted: get created

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.

- 19/1/10 11:59
Deleted: What are the roles of members of the ICANN community and the wider domain registration community in partaking in such botnet disruption activities when it comes to preventing (or allowing) the use of specific domain names?

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

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

- 19/1/10 12:00
Deleted: <#>Recommendations

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.

- 19/1/10 14:57
Deleted: out there however

- 19/1/10 14:57
Deleted: approaches seemingly daily

- 19/1/10 14:38
Deleted: players

- 20/1/10 13:42
Deleted: *Models from other industries*

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 takes 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
    - Security resources of use or interest to registrars and registries

Addressing use of Stolen Access Credentials

- Idea – regular dissemination of best practices for protecting account access
- Idea – adoption of minimum standards for protecting registrant login credentials (password aging, strong passwords, etc.)
- Idea – codify registrant rights/responsibilities for account access security management – is there a potential for liability limitation for registrants vs. registrars vs. resellers?
- **Addressing use of Stolen Financial Credentials**
- [Placeholder for now]
- Idea – regular dissemination of best practices for detecting stolen financial credentials
- Idea – adoption of minimum standards for registrars/resellers who accept credit cards, alternative payments, and bank drafts/transfers. Look to PCI
- Idea – provide policy framework to ALLOW information sharing between registrars on fraudulent domain registrations and registration attempts.
- Idea – create information sharing clearinghouse to facilitate information sharing between registrars (and resellers) on fraudulent domain registrations and registration attempts. Data elements could include aspects of domain registrations including nameservers and contact details. Sharing of stolen credential information itself is highly problematic and would require a specialized third party if even possible. Locations of fraudulent registration attempts (IP addresses) may be feasible in some venues.

- 20/1/10 13:47
Deleted: **Addressing use of Stolen Identity Credentials** ... [1]

- 20/1/10 13:47
Deleted: <#>[Placeholder for now]

7. Whois Access

- 20/1/10 09:30
Deleted: Problems

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.[38]

- The Inter-Registrar Transfer Policy Part A PDP Working Group (IRTP-WG)[39] 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."[40]

[38] "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

[39] "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

[40] "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."[41]

7.2 Background

Marika.Konings 27/1/10 11:22
Formatted: Underline

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.[42]

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,[43] so registrar WHOIS accessibility is very important. When displaying WHOIS data for

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

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

[43] "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)[44] 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.

Faisal Shah 24/1/10 19:05
Deleted: R

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

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

was 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:

- ThreeTwo 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 (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[45], 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.

Faisal Shah 24/1/10 19:25
Deleted:

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."[46]

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

[46] 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 notice becomebecomes 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.”

Faisal Shah 24/1/10 19:37
Deleted: d

Mike O'Connor 20/1/10 09:34
Comment: Unpaired quote.

Faisal Shah 24/1/10 19:38
Deleted: An

So, it appears that some contractual violations are cured in an amicablea friendly 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.

Faisal Shah 24/1/10 19:39
Deleted: were

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

[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

Marika.Konings 27/1/10 11:22
Formatted: Underline

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]

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 restricting access to their port 43 Whois servers, and b) the results of an annual compliance audit of compliance with contractual WHOIS access obligations.

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

- 19/1/10 12:02

Deleted: The Expedited Registry Security Request (ERSR)

The Expedited Registry Security Request (ERSR)[49] 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 comment in September 2009. The ERSR was included in the Draft Applicant Guidebook, draft 3 (DAG3) so that it will be available for 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.

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.

- 19/1/10 12:03
Deleted: are

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.

- 19/1/10 12:03
Deleted: WG therefore

- 19/1/10 12:03
Deleted: .

8.2 Background

Marika.Konings 27/1/10 11:22
Formatted: Underline

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.

- 8/1/10 18:10
Comment: Deleted the material and referred to Web site, so that we can focus attention on the findings.

8.3 ICANN Agreement Landscape:

Marika.Konings 27/1/10 11:22
Formatted: Underline

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)

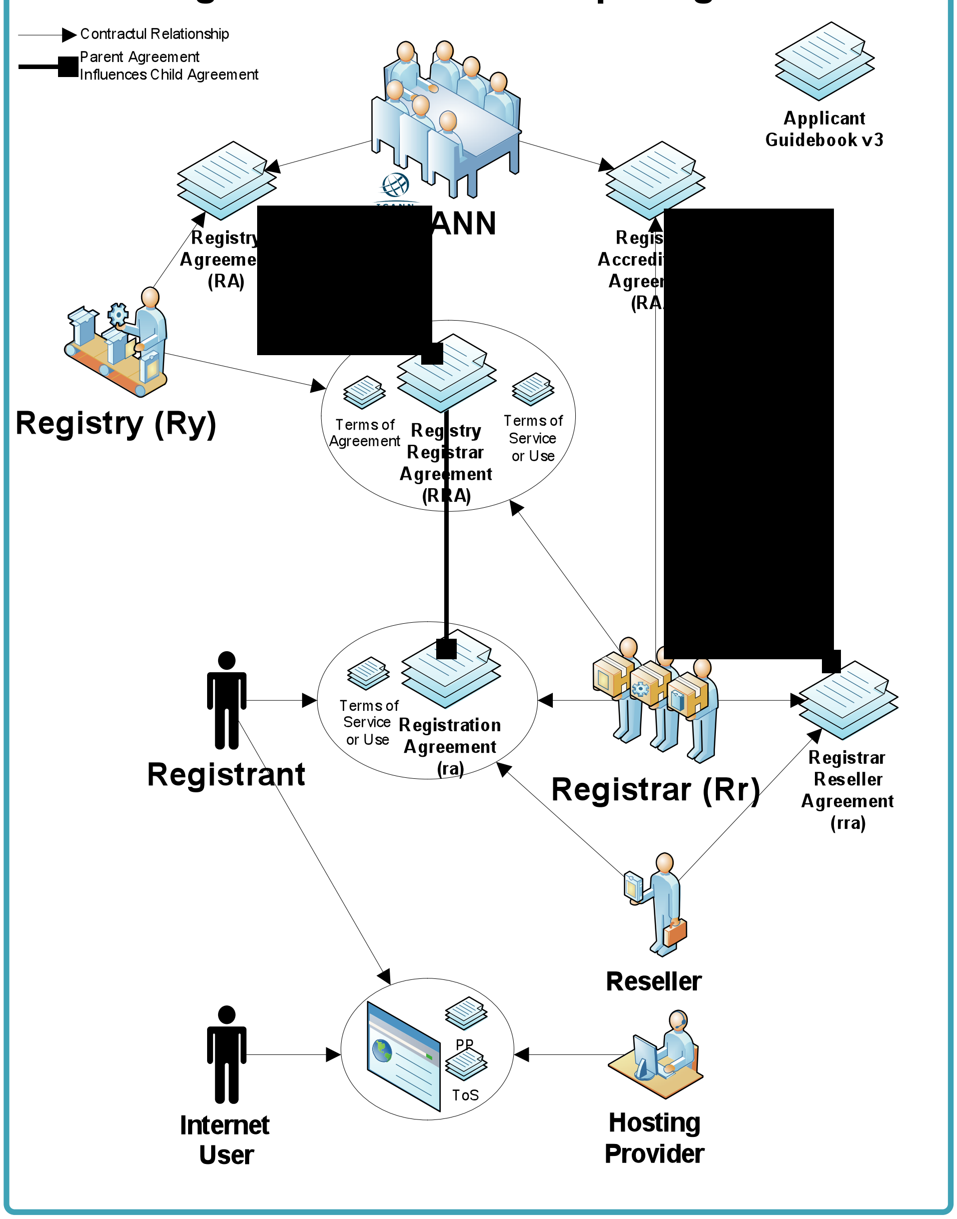
- Registrant
- Hosting Provider
- Internet User

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



Dispersion Findings:

Code	Agreement	Dispersion Found?	Supporting Data	Appendix	Summary Comments
RA	Registry Agreement	Yes	GNSO Registration Abuse Policies Issues Report	1	Some variance exists across the Registry Agreements. Some TLDs contain abuse provisions within the RA, while others contain the abuse provision in the RRA template nested within the RA. Other TLDS have abuse language within Acceptable Use Policies or Terms of Agreement posted on their respective web site.
RRA	Registry Registrar Agreement	Yes	GNSO Registration Abuse Policies Issues Report	2	Not every Registry Agreement contains an RRA Template, and as such, is where the dispersion begins. In the Registry Agreements that do contain an RRA, the templates appear to be consistent. Some members questioned whether they lack sufficient abuse definitions and indemnification language to combat abuse.
RAA	Registration Accreditation Agreement	Indirectly	2009 RAA Gap Analysis	3	The RAA is a template agreement for each Accredited Registrar, and as such does not have dispersion. However, the RAA does not contain any provisions relative to abuse definition, nor indemnification to sufficiently combat abuse.
ra	Registration Agreement*	Yes	UofC Dispersion Matrix & GNSO Registration Abuse Policies Issues Report	4	Across the sample of registrars used in the dispersion research, the structure of agreements did have many similarities, but significant dispersion across agreement titles, standard contract content, abuse content, and lack of abuse content did exist. The agreements themselves were often titled differently, ranging from Registration Agreements to Terms of Service, to Terms of Use, thus blurring scope with "Registration Agreements." Lastly, location of the agreements on Registrar sites varied greatly. See also ToS.
rra	Registrar Reseller Agreement	na	na	-	These agreements were not reviewed for dispersion, but we suspect great dispersion in how these agreements are structured
ToS	Terms of Service*	Indirectly		-	The use of this legal agreement does vary greatly across all industry participants. For the most part, these types of agreements are out of scope, however, some participants do label Registration Agreements as Terms of Service, and/or, Registration Agreement provisions became sub-sections within ToS agreements.

- 19/1/10 15:58
Deleted: Significant ...While o...s...contain ... [2]

Marika Konings 14/1/10 13:59
Formatted ... [3]

Marika Konings 14/1/10 13:59
Formatted ... [4]

- 19/1/10 12:05
Deleted: However,

- 19/1/10 12:05
Formatted: Font:Not Bold, Not Superscript/ Subscript, Not All caps, Not

Marika Konings 14/1/10 13:59
Formatted ... [5]

Marika Konings 14/1/10 13:59
Formatted ... [6]

Marika Konings 14/1/10 13:59
Formatted ... [7]

Marika Konings 14/1/10 13:59
Formatted ... [8]

- 14/1/10 11:25
Comment: Shouldn't we mention that that a ToS is legally binding when referenced in an ra?

ToU	Terms of Use*	Not Directly		-	" "
PP	Privacy Policy	na	na	-	none
AGv3	Applicant Guidebook version 3	na	na	-	Section within Agv3 relative to malicious conduct <out of scope for dispersion research>

*** Registrars vary greatly in how agreements are titled**

8.4 Conclusions & Guiding Principles

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

8.4.1 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.

8.4.2 Abuse Provision Baseline (APB)

- 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

- 14/1/10 11:25
Comment: What's the difference between a ToU and a ToS? My understanding is that they are just different terms for the same ting. Should ToU be deleted?

Marika Konings 14/1/10 13:59
Formatted ... [9]

Marika Konings 14/1/10 13:59
Formatted ... [10]

Marika Konings 14/1/10 13:59
Formatted ... [11]

Marika Konings 14/1/10 13:59
Formatted ... [12]

- 8/1/10 18:11
Comment: Suggest deleting this category – it's in flux, and it's basically just another flavor of RA.

Marika.Konings 27/1/10 11:23
Formatted: Underline

- 19/1/10 12:05
Deleted: acknowledges ..., and the... ...is ....
W ... [13]

- 19/1/10 12:06
Deleted: s...mitigation ....
I ... [14]

- 19/1/10 12:07
Deleted: s

- 19/1/10 16:01
Deleted: A

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 "desired model," but the sub-team team did not recognize variance among business types.

- The sub-team thought that any APB 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 registrationaAbuse 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.

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 include:

- Registries and registrars 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

- 19/1/10 16:01
Deleted: is

- 19/1/10 16:01
Deleted: the

- 19/1/10 16:01
Deleted: D

- 19/1/10 16:01
Deleted: M

- 19/1/10 16:01
Deleted: does

- 20/1/10 12:39
Deleted: An

- 19/1/10 16:02
Deleted:

- 19/1/10 12:10
Deleted: s

- 19/1/10 16:02
Deleted:

- 19/1/10 16:02
Deleted:

- 20/1/10 12:39
Deleted: R

- 20/1/10 12:39
Deleted:

- 20/1/10 12:39
Deleted: P

- 20/1/10 12:39
Deleted:

- 19/1/10 16:02
Deleted:

- 19/1/10 16:02
Deleted: agrees

- 19/1/10 16:02
Deleted: will be

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.

Some RAPWG members expressed that a general APB may not be a realistic goal. A concern is that the creation of “general language with broad powers to act against all kinds of abuse” 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. 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.

8.5 Recommendations

The RAP WG 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.

- 19/1/10 16:55
Deleted: a formal PDP

Marika Konings 14/1/10 11:48
Deleted: TBD from Berry Cobb

Marika.Konings 27/1/10 11:27
Formatted: Indent: Left: 0", Hanging: 0,5", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0" + Indent at: 0,25"

9. Meta Issues

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

- 19/1/10 12:10
Deleted: This working group has begun

- 19/1/10 12:10
Deleted: ying

- 19/1/10 12:31
Deleted: which are turning up in number of GNSO working-groups (RAP, Inter-Registrar Transfer Policy and Post-Expiration Domain Name Recovery) and ICANN advisory-groups (High Security TLD and Zone File Access) at the same time.

- 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

- 19/1/10 12:32
Deleted: <#>They are being discussed in several working and advisory groups simultaneously

- 19/1/10 12:32
Deleted: working and advisory

9.1 Meta-issue : Uniformity of reporting

- 19/1/10 12:32
Deleted: –

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.

- 19/1/10 12:33
Deleted: working group

- 19/1/10 12:33
Deleted: has

- 19/1/10 12:33
Deleted: their

- 19/1/10 12:34
Deleted: recommendation is a "meta-issue" because it is

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:

- 19/1/10 12:34
Deleted: things

- 19/1/10 12:34
Deleted: pretty rough

- 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.

9.1.2 Recommendation

The RAPWG suggests that this “meta-issue” be addressed either by a PDP working group, a best-practices working group or an ICANN advisory group, with the goals of:

- 19/1/10 12:35
Deleted: working group

- 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.

9.2 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.*

- 19/1/10 12:35
Deleted: The working group suggests, as a starting point for discussion, that every policy should have:

- 19/1/10 12:37
Deleted: –

- 19/1/10 12:37
Deleted: “

- 19/1/10 12:37
Deleted: ”

- 19/1/10 12:37
Deleted: working group

- 19/1/10 12:39
Deleted: the domain registration community to

- 19/1/10 12:37
Deleted: ollect

- 19/1/10 12:37
Deleted: in many

- 19/1/10 12:38
Deleted: for various participants in the field into some sort of knowledge base. Further, an efficient means to disseminate these practices to all the

- 19/1/10 12:38
Deleted: is desired

- 19/1/10 12:40
Deleted: Best practices should also be kept current and relevant.

> *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

- 19/1/10 13:12
Deleted: The Problem

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

- 19/1/10 13:09
Deleted: tackling

- 19/1/10 12:56
Deleted: they

- 19/1/10 12:56
Deleted: abuse and

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.

- 19/1/10 13:10
Deleted: are necessary but

- 19/1/10 13:10
Deleted: augers for the collection of

- 19/1/10 13:10
Deleted: and sharing of that information

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?

- 19/1/10 13:11
Deleted: many

- 19/1/10 13:11
Deleted: ould

9.2.3 Recommendation

The working group suggests that this “meta-issue” be addressed either by a PDP working group or an ICANN advisory group, with the goals of:

- 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 may be incorporated into more formal policies.

- 19/1/10 13:13
Deleted: <#>Establishing processes for updating best practices over time.

- 19/1/10 13:13
Deleted: e/

1852

- 19/1/10 13:12
Deleted: <#>Scope of discussion

Marika.Konings 27/1/10 11:17
Formatted: Bullets and Numbering

10. Conclusions, Recommendations, & Next Steps

- 19/1/10 13:12
Deleted: s

[TBD]

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 and Attendance

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[50]
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

Marika.Konings 27/1/10 11:42
Deleted: Registry

Marika.Konings 27/1/10 11:44
Deleted: Registrar

Marika.Konings 27/1/10 11:43
Deleted: Registry

Marika.Konings 27/1/10 11:43
Deleted: R

Marika.Konings 27/1/10 11:43
Deleted: egistry

Marika.Konings 27/1/10 11:44
Deleted: Registrar

Marika.Konings 27/1/10 11:46
Deleted:

Marika.Konings 27/1/10 11:44
Deleted: Registrar

Marika.Konings 27/1/10 11:44
Deleted: Registrar

Marika.Konings 27/1/10 11:46
Deleted:

Marika.Konings 27/1/10 11:46
Deleted:

Marika.Konings 27/1/10 11:46
Deleted:

Marika.Konings 27/1/10 11:44
Deleted: Registrar

Marika.Konings 27/1/10 11:46
Deleted:

[50] RySG = Registry Stakeholdergroup, RrSG = Registrar Stakeholdergroup, 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[51]	CBUC
Michael Young	RySG
Rod Rasmussen	Individual
Edward Nunes	NCUC
Frederick Felman	IPC
Evan Leibovitch	ALAC
Caleb Queern	CBUC
Avri Doria	NCUC
Chuck Gomes (GNSO Chair)	RySG

Marika.Konings 27/1/10 11:44
Deleted: Registry

Marika.Konings 27/1/10 11:44
Deleted: R

Marika.Konings 27/1/10 11:44
Deleted: egistry

Marika.Konings 27/1/10 11:44
Deleted: NCA

Marika.Konings 27/1/10 11:44
Deleted: Registry

[Include attendance sheet]

[51] Left the Working Group on [insert date]

Annex III – Uniformity of Contracts: Additional Background Materials

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.

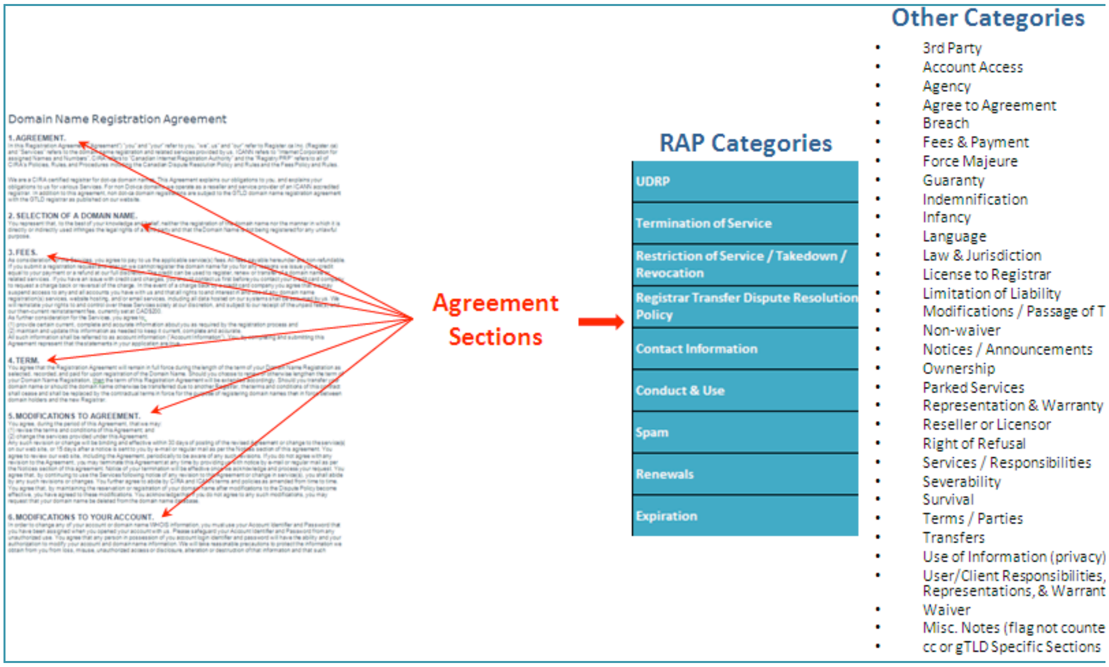
By review of the various registration agreements, sections began to naturally form in to forty or so categories in which the registration agreements could be inventoried. For each of the 22 Registrars, from the representative pool, an Excel spreadsheet was used to track the binary existence of each agreement 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 labeled in the blue boxes pertain to the abuse types within scope of the RAPWG.



Domain Name Registration Agreement

1. AGREEMENT.
In this Registration Agreement ("Agreement") "you" and "your" refer to you, "we", us" and "our" refer to Register.ca Inc. (Register.ca) and "Services" refers to the domain name registration and related services provided by us. ICANN refers to "Internet Corporation for assigned Names and Numbers". CIRA refers to "Canadian Internet Registration Authority" and the "Registry PRP" refers to all of CIRA's Policies, Rules, and Procedures including the Canadian Dispute Resolution Policy and Rules and the Fees Policy and Rules.

We are a CIRA certified registrar for dot-ca domain names. This Agreement explains our obligations to you, and explains your obligations to us for various Services. For non Dot-ca domains we operate as a reseller and service provider of an ICANN accredited registrar. In addition to this agreement, non dot-ca domain registrations are subject to the GTLD domain name registration agreement with the GTLD registrar as published on our website.

2. SELECTION OF A DOMAIN NAME.
You represent that, to the best of your knowledge and belief, neither the registration of the domain name nor the manner in which it is directly or indirectly used infringes the legal rights of a third party and that the Domain Name is not being registered for any unlawful purpose.

3. FEES.
As consideration for the Services, you agree to pay to us the applicable service(s) fees. All fees payable hereunder are non-refundable. If you submit a registration request and later we cannot register the domain name for you for any reasons we issue you a credit equal to your payment or a refund at our full discretion. The credit can be used to register, renew or transfer of a domain name or related services. If you have an issue with credit card charges, you should contact us first before you contact your credit card company to request a charge back or reversal of the charge. In the event of a charge back by a credit card company you agree that we may suspend access to any and all accounts you have with us and that all rights to and interest in and use of any domain name registration(s) services, website hosting, and/or email services, including all data hosted on our systems shall be [illegible] by us. We will reinstate your rights to and control over these Services solely at our discretion, and subject to our receipt of the unpaid fees and our then-current reinstatement fee, currently set at CAD$200.
As further consideration for the Services, you agree to:
(1) provide certain current, complete and accurate information about you as required by the registration process and
(2) maintain and update this information as needed to keep it current, complete and accurate.
All such information shall be referred to as account information ("Account Information"). You, by completing and submitting this Agreement represent that the statements in your application are true.

4. TERM.
You agree that the Registration Agreement will remain in full force during the length of the term of your Domain Name Registration as selected, recorded, and paid for upon registration of the Domain Name. Should you choose to renew or otherwise lengthen the term of your Domain Name Registration, than the term of this Registration Agreement will be extended accordingly. Should you transfer your domain name or should the domain name otherwise be transferred due to another Registrar, the terms and conditions of this contract shall cease and shall be replaced by the contractual terms in force for the purpose of registering domain names then in force between domain holders and the new Registrar.

5. MODIFICATIONS TO AGREEMENT.
You agree, during the period of this Agreement, that we may:
(1) revise the terms and conditions of this Agreement; and
(2) change the services provided under this Agreement.
Any such revision or change will be binding and effective within 30 days of posting of the revised Agreement or change to the service(s) on our web site, or 15 days after a notice is sent to you by e-mail or regular mail as per the Notices section of this agreement. You agree to review our web site, including the Agreement, periodically to be aware of any such revisions. If you do not agree with any revision to the Agreement, you may terminate this Agreement at any time by providing us with notice by e-mail or regular mail as per the Notices section of this agreement. Notice of your termination will be effective once we acknowledge and process your request. You agree that, by continuing to use the Services following notice of any revision to this Agreement or change in service(s), you shall abide by any such revisions or changes. You further agree to abide by CIRA and ICANN terms and policies as amended from time to time. You agree that, by maintaining the reservation or registration of your domain name after modifications to the Dispute Policy become effective, you have agreed to these modifications. You acknowledge that if you do not agree to any such modifications, you may request that your domain name be deleted from the domain name database.

6. MODIFICATIONS TO YOUR ACCOUNT.
In order to change any of your account or domain name WHOIS information, you must use your Account Identifier and Password that you have been assigned when you opened your account with us. Please safeguard your Account Identifier and Password from any unauthorized use. You agree that any person in possession of you account login identifier and password will have the ability and your authorization to modify your account and domain name information. We will take reasonable precautions to protect the information we obtain from you from loss, misuse, unauthorized access or disclosure, alteration or destruction of that information and that such

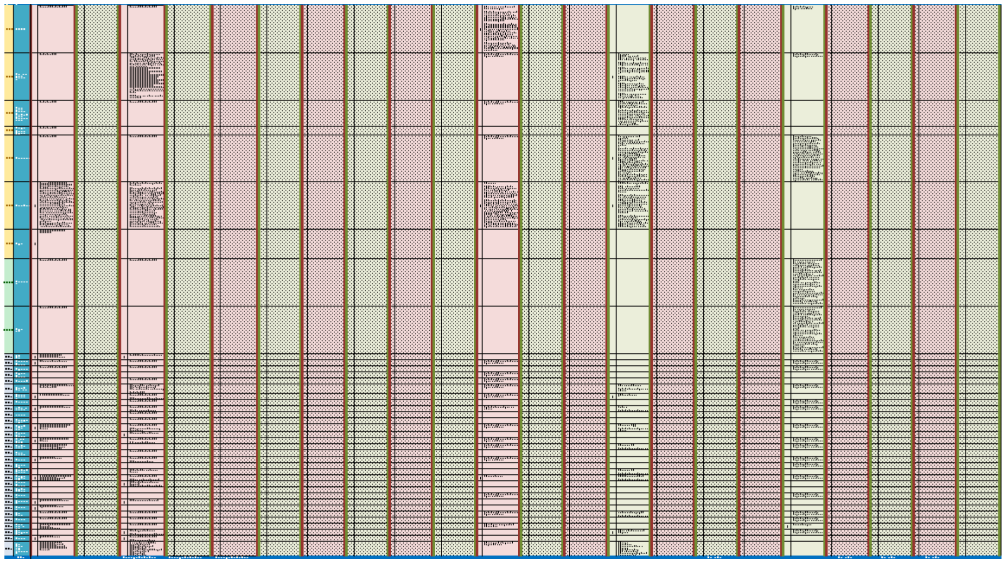
RAP Categories

- UDRP
- Termination of Service
- Restriction of Service / Takedown / Revocation
- Registrar Transfer Dispute Resolution Policy
- Contact Information
- Conduct & Use
- Spam
- Renewals
- Expiration

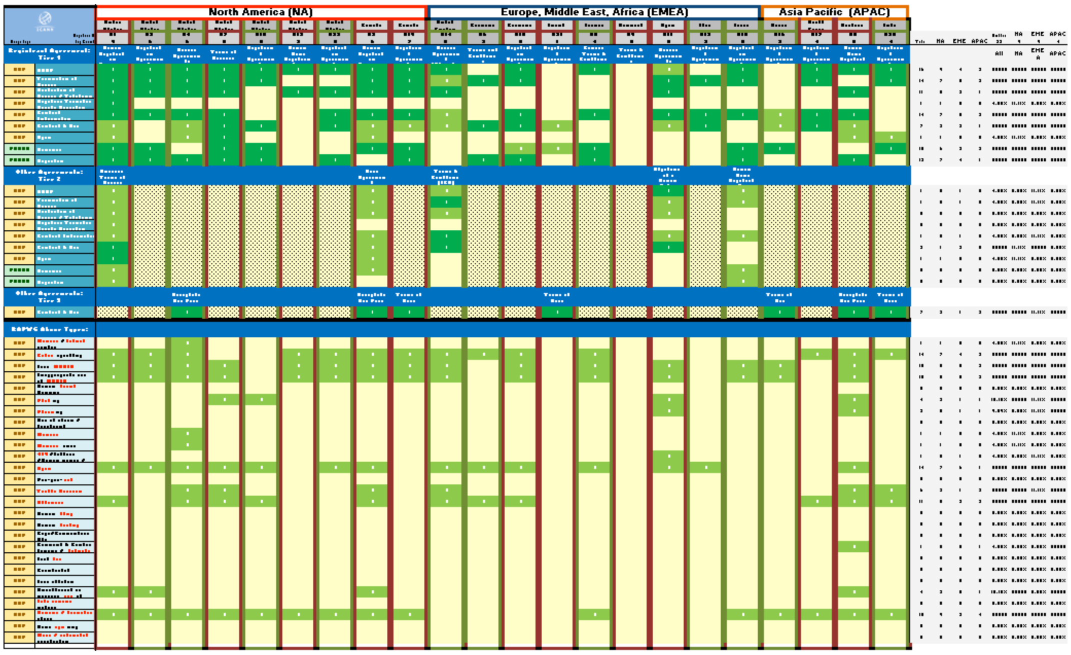
Other Categories

- 3rd Party
- Account Access
- Agency
- Agree to Agreement
- Breach
- Fees & Payment
- Force Majeure
- Guaranty
- Indemnification
- Infancy
- Language
- Law & Jurisdiction
- License to Registrar
- Limitation of Liability
- Modifications / Passage of T
- Non-waiver
- Notices / Announcements
- Ownership
- Parked Services
- Representation & Warranty
- Reseller or Licensor
- Right of Refusal
- Services / Responsibilities
- Severability
- Survival
- Terms / Parties
- Transfers
- Use of Information (privacy)
- User/Client Responsibilities, Representations, & Warrant
- Waiver
- Misc. Notes (flag not counte
- cc or gTLD Specific Sections

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:



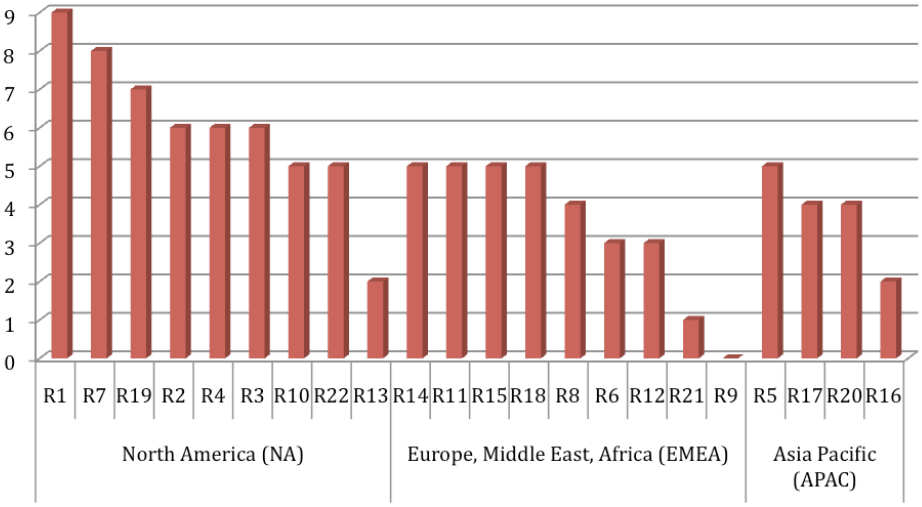
This screen shot represents a summary view of the previous spreadsheet. The legend is listed below, but basically the variance between the green and yellow coloring depicts the dispersion found within agreements relative to abuse. The gray section to the right provides “hit rate” percentages of agreement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


North America (NA)
Europe, Middle East, Africa (EMEA)
Asia Pacific (APAC)

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

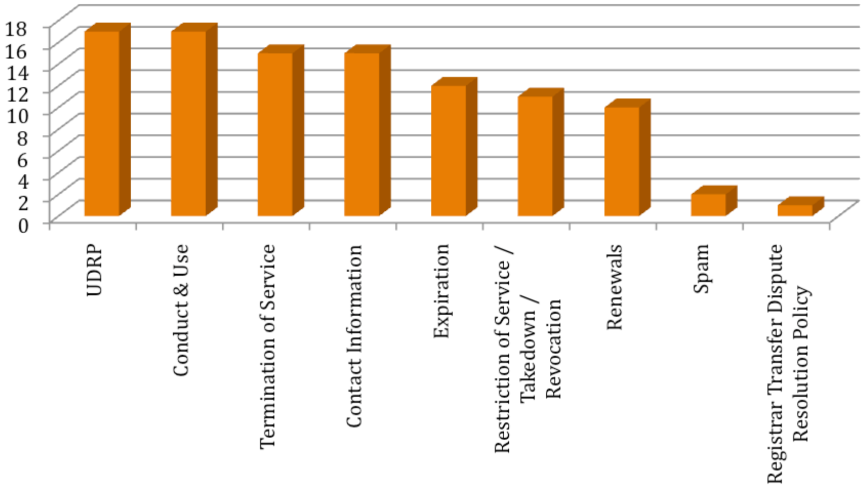
The chart below provides a different view at the dispersion across Registration Agreements. The Y Axis represents the number of categories where the agreement satisfied the formal section definition requirements while the X Axis represents registrars by region, sorted highest to least (left to right).



2043

2044

2045 This chart represents categories with the greatest achievement of section definition.



2046

2047

2048 **APB Example:**

Definition of Abuse

a. Abuse is an action that: --- **(source: RAP – WG Definition; DRAFT Only!)**-----

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

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

b. Domain abuse creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general. ***<Registry>*** *defines abusive use as the wrong or excessive use of power, position or ability, and includes, without limitation, the following*: --- **(source: .info Domain Anti-Abuse Policy)**-----

   i. Illegal or fraudulent actions;

   ii. Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;

   iii. Phishing: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;

   iv. Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;

   v. Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent.

   vi. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses;

   vii. Fast flux hosting: Use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of Affilias;

   viii. Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);

ix. Distribution of child pornography; and

x. Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Indemnification - --- **(source: .info Domain Anti-Abuse Policy & .org RRA - 3.6 Additional Requirements for Registration Agreement/3.65)**-----

a. Pursuant to the RRA, **<Registry>** reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of **<Registry>**, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by **<Registry>** or any Registrar in connection with a domain name registration. **<Registry>** also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute. Abusive uses, as defined above, undertaken with respect to **<TLD>** domain names shall give rise to the right of **<Registry>** to take such actions under RRA in its sole discretion.

Page 52: [1] Deleted – 20/01/10 13:47

Addressing use of Stolen Identity Credentials

[Placeholder for now]

Idea – regular dissemination of best practices for identifying stolen identities

Idea – provide policy framework to ALLOW information sharing between registrars on fraudulent domain registrations and registration attempts.

Idea – create information sharing clearinghouse to facilitate information sharing between registrars (and resellers) on fraudulent domain registrations and registration attempts. Data elements could include some aspects of stolen identity credentials.

Page 66: [2] Deleted – 19/01/10 15:58

Significant

Page 66: [2] Deleted – 19/01/10 12:04

While o

Page 66: [2] Deleted – 20/01/10 12:55

s

Page 66: [2] Deleted – 20/01/10 12:54

contain

Page 66: [3] Formatted Marika Konings 14/01/10 13:59

Not Superscript/ Subscript, Not All caps

Page 66: [3] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [3] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [4] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [4] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [5] Formatted Marika Konings 14/01/10 13:59

Not Superscript/ Subscript, Not All caps

Page 66: [5] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [5] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [5] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [6] Formatted Marika Konings 14/01/10 13:59

Not Superscript/ Subscript, Not All caps

Page 66: [6] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [7] Formatted Marika Konings 14/01/10 13:59

Not Superscript/ Subscript, Not All caps

Page 66: [7] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [7] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [7] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [7] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [8] Formatted Marika Konings 14/01/10 13:59

Not Superscript/ Subscript, Not All caps

Page 66: [8] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [8] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 66: [8] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not Superscript/ Subscript, Not All caps

Page 67: [9] Formatted Marika Konings 14/01/10 13:59

Not All caps

Page 67: [9] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [10] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [10] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [10] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [11] Formatted Marika Konings 14/01/10 13:59

Not All caps

Page 67: [11] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [11] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [11] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [11] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [11] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [12] Formatted Marika Konings 14/01/10 13:59

Not All caps

Page 67: [12] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [12] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [12] Formatted Marika Konings 14/01/10 13:59

Font:Not Bold, Not All caps

Page 67: [13] Deleted – 19/01/10 12:05

acknowledges

Page 67: [13] Deleted – 19/01/10 12:06

, and the

Page 67: [13] Deleted – 19/01/10 12:06

Page 67: [13] Deleted – 19/01/10 12:06

is

Page 67: [13] Deleted – 20/01/10 14:02

.

Page 67: [13] Deleted – 19/01/10 12:06

Page 67: [13] Deleted – 19/01/10 12:06

W

Page 67: [14] Deleted – 19/01/10 12:06

s

Page 67: [14] Deleted – 19/01/10 16:41

mitigation

Page 67: [14] Deleted – 19/01/10 12:06

.

I