C O A L I T I O N F O R O N L I N E A C C O U N T A B I L I T Y
WWW.ONLINEACCOUNTABILITY.NET

C/O MITCHELL SILBERBERG & KNUPP LLP ● 1818 N STREET N.W., 8TH FLOOR ● WASHINGTON, D.C. 20036-2406
TEL: (202) 355-7900 ● FAX: (202) 355-7899 ● E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

COMMENTS ON PPSAI WORKING GROUP INITIAL REPORT

July 7, 2015

The Coalition for Online Accountability (COA) appreciates this opportunity to comment on the initial report of the Privacy and Proxy Service Accreditation Issues (PPSAI) Working Group ("initial report"). See https://www.icann.org/public-comments/ppsai-initial-2015-05-05-en

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners. They are the American Society of Composers, Authors and Publishers (ASCAP); Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. COA's counsel, and representatives of several COA participating organizations, participated actively in the work of the PPSAI Working Group.

COA generally endorses the conclusion of the GNSO Intellectual Property Constituency: that the initial report represents a constructive contribution toward replacing the current chaos of the privacy/proxy registration marketplace with a clear, balanced and enforceable set of accreditation standards that privacy/proxy services would be required to fulfill. In particular, we believe that Annex E of the Initial Report – the Illustrative Disclosure Framework for disclosure of contact data in response to complaints of intellectual property infringement – goes far toward achieving its goals of balancing predictability for requesters, flexibility for providers, and protection of registrants. This Framework is the product of protracted negotiations, first between intellectual property interests and leading registrar participants in the Working Group, and then among these interests and those of privacy advocates, registrant representatives from the at-large community, business interests, and other participants in the working group. While we agree with IPC that some changes are needed, all the participants should be proud of what they have produced and should be taking up the challenge of explaining and justifying the compromises reflected in the initial report. It is disappointing to COA that some of those with whom we have been negotiating and discussing these issues over the past two years within the Working Group have chosen a different and less constructive path.

One of the first tasks before the Working Group once the public comment period closes is to decide how to deal with many thousands of comments generated by a couple of websites

sponsored by accredited domain name registrars. The substance of these comments either call for a standard that would make privacy/proxy service accreditation impossible, or else appear to support the initial report, and at most have relevance only to one contested issue considered by the Working Group. The form of these comments strongly suggests that it is highly unlikely, at best, that the commenters read any part of the Working Group's initial report, and that these comments are reactions to the way the websites described the report, which bears little relationship to the report itself. This submission addresses each of the sets of comments in turn, in an attempt to assist the Working Group in its discussions about how to best understand and value these machine-generated/petition-style comments in the context of the Working Group's mandate and goal.

A. Machine-generated petitions and comments

1. respectourprivacy.com

One such website, respectourprivacy.com, is clearly the source of thousands of individual comments generated when site visitors clicked on an e-mail link presented by the site. The full text of these machine-generated comments is as follows:

"Dear ICANN –

Regarding the proposed rules governing companies that provide WHOIS privacy services (as set forth in the Privacy and Policy Services Accreditation Issues Policy document):

I urge you to respect internet users' rights to privacy and due process.

– Everyone deserves the right to privacy.

– No one's personal information should be revealed without a court order, regardless of whether the request comes from a private individual or law enforcement agency.

Private information should be kept private. Thank you."

No existing privacy/proxy service participating in or reviewed by the Working Group, and probably no such service in existence, could function under the standard called for by this mass comment. It advocates a system in which signing up for a proxy or privacy service creates an irreversible entitlement to anonymity. Nothing that the customer does or fails to do with respect to the service or the underlying registration would be allowed to negate that entitlement, unless a "court order" requires that it be negated. Effectively, the customer would be privileged to refuse to make any payments for the service; to refuse to provide the service with reliable contact information; to use the domain name to carry out crimes or any other kind of illegal activity; or to refuse to conform with any other terms of service, all without any possibility that the customer's contact information would be disclosed to any party, or published in the publicly accessible Whois. Under this standard, the terms of service of at least many major service providers operating today, as set forth in the Appendix to this comment[1], and probably of

[1] The Terms of Service excerpted in the Appendix to this comment are drawn either from registrars listed as sponsors of one or

virtually every such service on the planet, would be ruled invalid, and presumably any accredited registrar knowing doing business with (much less itself operating) such a service would be subject to enforcement action by ICANN compliance.[2] It should not be difficult for the Working Group to conclude that adopting this proposal would be completely contrary to its mandate and must be rejected.

2. savedomainprivacy.org

A second website, savedomainprivacy.org, invites users to sign a petition, which the sponsoring accredited registrars say they will deliver to ICANN at the conclusion of the public comment period. The full text of the petition reads as follows:

I, the undersigned, support

- The legitimate use of privacy or proxy services to keep personal information private, protect physical safety, and prevent identity theft

- The use of privacy services by all, for all legal purposes, regardless of whether the website is "commercial"

- That privacy providers should not be forced to reveal my private information without verifiable evidence of wrongdoing

Since all these statements are consistent with the initial report, these petitions should be considered as supportive of the report.

The first point stated in the petition – that P/P Services can serve legitimate purposes – is such a fundamental premise of the Initial Report that it essentially goes unstated in the document: the entire ***purpose*** of the Initial Report is to develop an accreditation scheme or accepted set of baseline best practices for P/P Services[3], which of course assumes that P/P Services will exist for some legitimate purpose.

On the second point, the Initial Report explicitly states that "the mere fact that a domain name is registered by a commercial entity or by anyone conducting **commercial activity** should **not** preclude the use of P/P services"(sec. 1.3.3.)(emphasis added). The initial report goes on to note that while there was a minority position in the WG in favor of limiting the availability of P/P Services for domain names "actively used for commercial transactions," "most WG members did not believe such a prohibition is necessary or practical."[4] There was also no consensus position in the Initial Report about whether to permit use of p/p registrations for sites engaged in online financial transactions in a commercial context. The petitions may have some relevance for the WG's further deliberations on this last point, but subject to the caveats below.

(…continued)
both websites discussed in this comment, or from the affiliated proxy service provider to one of such registrars.

[2] The Initial Report repeatedly notes that the ability of service providers to enforce their Terms of Service and to disclose or publish customer contact data for violations of the same must be preserved. See, e.g., Recommendations 6 and 8 (disclosure of conditions for publication and disclosure); Annex E, section I.D. (savings clause for enforcement of terms of service). Certainly this would not be allowed under the regime advocated by the sponsors of respectourprivacy.com.

[3] Initial Report at 5.

[4] Initial Report at 15-16.

On the third point, the Initial Report reserves to providers considerable discretion about when to reject a request for disclosure in general; and in the sole area in which the Initial Report proposes more detailed standards, the Illustrative Disclosure Framework applicable to intellectual property complaints specifically contemplates that P/P Providers will only be required to disclose P/P Customer contact details when presented with "verifiable evidence of wrongdoing" – namely, a good faith statement, either under penalty of perjury or notarized or accompanied by a sworn statement (or the German equivalent, "Versicherung an Eides statt"), that provides a basis for reasonably believing that the use complained of is infringing and is not defensible (in addition to other verifiable evidence as to the complaining party's contact information, ownership of the trademark or copyright in question, etc.).[5] Even in cases in which all these criteria for providing "verifiable evidence" are met, the Disclosure Framework recognizes the discretion of the service provider to reject claims for which it has a specific basis for determining that the disclosure request is pretextual.

In light of these points of agreement, it is not clear what exactly those who sign the savedomainprivacy.org petition would ***change*** about the Initial Report. For that reason, any petitions submitted through the campaign must presumably be understood by the WG as supporting the Initial Report.

B. Human-generated comments arising from the websites

Both websites enable users to add additional comments or statements in addition to the pre-packaged petition/comment language to which they were invited to click assent. While the vast majority evidently did not avail themselves of this option, a handful did so, and these additional comments should be considered by the Working Group. However, the context in which they were received is important. While both websites also provide a link to the full text of the report, it would be unwise to assume that any of these commenters actually reviewed the report itself, at least absent any indication in their comments that they had done so (e.g., citation to or quotations from the Initial Report). Many of these handful of commenters more likely relied solely, or at least predominantly, upon the information presented on the websites.

Accordingly, in considering how much weight to accord to these website-generated comments (in those rare cases in which anything beyond the pre-packaged petition language was submitted), it is necessary to review the information presented on the websites for accuracy and completeness. This review indicates that many of the statements made on these website about key aspects of the Initial Report are misleading and incomplete, and in some cases simply false. The resulting comments should be evaluated in this context.

1. Respectourprivacy.com[6]

The full text appearing on this website to explain what is in the Initial Report is reproduced within quotation marks below, along with our commentary/response in *italics*.

---

[5] Initial Report at 86-90.

[6] Note that the text presented on the respectourprivacy.com website is headed "Save Domain Privacy." It is not clear whether this is coincidental or whether the two sites are coordinated.

*"*Under new guidelines proposed by MarkMonitor and others who represent the same industries that backed SOPA, domain holders with sites associated to 'commercial activity' will no longer be able to protect their private information with WHOIS protection services.*"*

False. In fact, the Initial Report reflects that "the WG agreed that the mere fact that a domain name is registered by a commercial entity or by anyone conducting commercial activity should ***not*** *preclude the use of P/P services"(sec. 1.3.3.)(emphasis added). This conclusion was adopted without dissent, and thus could be considered to have been supported as much by accredited domain name registrars and privacy advocates as by those mentioned on the website. The issue is not over "commercial activity" but rather over the question "whether domain names that are actively used for commercial transactions (e.g., the sale or exchange of goods or services) should be prohibited from using P/P services." (Id.) As noted above, the report states that "most WG members" did not support such a prohibition but that "some members" did.*

""Commercial activity" casts a wide net, which means that a vast number of domain holders will be affected."

Misleading. As noted above, the issue in contention is not "commercial activity" but "commercial transactions," and specifically "online financial transactions for commercial purposes." Furthermore, it is clear from the initial report that no definition of this term had been adopted, and members of the public were specifically asked "do you think it would be useful to adopt a definition of 'commercial' or 'transactional' to define those domains for which P/P service registrations would be disallowed"? If so, what should the definition(s) be?" In the absence of any definition, assertions that "a vast number of domain holders will be affected" are unsupported.

"Your privacy provider could be forced to publish your contact data in WHOIS or even give it out to anyone who complains about your website, without due process."

Misleading. While the use of "could" might save the statement from outright falsity, the misleading nature of the previous sentences undermines the veracity of assertions about "you" and "your website." More fundamentally, as noted above, the Initial Report does not dictate when P/P providers must respond positively to disclosure requests, and even in the Illustrative Disclosure Framework (which of course applies only to allegations of infringement, not of participation in "online financial transactions for commercial purposes"), ample provider discretion is preserved. To the extent that "due process" is read to exclude unilateral service provider enforcement of its terms and conditions, we have already noted that no existing p/p service could possibly meet this standard.

"Why should a small business owner have to publicize her home address just to have a website?"

False. As just noted, there was broad agreement within the WG that commercial entities should remain entitled to use p/p services under an accreditation regime.

2. SaveDomainPrivacy.org

Most statements about the Initial Report on this website appear on the page entitled "What's Changing?", and include the following:

"The Internet Corporation for Assigned Names and Numbers (ICANN) is working on a program that would create new restrictions on the companies offering WHOIS privacy services, or "Providers."

True – although many of the proposed accreditation standards are drawn from the current Terms of Service of providers (see Appendix for examples).

"Under the proposed new rules, Providers would be required to monitor your use of domain names and websites."

False. Nothing in the Initial Report requires this. All the mechanisms spelled out in it, such as Relay and Disclosure, are complaint-driven, and the proposed accreditation standards address how providers should react to requests; there is no reference at all to any proactive monitoring.

"Providers could be forced to terminate your privacy service and be required to publish your contact data in WHOIS."

False. While the Initial Report would require providers to publish their Terms of Service, including when publication of customer data in Whois would occur, and to explain these terms to customers, it contains no specific mandates requiring publication, leaving this instead to provider terms and conditions.

"Likewise, Providers could be required to give your private contact details to anyone complaining that your website violates their trademark or copyright."

False, even with the word "could," since the Illustrative Disclosure Framework applicable to such complaints makes clear that (1) complaints must meet specific detailed standards before triggering action (not "anyone complaining"); (2) providers retain discretion to reject complaints if they have a reasonable basis for believing infringement is not occurring or the use is defensible; and (3) even where (1) and (2) do not apply, complaints could be rejected if there is specific information demonstrating they are pretextual. See generally Annex E, section III.C.

"None of these scenarios would require a court order, search warrant, or due process of any kind."

False, since all the above "scenarios" are specious.

"It's important to emphasize that Providers do not want criminals to abuse these services to hide their online activities from law enforcement. But some of the proposed changes would treat all users equally, regardless of their intent. For millions of legitimate users, these services are no more suspicious than getting an unlisted telephone number."

While the premise of the first sentence is not contested, at least as to many providers, the implication that the Initial Report would treat users as if they were "criminals" is entirely misleading. Nothing in the report casts any doubt on the legitimacy of p/p services in many cases and for many users; it simply proposes minimum standards that providers of these services would need to meet in order to treat those customers fairly, and to create a more predictable and balanced system for relaying messages to those customers, and disclosing their identities on a limited basis where needed to resolve issues arising from verifiable evidence that their domain names are being used for illegal purposes.

The remainder of this page of the website consists of six brief narratives regarding hypothetical websites and registrants, each ending with the question whether the contact information of the customer "should" be disclosed. The clear implication is that the privacy of registrants in each scenario would be threatened if the Initial Report were approved; but the basis for any such assertion seems no more tangible that it is for the other characterizations of the Initial Report on this website. Nearly all these narratives, to the extent they are relevant to the WG's Initial Report, turn solely on the issue whether the activity described involves "online financial transactions for commercial purposes," and therefore would, under the view of a minority of WG participants, provide grounds for disclosure or publication of customer information. (As noted above, there was no dissent to the report's conclusion that parties engaged in commercial activity should not be precluded from using privacy/proxy services.) To the extent these narratives raise other issues, particular with regard to possible intellectual property claims, any comments referencing them should be evaluated in light of the provisions of the Illustrative Disclosure Framework in Annex E, and notably the provision authorizing rejection of pretextual disclosure requests (see section III.C.v.)

In sum, an examination of these registrar-sponsored websites leads to the following conclusions:

***Machine-generated comments from respectourprivacy.com should be treated as objections to the concept of privacy/proxy service accreditation, and to the concept of any enforceable Terms of Service for such services, and thus rejected as outside the WG's remit;

*** Petitions generated by the savedomainprivacy.org site should be treated as statements in support of the initial report;

*** Additional comments appended to submissions generated by either site should be evaluated in light of how these sites characterize the initial report, taking into consideration that in nearly every case, the implied or express characterizations are false, misleading, or seriously incomplete.

COA appreciates the WG's consideration of our views and stands ready to provide any additional information.

Respectfully submitted,

Steve Metalitz, counsel to COA

Appendix:
Selected Provisions from P/P Provider Terms of Service[1]

- **Blacknight Internet Solutions Ltd.**: the "WHOIS Privacy Service Terms" agreement "can be terminated by the Service Provider at any stage and for any reason which we deem appropriate with or without prior notice to the Customer"; and "Where this Agreement is Terminated prior to the expiration of its term, then all Whois information held by the Service Provider in connection with the services provided will be made public on the Whois Database."[2]

- **Whoisprivacy.com, Ltd.**: "Whois Privacy has the right at its sole discretion to suspend, cancel or modify the Service or to cancel your subscription of the Service (which would result in you becoming the official registrant of the Registered Name and your Personal Information becoming available on the publicly available Whois Directory) at any time."[3]

- **Namecheap, Inc./WhoisGuard, Inc.**[4]: "WhoisGuard reserves the right to alter, suspend, or discontinue the Site or any of the Services at any time and for any reason, without prior notice to you."[5]

- **EuroDNS S.A.**: "The Customer understands that any improper use of the Whois Protection Service may result in the immediate, and without prior notice, deletion of the Domain Name by EuroDNS and/or the Protection Agent, as well as the complete suspension of the Customer Account if EuroDNS deems it necessary… The Customer accepts that in certain circumstances, EuroDNS will be entitled to terminate the provision of the Whois Protection Service without prior notice, thus disclosing the Customer's Details to the public. Circumstances where such termination may happen, without it being deemed a default of EuroDNS towards its contractual or legal obligations, include but are not limited to . . . failure by the Customer to pay to EuroDNS any fee due for the Whois Protection Service provision."[6]

- **Namecheap, Inc./WhoisGuard, Inc.**: "If Whoisguard is unable to collect renewal or other fees, you agree that Whoisguard may contact you, but is not obliged to do so, and you agree that Whoisguard may suspend or terminate the WHOIS Privacy Services as a result of inability to obtain payment."[7]

---

[1] The Terms of Service excerpted in this Appendix are drawn either from registrars listed as sponsors of one or both websites discussed in the COA comment, or from the affiliated proxy service provider to one of such registrars.
[2] https://www.blacknight.com/acceptable-usage.html.
[3] http://www.whoisprivacyservices.com.au/terms.htm.
[4] WhoisGuard, Inc. is not a listed participant in the savedomainprivacy.org campaign, but Namecheap is: http://www.savedomainprivacy.org/about-us/, and is also the sponsor of the respectourprivacy.com website. WhoisGuard subscriptions are provided by WhoisGuard pursuant to its Services Agreement with Namecheap; WhoisGuard subscriptions can be used on domains registered with Namecheap only: https://www.namecheap.com/security/whoisguard.aspx. This comment will reference both the "Namecheap WHOIS Proxy Agreement" (located here: https://www.namecheap.com/legal/whoisguard/whoisguard-agreement.aspx) and the "WhoisGuard Terms of Service" (located here: http://www.whoisguard.com/legal-tos.asp) as applicable.
[5] http://www.whoisguard.com/legal-tos.asp.
[6] https://www.eurodns.com/terms-and-conditions/whois-privacy.
[7] https://www.namecheap.com/legal/whoisguard/whoisguard-agreement.aspx.

- **Blacknight Internet Solutions Ltd.**: "Reasons for termination include, but are not limited to the following: Non Payment of requested Fees within the specified period . . . ."[8]

- **1&1 Internet, Inc.**: "1&1 has the absolute right and power, as it deems necessary in its sole discretion, without providing notice and without any liability to you whatsoever, to (1) reveal to third parties the contact information provided by you to 1&1 in connection with the account for the applicable domain name, (2) populate the public WHOIS database with your name, primary postal address, e-mail address and/or telephone number as provided by you to 1&1, or (3) terminate your subscription to the Services . . . if any third party claims that the domain name violates or infringes a third party's trademark, trade name or other legal rights, whether or not such claim is valid."[9]

- **Domain.com, LLC**: "Domain.com expressly reserves the right, in its sole discretion and without any liability to you whatsoever, to suspend or cancel your use of the Service and/or reveal the Registration Information in any public WHOIS search or to any third party at any time without notice to you . . . [t]o resolve any and all third-party claims, whether threatened or made, arising out of your use of the Domain Privacy service, including without limitation, to avoid a dispute of any claim that the registered domain name violates or infringes a third party's trademark, trade name, or other legal rights."[10]

- **DomainIt, Inc.**: "You acknowledge and agree that DomainIt has the absolute right and power, as it deems necessary in its sole discretion, without providing notice and without any liability of DomainIt to Registrant whatsoever, to (a) reveal to third parties the contact information provided by Registrant to DomainIt in connection with the account for the applicable domain name, (b) populate the public WHOIS database with the registrant's name, primary postal address, e-mail address, fax number and telephone number as provided by Registrant to DomainIt, or (c) terminate Registrant's subscription to our Private Registration Service including but not limited to the following reasons:

  (i) for any violation of our Acceptable Use Policy;

  (ii) if DomainIt, in its sole discretion, determines that the administrative burden required to maintain the Private Registration Service on Registrant's behalf is unduly excessive;

  (iii) if any third party claims that Registrant's domain name violates or infringes a third party's trademark, trade name or other legal rights, whether or not such claim is valid;

  (iv) to comply with any applicable laws, government rules or requirements, UDRP, ICANN and/or Registry policies or requirements, subpoenas, court orders, requests of law enforcement or government agencies; or

  (v) if any third party threatens legal action against DomainIt that is related in any way, directly or indirectly, to the domain name, or claims that Registrant is using the domain name

---

[8] https://www.blacknight.com/acceptable-usage.html.
[9] http://www.1and1.com/TcPdr?__lf=Static.
[10] http://www.domain.com/legal/legal_domain.bml#domain-privacy-service.

registration in a manner that violates any law, rule or regulation, or is otherwise illegal or violative of a third party's legal rights."[11]

- **Moniker Privacy Services, LLC**: "You acknowledge and agree that Moniker Privacy Services, LLC has the absolute right, as it deems necessary in its sole discretion, to reveal to third parties, including to any UDRP or URS provider, the Contact Data provided by you to Moniker Privacy Services, LLC in connection with the applicable domain name and to suspend, cancel or terminate the Privacy Service if we reasonably perceive that . . . [t]he domain name violates or infringes a third party's trademark, trade name, or other legal rights or that you are utilizing the domain name to engage in activities prohibited by this Agreement."[12]

- **Whois Privacy Protection, Inc.**[13]: "If the IDP Domain(s) is (are) alleged to violate or infringe a third party's trademark, trade name, copyright interests or other legal rights of third parties . . . THEN You understand and agree that Backend Service Provider has the absolute right and power, in its sole discretion and without any liability to You whatsoever, to suspend the IDP Services, close Your Account, terminate provisionment of the IDP Services, list the information You provided in section 2 in the Whois output or provide the information You provided in section 2 to a claimant, resolve any and all third party claims, whether threatened or made, arising out of Your use of IDP Domain, or take any other action which Backend Service Provider deems necessary."[14]

- **Namecheap, Inc./WhoisGuard, Inc.**: "Namecheap reserves the right in its sole judgment and discretion to disclose your personal protected information, or instruct Whoisguard to disclose such information, in the event any of the following occur: . . . [i]f the Protected Domain(s) is (are) alleged to violate or infringe a third party's trademark, trade name, copyright interests or other legal rights of third parties."[15]

- **Web.com/Perfect Privacy LLC**: "Customer acknowledges and agrees that Web.com has the absolute right and power, in its sole discretion and without any liability to Customer whatsoever, to suspend the Services, close Customer's account, terminate provisioning of the Services, list Customer's personal information in the WHOIS output or unmask or otherwise provide the Customer's personal information to a claimant or other party to resolve any and all third party claims, whether threatened or made, arising out of Customer's use of the Domain Name or the Services, or to take any other action which Web.com deems necessary, in the event that (i) the Domain Name is alleged to violate or infringe a third party's trademark, trade name, copyright interests or other legal rights of third parties . . . ."[16]

---

[11] https://www.domainit.com/terms.html.
[12] http://www.moniker.com/legal/registration-agreement.
[13] P/P Service provider for Name.com.
[14] https://www.name.com/policies/idp.
[15] https://www.namecheap.com/legal/whoisguard/whoisguard-agreement.aspx.
[16] http://www.web.com/legal/terms-of-service/domains.aspx.