

~~DRAFT V.2~~ Subteam 4 Summary and Report [DRAFT 10-4-2015](#)

We are the “no comments left behind” subteam – the ones analyzing these comments for ideas, concepts, direction and guidance the WG may not have anticipated in our draft report or included in other parts of its analysis or within the specific structure of other subteams’ analysis. With ~~so many~~ [thousands of](#) comments submitted to the WG, there may have been ideas and concerns left unexplored and unanswered – and we hope to provide the WG with some insight and guidance on these issues.

Accordingly, we worked with materials from staff and our own review of comments to create a template that analyzed the comments for 7 categories of input:

- Category A – Issues involving Law Enforcement (e.g., procedures for access to customer data by LE)
- Category B – Methodology (e.g. periodic review/suggested processes after accreditation process is introduced)
- Category C - Other new or additional features that PPSAI WG should be consider
- Category D – Possible unintended consequences of disclosure of data for (1) registrants, (2) requestors, (3) providers (along with potential “fixes” in some cases)
- Category E – Additional reasons for/against the creation of the accreditation program
- Category F – Additional due process concerns possibly not already covered by other Sub Teams, and
- Category G - Other specific topics within WG scope possibly not captured by the above categories.

-

What follows is a summary of the Comments reviewed. For further details, please review the summary template of the comments.

- I. Category A – Issues involving Law Enforcement (e.g., procedures for access to customer data by LE)

We received a number of comments that respond to issues of Law Enforcement access to p/p Customer information. These responses address issues that we, the WG, have discussed. They include issues of jurisdiction and what jurisdictions Providers should be required to respond to (and not), scope of what is considered “law enforcement” for purposes of Reveal, and comments calling for the requirement of a court order or existing due process mechanisms prior to revealing data, including for law enforcement.

If and when the WG considers Reveal of Data by a) law enforcement and b) third parties other than intellectual property rights holders, we have a set of comments, concerns and guidance from commenters in the comments categorized as Category A.

As a Subteam, we recommend that the following follow-up actions take place by the WG:

In our Interim Report, we asked the public to comment on whether there is a difference if the ‘Requester is law enforcement vs. private party’ and we shared Annex E as a draft framework for private party requests. (Section 5.5, 4(b), page 35).

A number of commenters responded and provided input to the process by which Law Enforcement requests would be handled by Providers. Their input ranged from calls for court orders, to concerns over jurisdiction (and what jurisdiction the request is coming from), to concerns over LE and dissents in countries without many rights. Questions were raised about whether we (WG/ICANN) are staying within existing legal and jurisdictional rights with the proposals we are and will be making about LE and others.

We will not lay the full array here. If and when the WG take up the issue of LE requests, we ask it to pull pages 1-7 of our Template (table of comments).

- Category B – Methodology (e.g. periodic review/suggested processes after accreditation process is introduced)

Category B represents a range of commenters who ask the WG for post-implementation processes and reviews that check for success in implementation and confirm that additional problems have not been created:

Comments included:

- ; Ongoing Periodic reviews – P/P provide a refuge against “spam, harassment, and other third-party attacks” – a review would check whether p/p services after accreditation continue to do so and whether Reveal has created any problem in this area and whether it has “create[d] a chilling effect on online speech.”
- ; Accountability measures – are accountability measures and financial penalties, as adopted, being implemented and enforced? (See also, Category C, New Features, below).
- ; Has the Accreditation scheme, as ultimately adopted, been “built on a strong and robust contractual compliance enforcement system?”
- ; Is any accreditation model “integrated to the greatest extent feasible with the existing RAA so as to minimize accreditation and compliance costs.”

- ; Does the accreditation process, as adopted, take national laws into consideration and work within them them?
- ; Early Review – within a short period after adoption and implementation of the final rules, ICANN should implement a mandatory review process to survey customers to understand the impact of disclosures made pursuant to the requirements ICANN has imposed.

As a Subteam, we recommend that the following follow-up actions take place by the WG:

[The Subteam is split on how to move forward with the comments and recommendations in this section.](#)

[Some feel that:](#)

It is not clear to us how ICANN can survey customers of P/P services since their identities are not known. Instead, we propose ICANN establishing three data collection points so as to gather anecdotal comments for consideration in any future review process. These would include three outlets, one for each of providers, customers, and complaining parties to share their experiences with the accreditation scheme and compliance efforts in relationship. All comments could be submitted anonymously or contact information could be provided at the submitter’s discretion.

[Others feel that:](#)

[The WG should consider adoption of mandatory review processes to ensure that:](#)

- a) [In the short-term \(soon after implementation of PPSAI recommendations\), check to see that new rules are clearly and effectively communicated to Customers, Requestors and Providers, and](#)

[In the longer term, work with the Customers, Requestors and Providers to check for unintended consequences and inadvertent problems \(of the types pointed out by commenters\) and formulate ways to avoid them.](#)

- Category C - Other new or additional features that PPSAI WG should ~~be~~ consider

Comments included:

- ; Notification of ICANN Compliance about a Reveal or Publication breach by P/P Provider.
- ; Clarification of the accreditation and accountability processes, e.g. “Would like to see privacy/proxy services obligated to comply with the specifications applicable to

registrars/resellers/affiliates under the 2013 RAA” and the accreditation scheme “must be built on a strong and robust contractual compliance enforcement system.”

- ; Penalties for any array of violations:
 - For Requestors who would Reveal the data inappropriately
 - For Providers who would Publish the data inappropriately
 - For Providers who do not respond to demands for Reveal appropriately.e.g., “The success of the recommendations depends on strong implementation of accountability measures such as revocation of accreditation and financial penalties.”
- ; Making the language of our WG recommendations and procedures *much easier and more understandable for everyone who will be directly impacted*: “State legislation is crystal clear by comparison. Please reduce the amount of incorporation by reference,

Other comments in Category C asked us to:

- ; “look to established policies around disclosure that are already used by some country code managers, such as CIRA, who run the Canadian (.ca) country code” presumably to see how these policies handle similar issues to the ones we are evaluating.
- ; Look to international human rights standards
- ; Note the lack of separation of “online business presence from personal information, in some cases for cost reasons”
- ; Recognize commercial uses of p/p, including: “new product launches, business competitors, pre-launch websites”
- ; Note the impact that once “personal details have been made known either to an individual requestor or more broadly published,” the damage is done, therefore:
 - There should be compensation for the damage, and
 - Notification of ICANN Compliance when such a breach takes place.
- ; Providers should “maintain and publish statistics on the number of Publication and Disclosure requests they receive, as well as the number of instances in which those requests are honored.”
- ; WG should create a specific “retention period” for data revealed to a third party, and incorporate this into the disclosure procedures.
- ; Request for the transfer of personal identifiable data (PII) outside of the EU (and presumably other countries with national data protection laws, such as Japan and S. Korea, “must be met with evidence of compliance with the directive...” including controller and technical security safeguards for once the information is received.

As a Subteam, we recommend that the following follow-up actions take place by the WG:

--

We recommend that the WG consider some new features recommended by commenters, such as:

1. ~~require~~**Require** ICANN Compliance to develop a specific framework to accept and investigate notifications of breach of accreditation standards leading to improper reveal or publication, or improper refusal to reveal / disclose. ICANN Compliance can then enforce its contracts in the usual way when a breach has been identified.
2. Consider monetary damages or other penalties for ~~repetitive~~ abuses of the reveal/disclosure process.
- ~~3.~~ Retention of data timeframes – that the WG create limited retention period in response to national laws and direct and initial needs for the data.
- ~~4.~~
- 3.** ~~5.~~ Regarding the comment that Providers should “maintain and publish statistics on the number of Publication and Disclosure requests they receive, as well as the number of instances in which those requests are honored,” we suggest that the WG consider requiring ICANN to require ~~maintainence~~**maintenance** of such data for disputes and for periodic review processes. The WG may want to consider that the data should be aggregated **and/or** voluntary as we do not wish to create a market where nefarious users of the DNS find the P/P service least likely to reveal.
- ~~4.~~ **6.** Clarity throughout the entire document. We ask the WG and its co-chairs to carefully review the entire document for clarity. One commenter noted that the Interim Report was “a hall of mirrors” and strongly called on the WG to “reduce the amount of incorporation by reference...” As people will be reviewing and implementing this policy who are not lawyers and for whom English is not a first language, this complex policy should be crystal clear and easily accessible to all.

- Category D – Possible unintended consequences of disclosure of data for (1) registrants, (2) requestors, (3) providers (along with potential “fixes” in some cases)

There were many comments about unintended consequences. These included:

- ; Concerns about the impact of the policies on pricing for p/p services.

- ; Concerns about doxing and barring access to p/p services for financial transactions in connection with physical harm and harassment to women (including in a letter signed by 105 individuals, leaders in women’s communities and Internet communities, as well as 65 ~~womens~~women’s rights organizations).
- ; questions about whether the WG has fully considered the impact of policies on spam and on those who might be exposed to a) known abusers and b) “other unstable members of the public” through the policies WG is creating.
- ; Concerns about personal safety for dissidents or vulnerable populations.
- ; According to staff: concerns about Registrants who use pseudonyms and pen names for legal reasons (e.g. adult entertainers, erotica authors)
- ; According to staff: concerns over Data harvesting.
- ; If additional protections are created for speech, how can trademark owners still “effectively and efficiently police consumer confusion”
- ; Falsely in their name: How can trademark and copyright owners protect consumers against online fraud, pornography, phishing or malware perpetrated in their names?

there is exactly one circumstance under which involuntary Publication is appropriate: termination of the domain privacy provider's service. A properly-functioning and timely relay service, which is the fundamental function of a domain privacy provider, mitigates many situations that would otherwise require disclosure.

- ; The IPC raised the issue of whether or not attorneys who register domain names at the instruction of clients in their own name would fall into the accreditation scheme.

As a Subteam, we recommend that the following follow-up actions take place by the WG:

The WG should consider a process and criteria that will help Providers identify cases where “asylum” is necessary, for example, in cases where the content of the website is ~~purely~~largely political or religious, the P/P customer has requested the special protection and claimed an imminent non-commercial harm if the identity is disclosed, and there is no evidence submitted of any nefarious use of the domain name (e.g. phishing emails associated with what otherwise appears to be a pure political speech site).

The WG should discuss the issue of whether or not the accreditation scheme should result in the loss of the use of counsel to act anonymously for a domain name registrant. This raises significant issues related to the right of counsel.

In connection with the review mechanisms suggested above, the WG should consider mechanisms to permit rapid evaluation of whether such unintended consequences arise in a systemic manner and fixing them.

- Category E – Additional reasons for/against the creation of the accreditation program

Comments included:

Comments urged us to be careful in our WG work, e.g.,
; the loss of privacy is irreversible and should be guarded against.

Comments urged us to ban p/p services:
; Keep it simple: Just ban P/P services totally.

Comments urged us not to pursue accreditation and let the current marketplace dictate its own terms, e.g.:

- ; ICANN risks losing the confidence of the people if it enacts the proposed policies.
- ; Please simply discontinue the WHOIS database
- ; Abandon accreditation entirely
- ; This sort of accreditation/verification/enforcement activity is outside ICANN's scope and expertise.

As a Subteam, we recommend that the following follow-up actions take place by the WG:

~~We believe that~~As a subteam, we disagree as to whether the WG has addressed this concern adequately to date and some subteam members submit, as per recommendations above, that guidelines for implementation and post-implementation review are critical to combatting issues and concerns.

- Category F – Additional due process concerns not already covered by other Sub Teams, and

Comments included:

~~Comments included:-~~

- ; “Everyone deserves the right to privacy.
- ; The many comments about Law Enforcement requests and court orders prior to responding them.
- ; Concern that the WG may be allowing Third Parties to bypass Existing due process processes:
 - ⊖ Extraterritoriality: no response to extraterritorial requests absent “clear proof that the allegation of illegality is a) illegal in the country in which the domain name is registered and b) supported by existing evidence. Such a requirement will avoid the clear violation of Freedom of Expression and Free Speech”

As a Subteam, we recommend that the following follow-up actions take place by the WG:

Many of the Due Process comments in this category were part of comments that also fit into other categories. The conclusion that many of us in the subgroup seemed to draw is that the concerns raised by commenters might be addressed by major changes (or minor tweaks) to the due process work of the Accreditation Program.

The WG should also consider which law it deems should apply to the Request: the law of the P/P customer’s location, the law of the P/P provider’s location (likely the law mentioned in the agreement with the customer, the law of the location of the aggrieved party. ~~Requestor-~~ For trademark and copyright issues, there may be multiple options due to international operations. For LE issues, the impact of extraterritorial requests (which may invoke an allegation not criminal in the jurisdiction of the provider or customer), should be reviewed when the WG takes up the issue of LE requests.

- Category G - Other specific topics within WG scope not captured by the above categories.

Comments ~~included~~include:

- ; Clarity: Asking the WG to be much, much clearer as we set out our requests, requirements, policies and procedures -- State legislation is crystal clear by comparison. Please reduce the amount of incorporation by reference, especially in cases where the terms are neither defined.
- ; Asking WG to further evaluate what happens when p/p information becomes subject to spam or other types of violation – what type of action might a “website owner” take “against ICANN for the monetary damages suffered to the website owner as a result of ICANN's denial of their WHOISGUARD domain”

- ; No existing privacy/proxy service could function under the standard called for by [respectyourprivacy.com];
- ; On the [call by savedomainprivacy.org for “verifiable evidence of wrongdoing”], the report contemplates that P/P Providers will only be required to disclose P/P Customer contact details when presented with “verifiable evidence of wrongdoing”.
- ; No existing privacy/proxy service could function under the standard called for by [respectyourprivacy.com];
- ; On the [call by savedomainprivacy.org for “verifiable evidence of wrongdoing”], the report contemplates that P/P Providers will only be required to disclose P/P Customer contact details when presented with “verifiable evidence of wrongdoing”.
- ; Asking what percent of p/p are used for illegal data?

Some nice comments to note in passing include the ones thanking us for our work and the opportunity to comment.

As a Subteam, we recommend that the following follow-up actions take place by the WG:

The WG should consider having a public facing FAQ or other document designed (by some one who knows how to design them rather than by the WG) to make our conclusions readable by the average person who is not familiar with “ICANN-speak.” This will ultimately eliminate confusion leading to extreme reactions to the final report.

Consider the whole of the final report in context to review, assess (and correct as needed) whether “due process” has been incorporated at every stage of the processes being created.

~~Consider the~~ [Also, consider](#) concerns raised about the petitions.

Document comparison by Workshare Compare on Monday, October 05, 2015
12:59:15 PM

Input:	
Document 1 ID	file://H:/Vicky-Subteam 4 Report draft vfs 10-2-15.doc
Description	Vicky-Subteam 4 Report draft vfs 10-2-15
Document 2 ID	file://H:/Kathy-Subteam 4 Report - 10-4-2015 for first WG Review (00837771xB3D1E) (2).doc
Description	Kathy-Subteam 4 Report - 10-4-2015 for first WG Review (00837771xB3D1E) (2)
Rendering set	Standard

Legend:	
<u>Insertion</u>	
Deletion	
Moved from	
<u>Moved to</u>	
Style change	
Format change	
Moved deletion	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	21
Deletions	20
Moved from	0
Moved to	0
Style change	0
Format changed	0
Total changes	41