

**Privacy & Proxy Services Accreditation Issues (PPSAI) PDP Working Group
 Sub Team 4 – No Comment Left Behind
 Public Comment Review Tool for Sub Team Identifying & Allocating Additional Topics for Review
 22 September 2015**

CATEGORIES:

- 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 consider adopting
- Category D – Unintended consequences of disclosure of data for (1) registrants, (2) requestors, (3) providers (and hopefully ways WG might address them)
- Category E – Additional reasons for/against the creation of the accreditation program
- Category F – Additional due process concerns not already covered by other Sub Teams
- Category G - Other specific topics within WG scope not captured by the above categories

Note: The following table groups all comments reviewed to date according to the above-listed categories; the numbering therefore will appear out of order as this reflects the numbering from the original document, which listed all comments in general chronological order of submission.

#	Recommendation / Comment	Category	Additional Comments/Notes	Who / What ¹	Possible WG Response	WG Response/Action
46	Do not change anything, you need a warrant, I need privacy	A		Joe	Appears to be subsumed within those template comments calling for court orders before reveal or publication; no separate action.	

¹ A hyperlink to the actual comment has been provided where the commenter sent his/her input directly to the ICANN Public Comment Forum. Those comments without associated hyperlinks represent comments submitted by responders to the WG’s online question template, under a specific heading in that template for “Additional Comments”.

52	<p>I urge you to respect interne users rights to privacy and due process. Please let me explain why WHOIS Guard is required, from my personal perspective. The principal reason is the home address. I have a small blog, but why do I have to put my home address on the whole world just because I run a blog on a domain? Why do I have to open the door of harassment just because I have a website?</p> <p>-- If people know my home address, they can physically do almost anything if they do not like my website.</p> <p>Especially in my country Bangladesh, there is a tradition of killing the blog author if some group just do not like what blogger said. For</p>	A		Shahed Ahmmed	<p>Consistent with other comments demanding reveal/publication by Court order only; no specific action, other than remaining sensitive to the politic consequences of relay/publication.</p>	
----	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	--	---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

<p>example, one blogger, Avijit Roy, was murdered recently because some Islamic activists did not like his blog. See: https://en.wikipedia.org/wiki/Avijit_Roy-- How do you define whether a site is commercial or not? I am planning of placing adds on my blog, but not selling anything. Thereby, how can you classify whether it is a commercial or personal site? Putting adds on a website does not make it a commercial site, unless it sells something. -- And even if it is a commercial site, it may need privacy. Yes, I know that big commercial firms do not need Whois protection. But what about small business owners? Some of them definitely need this protection. For example, if I sell my</p>					
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--

	<p>books from my own website that also hosts my blog, do I have to disclose my home address?</p> <p>-- Besides, I use Whois privacy because otherwise spammers will know my personal email address, and I have to spend substantial amount of time and energy every day to find out which mail is spam and which is not. As I mentioned, I have to do this checkup in my inbox on a regular basis. As you see, if you prevent domain owners from using WhoisGuard protection, it will create more problems than that it will solve. Therefore, disclosure of Whois information should only be made upon a court order.</p>					
53	The privacy and rights of	A		Adam Miller	Appears to be subsumed in	

	regular internet users are the greatest concern above all others such as IP rights and law enforcement.				template comments; no specific action.	
56	All domains should be able to use privacy services. Only LEA should be able to request publication or disclosure.	A		Sebastian Brossier	Suggests only law enforcement should have access to disclosure; no specific action.	
84	11,000+ comments of individuals originating from the Respect our Privacy website which each stated: “-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”	A, F	Current Annex E, titled <i>Revised Illustrative Draft Disclosure Framework for Intellectual Property Rights-holders</i> . Where are the LE-framework comments being stored for future work by the WG?	11,000+ individual comments submitted to the WG from the Respect our Privacy website.	If and when an equivalent of “Annex E” is created by the WG for Law Enforcement (LE) requests, this request for court order as the definition of “due process” must be considered.	

85	<p>“Accredited privacy and proxy services should not be required to either Publish or Disclose registrant contact information other than when required by relevant law and utilizing relevant legal procedures.”</p> <p>Also,</p> <p>“Privacy and proxy providers should not be required to present, process or honor any forms required by ICANN in place of relevant legal processes. Similarly, frameworks for responses to both Intellectual Property Rights-Holders and Law Enforcement should be replaced with a general requirement for privacy and proxy services to</p>	A, F	Waiting for LE/Reveal discussion	Google; Senior Google Trademark Counsel	If and when an equivalent of “Annex E” is created by the WG for Law Enforcement (LE) requests, Google’s request for review only “when required by relevant law and utilizing relevant legal procedures” must be considered.	
----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------	----------------------------------	-----------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

	operate in accordance with relevant law.”					
86	“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.”	A, F	Waiting for LE/Reveal discussion	Muhammed A (Submitted with Save Domain Privacy petition) wrote:	For consideration if and when WG evaluates an equivalent of “Annex E” for Law Enforcement (LE) requests.	
87	“We use domain name privacy to keep our personal information "personal". I do not want our information released without a court order.”	A, F	Waiting for LE/Reveal discussion	Clay H (Submitted with Save Domain Privacy petition):	For consideration if and when WG evaluates an equivalent of “Annex E” for Law Enforcement (LE) requests.	
88	“In order to comply with human rights standards, any rules forcing PPSPs to disclosure or publish user data upon request	A, F	Waiting for LE/Reveal discussion	Access Now	For consideration if and when WG evaluates an equivalent of “Annex E” for Law Enforcement (LE) requests.	

	must comport with legal due process and require a court order or a subpoena for its execution whether the request is a private party or a law enforcement authority.”					
89	“[T]he framework for processing intellectual property complaints set out in Annex E is concerning because it allows for the circumvention of existing due process. The proposed framework would essentially allow a copyright owner to bypass existing DMCA processes to obtain private registrant information. Establishing an accreditation program that allows any one party (i.e., intellectual property owners) to bypass due	A, F	Bypassing DMCA is a problem; should reveal requests only apply to third parties with trademark concerns?	Endurance International Group	For consideration if and when WG evaluates an equivalent of “Annex E” for Law Enforcement (LE) requests. For consideration re: scope of Annex E.	

	<p>process opens the door for other parties to do the same (e.g., law enforcement agencies). Further, the proposed framework ignores existing jurisdictional and legal rights applicable to registrants and privacy providers around the world.”</p>					
10	<p>[W]ithin 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.</p> <p>In addition, ICANN should seek to assess on a continuing basis whether these rules create a chilling effect on</p>	B		<p>CDT/Open Technology Institute/Public Knowledge: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11431.html</p>	<p>Consider adding the following criteria in any follow-on / periodic review of the PPSAI standards:</p> <ul style="list-style-type: none"> - p/p customers are made aware of information about the standards for disclosure <p>The comments also suggest reviews on whether the rules “create a chilling impact on free speech”. If we were to consider this, we would need to define what this means for review/measurement</p>	

	online speech.				purposes.	
26	This whole policy is totally stupid. Put it in the trash and start all over again.	B	Methodology, Scope	Liam	Evaluate if continuing with current policy effort is supported by all stakeholders.	
11	Any accreditation process or ICANN rules must take national laws into consideration.	B, C		1&1 Internet SE: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11333.html	I believe this may already be covered, either expressly or impliedly.	
2	The success of the recommendations depends on strong implementation of accountability measures such as revocation of accreditation and financial penalties.	B, C, E (for)	Support accreditation process as a measure of accountability.	BC: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11451.html	Consider express measures for failure to comply with accreditation standards	
3	[An accreditation scheme] must be built on a strong and robust contractual compliance enforcement system.	B, C, E (for)	Support accreditation process as a measure of accountability.	MPAA: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11389.html	Consider express measures for failure to comply with accreditation standards	
82	f) Spam, scams and identity theft (e.g. phishing attempts)	D, F, B	Question: have we put enough procedures into place to prevent spam, scams,	Many commenters (according to staff report to subteam)	Has the WG put sufficient procedures in place to prevent spam, scams and identity theft? Do we need to add more? Should there be	

			identity theft and phishing? Can we test later to ensure that an accreditation program “did no harm?”		reviews of the work to ensure that an accreditation program does not open a path to future problems?	
4	Accreditation model for P/P service providers should be integrated to the greatest extent feasible with the existing RAA so as to minimize accreditation and compliance costs.	B, E (for)		ICA: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11377.html	Keep Annex E to	
22	Any changes in Whois Privacy requirements must be considered against the backdrop of previous Whois reform initiatives, because at the end of the day, it's the end-user Registrants who have to adjust to functioning under the combined effect of all of these new policy modifications. ICANN has thus far implemented two	B, E, G	Excellent detailed and informed comment that we should take the core concepts of to the WG whole.	Mark Jeftovic (EasyDNS)	TO BE TAKEN TO WG LEVEL	

	<p>policies around Whois reform which should be considered failures in that they do not accomplish their stated goals [i.e. WDRP and WAP]. Change is certainly needed but it needs to be genuine change, a ground up rewrite of the entire protocol.</p> <p>Recommend:</p> <ol style="list-style-type: none"> 1) The entire Whois Privacy Policy revisions should be tabled until the entire Whois database is re-engineered as the next generation RDS 2) That a guiding principle of any future RDS Working Groups should incorporate legal due process and end-user, that is Registrant control over their own data records, complete with automated mechanisms to alert 					
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--

	Registrants when inquiries are made into their records, what the purpose of those inquiries are and allowing Registrants the ability to withhold disclosure (except in cases of overt net abuse or where a law enforcement agency is pursuing a legitimate investigation subject to a valid warrant).					
69	Spam, harassment, and other third-party attacks are too numerous for WHOIS to operate as intended; in fact, the presence of privacy and proxy services is largely due to this vulnerability. ICANN should not seriously restrict the availability of these services, <i>nor make rules that impair their ability to adapt to changing conditions</i> , at least as long as WHOIS data is	B (Periodic review), E, G (Other) concerns about ability of accreditation system to adapt to changing conditions .	Question for WG: have we left sufficient room for P/P Providers to change and adapt to “changing conditions?” Also, have we taken sufficient steps to ensure that 3 rd parties seeking data for “malicious purposes” can be blocked? This comment	Jason Burns	WG should review existing proposed policies to ensure that spam, harassment and other third party attacks are avoided as much as possible. WG should create a periodic review of the policy after adoption to ensure that “changed conditions” do not in the future allow for revealing of data for “malicious purposes.”	

	available to third parties who might want contact information for malicious purposes. [Emphasis added.]		appears to call for both a review of proposed policies, and a periodic review of what is ultimately adopted to determine over time whether changes are needed to made to policies to accommodate “changed conditions and newly-discovered patterns of malicious conduct.			
9	[S]uggest that the Working Group 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.	C		Blacknight: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11337.html	Unfortunately, no express recommendations made, and I wasn’t able to access the disclosure noted to see what the additional suggestions might be.	
12	The most protective approach towards user privacy must be adopted in the case of any gaps between domestic	C		Access Now: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11327	The comments do not specify what is the gap in question that must be reconciled. In any event, such considerations must be	

	legislation and international human rights standards.			.html	balanced against the rights of others that are affected by the relevant behavior at issue.	
Unnumbered in Staff summary	This document is a hall of mirrors. State legislation is crystal clear by comparison. Please reduce the amount of incorporation by reference, especially in cases where the terms are neither defined.	C		Michael Ho	Is there a final report format that would work better for the end user?	
79	Many comments submitted which noted the lack of separation of online business presence from personal information, in some cases for cost reasons and especially for home-based or small businesses (e.g. online shop owners, freelancers, self-employed persons, writers)	C	Seek understanding of and protection for those who personal data and business data overlap, e.g., home-based and small businesses.	Many commenters (according to staff report to subteam)	Do we need new features to better protect those individuals whose personal data is fused with their business data, e.g., "online shop owners, freelancers, self-employed persons, writers."	
83	Many commenters wrote of commercial needs for	C	Have we protected commercial needs		Do WG policies fully protect business engaged in new	

	privacy of domain information, e.g. new product launches, business competitors, pre-launch websites		for p/p such as new product launches, protection from business competitors and privacy of pre-launch websites?		product launches and pre-launch pre-launch websites from misuse of reveal procedures by business competitors?	
90	<p>Once personal details have been made known either to an individual requestor or more broadly published, the damage has been done. Depending on the facts of each case, there may be compensation for damage caused by a breach of contract thru civil means.</p> <p>ICANN Compliance must be notified since such breach may also amount to a breach of the Specification.</p>	C	<p>Notify ICANN Compliance when Reveal breaches are found.</p> <p>Find a way to compensate victims a breach of contract.</p>	ALAC: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11473.html	WG advised to consider: + compensation for breach to Customer; + notification to ICANN Compliance of all breaches.	
1	Would like to see privacy/proxy services	C, E (for)		ALAC: http://forum.icann.org	Include this requirement as part of the accreditation	

	obligated to comply with the specifications applicable to registrars/resellers/affiliates under the 2013 RAA.			org/lists/comments-ppsai-initial-05may15/msg11473.html	standards.	
6	<p>ICANN community should consider focusing on work that better and more directly addresses underlying issues rather than devoting more time to WHOIS-related work.</p> <p>Privacy and proxy 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.</p>	C, E (against)		<p>Google: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11370.html</p>	<p>Consider suggestion that p/p services provide data on disclosure requests</p> <p>Consider suggestion to look at additional, non ppsai mechanisms to address phishing/pharming. However, the fact that other mechanisms to address these issues are available doesn't discount the work or need for PPSAI.</p>	
23	[D]isclosure framework does not specify the retention period of information transferred to a third party. We recommend that a	C (multiple new features suggested),	New Features recommended: (i) WG define and adopt specific retention	Cyber-Invasion	<p>WG should consider whether to:</p> <p>+ define and adopt specific retention period for Customer data transferred to</p>	

	<p>specific retention period should be developed by the working group and incorporated into the disclosure framework.</p> <p>For registrants who are located within the European Union (EU) transferal of registration data between parties constitutes a transmission of Personally Identifiable Information as per the EU Data Protection Directive 95/46/EC1, as such for reveal requests where the address of the registrant is located within the EU the requestor must be able to provide evidence of compliance with the directive, including but not limited to identification of the Data Controller and technical security safeguards for the information once</p>	<p>F (due process on extraterritorial requests)</p>	<p>period for Customer data transferred to a third party.</p> <p>(ii) WG require encryption for transfer of personal data</p> <p>(iii) WG evaluate European data protection laws and consider requirement Providers to show “proof of compliance” with transfer of data provisions.</p> <p>(iv) WG should limit extraterritor</p>		<p>a third party;</p> <p>+ require encryption for transfer of personal data</p> <p>+ evaluate European data protection laws and consider requiring Providers to show “proof of compliance” with transfer of data provisions.</p> <p>+ limit extraterritorial request “absent clear proof that the allegation is illegal in the country in which the domain name is registered and supported by existing evidence.</p>	
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

	<p>received. For requestors located in the United States a Safe Harbor certificate should be provided to the provider to demonstrate compliance.</p> <p>[R]ecommend that the working group consider the mandatory use of encrypted communications channels during the transmission of all PII regardless of the jurisdiction of the registrant and requesting party as a matter of technical best practice.</p> <p>WG final recommendations must ensure that extraterritorial requests are not facilitated absent clear proof that the allegation of illegality is a) illegal in the country in which the domain name</p>		<p>ial request “absent clear proof that the allegation is illegal in the country in which the domain name is registered and supported by existing evidence.</p>			
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

	is registered and b) supported by existing evidence. Such a requirement will avoid the clear violation of Freedom of Expression and Free Speech ...					
7	Privacy/proxy services can be priced out of existence requirements to validate data, and requirements for the registrars to pay for delivery of legal documents to the beneficial owner of the registration.	D		Stephanie Perrin: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11359.html	No data was provided to support this proposition. Either it should be discarded or we should ask for evidence to back it up.	
15	[R]ecommend that ICANN revisit its own findings from 2013 and move toward making WHOIS privacy the default for everyone in light of stalking, doxing and swatting concerns for women and LGBT communities, among others.	D		OAPI: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11319.html	The comments appear to be addressed to whois generally, and not to the disclosure / reveal standard requirements set forth in the PPSAI.	

28	I use privacy to assist in limiting my exposure to spam, as well as to feel secure when operating online due to the knowledge that my abusive father (and other unstable members of the public) are less likely to track me down. In the event that the option to make my contact details privacy is removed, I have a very real fear for my life. I see this as a major concern for all victims of domestic violence or bullying, along with any social service that seeks to assist those in such situations, especially when seeking financial independence.	D	Case of potential impact	James	Ensure that we give a strong rationale in our final proposal as to how we are mitigating these risks.	
49	Please stop being the puppet of large business interests. While it is inconvenient for them to not be able to violate the privacy of everyone who	D		Private	Raises concerns about life and death consequences for marginalized people of relay or publication. Raises concerns about the effects on political speech; Discuss	

	<p>threatens their 20th century business models, this a matter of life and death for those of us who engage in unpopular political speech. All frameworks for defining and violating privacy will be abused. A momentary leak of private information means death for atheist bloggers in Bangladesh, death for political dissidents in Russia, and death for transgender individuals in the United States. Please do not kill us because a record company wants to marginally improve how efficiently they exploit some dumb kids with music instruments.</p>				<p>again how site content might affect the decision to relay or publish. How can/should providers determine what complaints appear designed to stifle free speech and which customer responses raise real issues of free speech (in other words, how to allow for online “asylum” while not making the assertion of the need the catchall to ensure no disclosure even where there is no real need. Also, how to allow providers to balance their need to not be involved in illegal speech (i.e. there is no universal first amendment).</p>	
66	<p>Online privacy needs To be taken as seriously as medical and lawyer secrecy.</p>	<p>D – Unintended Consequences (serious</p>	<p>Commenter calls for WG to raise the level for disclosure to the level of a doctor or lawyer disclosing</p>	<p>Uncredited</p>	<p>WG should review the specific consequences that might arise for a disclosed party and consider raising the due process protections for Customers to the level of</p>	

	It must be made clear that a Chinese dissident, or a Saudi blogger face death penalty or 1000 whip lashes when privacy is breached.	ones); Also overlap with Subteam 3's work, F	information (often protected under special health care laws or attorney-client privilege). That is a very high standard and one being suggested to the WG with a clear view of the individual cost when a dissenter's name and address are disclosed. Runs to both Reveal and Publication.		medical and legal confidentiality and protection.	
77	Many comments received by the WG sharing deep concern about Doxing/SWAT-ing and concerns about physical safety (e.g. stalking, harassment or where registrant is in an unsafe or threatening location)	D, F	These comments makes clear the cost of errors in our policies will be very high!	Many commenters (according to staff report to subteam)	WG urged to keep in mind <i>physical safety considerations</i> of disclosure for Doxing and Swatting, stalking and harassment when an individual's location is revealed: (i) has the WG put enough procedures into place to prevent inadvertent or unnecessary Reveals or Publications?	

78	Many comments received by the WG about Anonymity Needs for certain individuals and organizations (e.g. those serving at-risk communities, targeted minorities, women and political and religious activists)	D, F	These comments urge the WG to keep in mind the many important uses of p/p registration, and question whether there are enough protections to avoid exposing individuals, organizations and religious institutions who merit protections.	Many commenters (according to staff report to subteam)	Has the WG adopted sufficient procedures and protections to protect “at-risk communities, targeted minorities and political and religious activists?” What more can we do to help the many, many worried commenters who we heard from?	
80	Many commenters expressed deep concern about Registrants who use pseudonyms and pen names for legal reasons (e.g. adult entertainers, erotica authors)	D, F	Question: have we put enough procedures into place to prevent inadvertent or unnecessary Reveals or Publications for those who legitimate use pseudonyms and pen names?	Many commenters (according to staff report to subteam)	What processes can the WG adopt to ensure that the next George Sand or Mark Twain are able to protect their pen names and pseudonyms, even when their copyright or trademark is informally challenged in a Reveal request?	
81	Many commenters	D, F	Question: have we	Many commenters	Has the WG put enough	

	expressed concern to the WG over Data harvesting.		put enough procedures into place to prevent data harvesting now and in the future?	(according to staff report to subteam)	procedures into place to prevent data harvesting? Do we need to add more?	
14	ICANN's accreditation standards for P/P Providers should: 1) limit the availability of P/P Services to those circumstances when a compelling interest in preserving a registrant's anonymity justifies the increased risk to consumers that P/P Services create; and 2) in those cases, implement mechanisms to mitigate that increased risk by ensuring that trademark owners can still effectively and efficiently police consumer confusion.	D, G		INTA: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11303.html	Consider supporting alternative that calls for increased likelihood of disclosure in cases involving financial commercial transactions.(TBD if this belongs here or should be referred to subteam 2.)	
62	All I care about is Being spammed. If Our email is Publicly available Someone will write	D (unintended consequences) &	This comment seems applicable to both the WG when it thinks about: a) publication and	Ian McNeil	Consider with similar unintended consequences comments and review policies to ensure problems such as spam being avoided.	

	<p>a bot to harvest and sell this and we will be buried In spam mails Meaning any Mail to this address Will be treated As spam and ignore, completely defeating the whole purpose of it.</p>	G (other topics)	<p>the globally available state of Customers' emails when/if they are made available to the world</p> <p>b) notice prior to publication so that the Customer knows and can anticipate spam and other problems before the start to arise.</p> <p>c) the existence and value of privacy/proxy services.</p>			
5	<p>p/p service providers must be accredited in a way that ensures that trademark and copyright owners can protect consumers against online fraud — or pornography, phishing, malware, etc. — that is falsely perpetrated in their</p>	E (for)		<p>Turner Broadcasting: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11152.html</p>	<p>Support for procedures to guard against harm to consumers from bad acts perpetrated by third parties in the rights holders names</p>	

	names.					
16	Cost of Proxy/Privacy Services must remain affordable.	E, potentially against	Are we addressing this in our discussion of who bears the cost of physical contact? Will accreditation require an increase in P/P Provider costs?	NCSG	Analysis with P/P Providers insides (and possibly outside) of the WG about whether and what types of costs the accreditation program proposals would imposed on the P/P service and what costs it might add to registration?	
17	Publication is much simpler [than disclosure]. Publication is impossible for an independent domain privacy provider. It can only be performed by the registrant, the registrar, or the registry. Keeping that in mind, 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	E	Suggestion that a relay service is sufficent.	Jeff Wheelhouse	Evaluate weather we are giving sufficient weight to the initial relay procedure as part of the WG's deliberations.	

	privacy provider, mitigates many situations that would otherwise require disclosure.					
18	<p>In general, privacy of sensitive personal data is desirable for domain owners (or “registrants”). Therefore, the PPSAI-WG must adopt the overarching principle that privacy is desirable for domain registrants, and that mandatory disclosure of a registrant’s personal information must always be a narrowly-circumscribed exception to the general rule in favour of privacy.</p> <p>We recommend that registrars be mandated to publish statistics about the number of disclosure requests they receive, and also the</p>	E	Suggests that privacy should be the ‘default’ and that we may be too broad in our allowances for disclosure.	Shardul Amarchand Mangaldas (Adv. & Solicitors, India):	<p>Is the WG maintaining privacy as the default in all aspects of our framework?</p> <p>Evaluate monitoring/statistics disclosure in the vein of a transparency report as part of the accreditation regime.</p>	

	number of such requests they comply with.					
30	IP, trademark and copyright infringement is on everyone's mind because the companies that profit from those activities are spending large amounts of money to make sure it is. The same was true of the publishing industry when libraries first started to appear. I think many would find it hard to argue that libraries have been good for mankind. Here too the publishing companies have flourished. I think the same will be said when history looks back on this period of time. However the loss of privacy is irreversible and should be guarded against. Individuals lack the resources to stand up to the giant corporations that want all of their	E	Appears to not support Annex E/Overall Framework.	Dr M Klinefelter	Are we meeting the publics privacy needs in Annex E and the accreditation framework as a whole?	

	information - so they can profit from it. I believe the internet should not be for the profit of a few companies but for the sharing of ideas and betterment of mankind overall. Please protect the privacy of the individual.					
47	Hosting own domain with some required software is a good defense against online profiling for various purposes. The infrastructure in place has been good enough, there is from my point of view nothing to fix. Why would ICANN try to stop that??	E		Harish	Appears to be consistent with other comments calling for no change to the current system; No separate action needed.	
48	These regulations might trigger the end of ICANN, it makes domain holders conscious of the urge of looking for an alternative system of url resolving	E		D. Miedema	No specific action other than continued awareness that ICANN must balance the concerns of various stakeholders in order to avoid fracture.	

50	Keep it simple: Just ban P/P services totally.	E		Gary Miller	Believes simplicity is a higher good than maintaining current or establishing revised P/P framework; No specific action other than for WG to remembers that there are users who would prefer that there be no P/P services allowed at all.	
55	ICANN risks losing the confidence of the people if it enacts the proposed policies.	E		Darin McGill	No specific action other than continued awareness that ICANN must balance the concerns of various stakeholders in order to avoid fracture.	
57	Individuals need to be protected. However, it is better that these are done at the local level (e.g., my .co.uk are protected by my UK level registrar; I simply declare myself as an individual) – so if that was done across the board, then there would be no need for third party privacy services...and hence a lot	E		Michelle Knight	Suggests that each registrant be afforded the privacy protections of their individual jurisdictions; Consider the feasibility of implementing such a system where it is the registrant's location that drives requirements rather than the registrar location and/or ICANN policy.	

	of grief would be saved.					
58	Please simply discontinue the WHOIS database.	E		Andrew Merenbach	Calls for the abolition of WHOIS (which would make P/P Accred. Moot); No specific action.	
59	Abandon accreditation entirely	E		Jawala	Calls for the abandonment of the P/P process; No specific action.	
60	Get out of the P/P business. Kill the accreditation program.	E		Aaron Dolton	Calls for the abandonment of the P/P process; No specific action.	
61	“Just... Go away and leave individuals alone, please.”	E, against accreditation program	Appears that the individuals does not want the creation of an accreditation system	Stephen Black Wolf	Consider the overall number of comments that ask for accreditation system to be deleted vs. those seeking to create and develop it.	
63	KEEP MY PRIVATE INFORMATION PRIVATE! (emphasis in original)	E, No accreditation; no disclosure ?		M.B.		
64	My privacy is more important than your right to know my personally identifying information.	E, no accreditation; no disclosure		Belinda van Sickle		
67	“ imposing these sorts of	E, against	A call to let the	Mario Hellmann	Should be considered with	

	requirements onto proxy/privacy service providers may threaten to only further disorganize and disintegrate the system in place. These practices and their implementation are best left to the domain registrars themselves, as it is both in their interest and the interest of their customers.	accreditation program	existing p/p marketplace work without intervention by ICANN.		similar comments.	
68	Please let the existing system continue. We need the right to privacy and right to free speech preserved. There is absolutely no use in these new processes and in turn stealing users of their freedom. We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves	E, against accreditation program	No accreditation program	Anand S.	Should be evaluated with similar comments.	

	are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.					
71	This sort of accreditation/verification/enforcement activity is outside ICANN's scope and expertise.	E, no accreditation program	Calls into question ICANN's scope and mission	Gregory Antonellis	It is incumbent on the WG in our Final Report to more clearly address how this P/P accreditation process will fall within ICANN's scope and mission.	
72	I think the planned changes are foolish and would prefer that no changes occur.	E, no accreditation program		Aaron Holmes	Consideration by WG with similar comments opposing accreditation.	
75	Please abandon this ill fated attempt to assert control over something that will do more harm than help by enabling the "legitimate" authorities or violent people to seriously injure random people on the internet.	E, no accreditation program		Anonymous Turtle	Consideration by WG with similar comments opposing accreditation.	
20	1. When a website owner has been scammed or have had its personal information violated in a	G, E	Potential increase in WHOIS accuracy, potential additional costs to ICANN as a	Nathan Parker	Potential risk scenario to be developed to assess impact on ICANN costs as a result of the accreditation regime.	

	<p>way that would cause financial damage to the website owner, the website owner will need to seek legal action against ICANN for the monetary damages suffered to the website owner as a result of ICANN's denial of their WHOISGUARD domain privacy protection.</p> <p>2. Web hosting companies and/or web designers are going to have to begin "falsifying" WHOIS information in the database as a means to protect website owners' personal information. Doing so may be against ICANN's policies and/or against the law, but it is a measure ICANN will force web hosting companies and/or web designers into if it proceeds with this ruling</p>		<p>result of the accreditation framework</p>		<p>Assess potential impact on WHOIS accuracy as a result of accreditation regime.</p>	
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	----------------------------------------------	--	---------------------------------------------------------------------------------------	--

21	<p>The proposal to accredit providers of privacy and proxy services currently operating independently from the realm of ICANN is not an adequate or necessary and will likely result in a substantial financial and administrative burdens on ICANN, provider and end customers alike. The proposal to follow the path of accrediting these [proxy] providers essentially proposes a direct contractual relationship between the provider as a registrant and ICANN [and] introduce a new class of contracted parties and may therefore impact the GNSO structure in ways that cannot yet be foreseen.</p> <p>[Proposal of alternatives other than</p>	E,G	<p>Potential increase in legal costs to ICANN fas a result of accreditation.</p> <p>Suggestion of a non-accreditation regime.</p>	Key Systems	<p>Perform fact based analysis on non-accreditation options in place of an accreditation regime, can we meet our goals in a different and simpler manner?</p> <p>Suggest review of policy after fixed term with sunset clause if goals not met.</p>	
----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----	-----------------------------------------------------------------------------------------------------------------------------------	-------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

	<p>accreditation:] certification of compliance with policy requirements, adherence to a set of best practices or other means. Enforcement would be covered by modifying the requirements or registrars in the RAA and consensus policies when working knowingly with privacy or proxy service providers.</p> <p>[Suggest] extensive cost-risk-benefit analysis.</p> <p>We propose that any policy recommendation include a sunset term, with automated renewal of the policy recommendation to be dependent on an analysis of whether it has delivered on its intended benefits and whether it has led to</p>					
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--

	additional costs or issues not foreseen by the WG when it made the recommendations.					
8	<p>No existing privacy/proxy service could function under the standard called for by [respectyourprivacy.com] ;</p> <p>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”.</p> <p>[M]any 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</p>	G		<p>Coalition for Online Accountability: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11340.html</p>	<p>Consider the value of the respectyourprivacy.com comments in light of current practices and alleged inability of p/p services to function with such a requirement.</p> <p>Consider that both the report and one of the petitions use the same term “verifiable evidence” and the implication that when read together should those terms mean the same thing.</p> <p>Consider the validity of comments submitted under the respectyourprivacy.com and savedomainprivacy.com petitions in light of allegations of misinformation in the petition.</p>	

	should be evaluated in this context					
13	IPC would strongly support identifying [existing provider policies that ban some commercial usages] as a best practice for service providers at a minimum.	G		IPC: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11323.html	Consider supporting this alternative that recommends identification of current best practices for dealing with certain site engaged in commercial transactions. (TBD if this belongs here or should be referred to subteam 2.)	
19	It has been estimated that 15 - 25% of domains use privacy (see http://www.inta.org/Advocacy/Documents/November202009Whois.pdf), and this strikes me as a very large potential impact. Has any study been made as to what percentage of these domains may be hosting illegal data? Has any study been made into what percentage of domains which are *not* using privacy are hosting illegal data? Are there any numbers or statistics	G	Potential increase in WHOIS inaccuracy.	Brendan Conniff	Have we analytically assessed the potential impact on WHOIS accuracy?	

	which might suggest this proposal will actually have a positive impact on piracy, or is this simply an attempt to appease a special interest? Who will take responsibility for the damage this may do to the private sector, damage to a sector of the industry where innovation stands strong in light of a troubled economy?					
24	There should be a mechanism for Published Whois info to be protected from spidering or other automated scanning.	G	May be out of scope for this WG	Phil Crooker	The WG may suggest this is out of scope for this policy effort.	
25	If ICANN should be doing anything, it would be the verification of the administrative and technical *EMAIL* contacts. As an administrator, unless I want to forward it to legal, a home address is absolutely and utterly	G	Impact on WHOIS Accuracy	Edward Epstein	Suggest that the WG ensure we have looked at the interrelationship between WHOIS accuracy and P/P in sufficient depth	

	meaningless and unhelpful. A phone number is more helpful, but not always appropriate.					
51	I suggest the introduction of a new top level domain solely for personal rights purposes, like freedom of speech. Registering Domains under that TLD should be possible completely pseudonymous, without giving any contact details but a working email address. The commercial use of that TLD must be strictly prohibited, including any kind of advertising. Only strictly personal use by non-commercial individuals should be allowed.	G		Stephan Grunder	Suggests an anonymous, non-commercial TLD. It is not clear whether that is in addition to or in lieu of a P/P framework in other TLDs; Could we add a section on "other possible items to consider" that are not adopted by the WG necessarily, but keeps the idea alive?	
65	The voice of the IPC is way too loud in this proposal. This flies in the face of consensus and developing an internet	G- other		Arthur Zonnenberg	WG should evaluate whether a balance among all stakeholders in this PDP has been achieved? Is there more we should be doing?	

	everybody can use and enjoy.					
27	Please remember many individuals do some "commercial" work that is different from multi-national commercial operations.			John Lawrence	Addressed in other sub-teams work.	
29	WHOIS privacy should be maintained at all costs to protect commercially sensitive information, prevent a massive deluge of spam to domain owners. GoDaddy needs to relay ALL domain registration information to other sites, they are NOT a special case.			J Wilson		
54	Thank you for the opportunity to comment on our work.			Vanda Scartezini	Nice comment thanking ICANN for the public comment period; No action.	
70	Privacy is a fundamental human right, a single organization can't decide who "deserves" that right, as everyone does.	For Subteam 2		Lucas Stadler	A strong response against limitations on p/p access.	
73	Tx for comments					

	opportunity					
74	Obscenity					
76	For the reasons outlined above, the OAIC does not consider a prohibition against the use of privacy and proxy services to be an appropriate solution to the issues raised by some Working Group members. I urge the Working Group members to adopt a model that sees the continuing wide availability of privacy and proxy services.	Support for P/P Services	Australian Government Office seeks wide availability of p/p services.	Office of the Australian Information Commissioner	WG should consider the views of the Australian Government and note whether we have received any other governmental inputs in this comment process.	
Skipped row						
56161	[Direct quote/relevant extract/summary of comment]		2	[Name of Individual / Group Name]		