PPSAI PDP WORKING GROUP

Sub Team 1 – Section 1.3.2

Summary & Analysis of Question 2 – Disclosure & Publication of Requests from LEA and other Third Parties other than IP Rights Holders (5 September 2015)

QUESTIONS FOR WHICH PUBLIC COMMENT WAS SOUGHT:

(1) Should it be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer?

(2) Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity?

(3) What (if any) should the remedies be for unwarranted Publication?

(4) Should a similar framework and/or considerations apply to requests made by third parties other than LEA and intellectual property rights-holders?

	Q1	Q2	Q3	Q4	Other/Comments
1.	Yes	Yes, if illegal activity established and to use responses in law and RAA	Yes, on a case by case basis possible compensation. ICANN compliance notified	N/A	Up to each provider to decide on contact requests
2.	Yes, if compliance with local law. If not addressed by law should be developed with LEA input	No – market controlled	No – market controlled	Yes, appendix E to serve as model for non-LEA requests in particular on malware	Polices need to be developed if not addressed by law in notifying registrant
3.	Yes, only if LEA request has been deemed valid	Yes, as critical for preventing abuse	Depends on reason for publication and contract law should provide sufficient remedies. Suggests	N/A	

			complaints to ICANN and for ICANN to withdraw accreditation		
4.	No, important to define LEA request – should operate within local laws	N/A	N/A	N/A	Important to differentiate between LEA and non-LEA requests. Different laws in different jurisdictions regarding disclosure
5.	Maybe - disclosure to depend on local laws of requestor	N/A	N/A	No, non-LEA organisations should be treated as complainants and an independent adjudicator to determine claim	Different jurisdictions have different laws on LEA requests
6.	No, disclosure only if required by relevant/local law	N/A	N/A	No, any framework should be replaced with operating within the relevant law and other such processes already in place	A number of remedies are in place for IP holders including UDRP
7.	No, any issues LEA have should be resolved by government	N/A	N/A	No, polices should be established by using examples already in use e.g. CIRA	
8.	No, data should only be disclosed in exceptional	N/A	N/A	N/A	

	circumstances, e.g. likelihood of abuse – allegations are not sufficient alone. Domain owners to be allowed to respond to claims				
9.	No, should be on a case by case basis	No	None	No, any process should be governed by local law	Difficulties with putting the same burden on providers as hosting companies. Not dealing with content. Provider may disclose anyway if thought to be held liable. Local law should always be taken into consideration
10.	No, only if complies with relevant legal process and court order. Privacy must be protected	N/A	N/A	N/A	Human rights issues. To protect privacy find the gaps between local law and human rights
11.	No, only if legal due process is followed. No right to grant any extended rights to LEAs	No, too much – P&P providers should agree to take reasonable steps to investigate and respond to complaints	N/A	No not necessary	
12.	Yes but local LEA requests to be treated	No, follow local law in respect of	N/A	N/A	Final recommendations

	differently to LEAs from other jurisdictions. Take language from RAA	publication; access only granted to LEAs in local jurisdiction in and ICANN's jurisdiction			must ensure that any allegation is not illegal in the jurisdiction and is supported by evidence
13.	No and disclosure only an exception to the rule and dealt with in compliance with local law	N/A	N/A	Yes but limit source of demands for disclosure and have strict safeguards dependent on whether LEA, IP owners or third parties	Privacy is key and disclosure must be subject to local laws in the applicable registry's jurisdiction
14.	No, disclosure should be provider's decision	N/A	N/A	No - third parties requests only accepted if served by local LEA	No automatic process
15.	No, providers to follow local law re notification not be compelled to do so. Disclosure only to LEAs in provider and ICANN's jurisdiction	N/A	N/A	Yes, local LEA requests to be treated differently to LEAs from other jurisdictions. Take language from RAA	Final recommendations must ensure that any allegation is not illegal in the jurisdiction and is supported by evidence. Violations of free speech and privacy
16.	No, unless gag order – up to LEA and provider	No, unless agreed by experts	Unsure – did have a few suggestions	Yes and requests to be agreed by experts	
17.	No, unless gag order. Customer deserves to know who wants his info. Must maintain	N/A	N/A	N/A	Privacy driven

	privacy of registrant even against LEA				
18.	No	N/A	N/A	N/A	Interesting suggested process
19.	No	No	No	N/A	No to disclosure to copyright holders
20.	No, only to keep confidential in matters of national security or with a court order	No, as not up to providers only the web host	No, no complaints procedure to be established with accreditation process. If publication unwarranted then provider could face a fine	No	Not sure how to providers will define national security or what is the highest legal proof?
21.	Maybe – dependent on jurisdiction and local law	N/A	N/A	N/A	
22.	Yes	Yes	No – a matter between the customer and the provider	Yes	
23.	No, unless allowed under local law	No disclosure can be made through the usual channels	N/A	No, existing process sufficient	
24.	Maybe – if site is hacked scenario – suggesting registrar changes name servers and then domain owner to remove malware.	N/A	N/A	N/A	Interesting scenario but not practical
25.	No, disclosure only	N/A	No, as once	N/A	

	under a court order and based on local law		published then no return.		
26.	No, only with a court order to allow registrant to appeal	N/A	N/A	N/A	
27.	No, always notify registrant	No	Yes, provider to be penalised somehow	No, must be strict over request process	
28.	No	No	None	No	
29.	No, always notify registrant	No	No	No	Privacy to be guarded at all times
30.	No	No	N/A	N/A	IP holders not to make requests only through courts and local law
31.	No	No	No	No	I think the point of question 3 was lost here
32.	Unsure	Unsure	Unsure	Unsure	Not clear on anything here
33.	N/A	N/A	N/A	N/A should not confuse trade marks and domain names	There are unregistered rights which are protected. Thanks for sharing
34.	N/A	N/A	N/A	N/A	Does not agree with LEA definition
35.	No	No	No	No	No regulation for providers and current legal remedies sufficient
36.	N/A	N/A	Yes, if published then registrant has all costs, including	No	Should not have to provide personal info for a domain

			litigation and losses should be covered by ICANN		
37.	No, only if provided for by local law	No, unless in accordance with local law	N/A	N/A	For changes in law, lobby government
38.	No, only if provided for by local law	N/A	N/A	N/A	
39.	N/A	N/A	N/A	N/A	Not strictly relevant but one for you Alex??? Sausages???
40.	No	No	No, only if provided for under local law	No	
41.	No	No	No	No	
42.	No, only if provided for under local law	N/A	N/A	N/A	No framework for LEA or IP holders. Otherwise an abuse of privacy
43.	No	No	N/A	No	
44.	No, for freedom of speech reasons	No or would affect file sharing sites	Yes and revocation of accreditation	Yes	Questions illegal activity and jurisdiction
45.	No, already have court order process in place	No	No	No	
46.	No, must inform registrant regardless	No, for privacy reasons	Yes, against ICANN and the publisher of the data	No	Large mandatory fines in the remedies
47.	No, notify customers	No, providers should protect the privacy of registrants	N/A	No and inform registrant of any non-LEA requests	
48.	No, questioning which LEA and jurisdiction	Yes	None	No, providers should protect privacy against third parties	

49.	Yes, only if LEA request is deemed valid	Yes, to prevent abuse and harm those using privacy services for legitimate reasons	Maybe – depends upon reasons for publication, e.g. negligence. Breach of contract remedies are already available and complaints to be lodged with ICANN, with loss of accreditation to follow.	Yes, to prevent and stop cybercrime. Not always LEAs who have an interest in doing so	Concerns about cybercrime and repeat offending. Auditing of providers and publication of errors would ensure accountability. See ICANN study. The provider's T&Cs should be clear on breaches
50.	Yes	Yes	N/A	Yes	
51.	No, providing no tip offs and no abuse by LEAs.	Yes, if registrant is made fully aware of all issues	N/A	N/A	ICANN oversees the world??
52.	No, providers should abide by local law	N/A	N/A	No, unnecessary for anyone including LEAs	ICANN should not create new rights which are not in law
53.	No, disclosure only on court order	N/A	N/A	N/A	Succinct
54.	Yes	No, as problematic	Not sure	No	Needs to think of remedies
55.	No	No	No	No	LEA and IP holders concerns not sufficient to affect privacy
56.	No	N/A	N/A	N/A	
57.	No, registrant to be able to seek court order to block disclosure	N/A	N/A	N/A	Registrant to be able to request information on requester
58.	No, if only request, yes	No	Yes, compensation	No, should only	Privacy concerns

	if court order			apply to LEA	
59.	No, providers should only act in accordance with local law	No, as contact details may well be fake	No. only if requested to do so by LEA as no return once published	No should only apply to LEA	
60.	Yes	Yes	N/A	Yes, Good idea	
61.	N/A	N/A	Local law takes precedence and if multi-national issues, involve the State Department	N/A	Recommends including “[in any standardized Disclosure/Publication request form] a limitation of "in accordance with the registrar's host/parent country".
62.	No, always notify the customer	No, in case of hacking	Yes, compensation by provider and/or ICANN and any other recourse allowed by law	N/A	
63.	No, unless provided with a court order otherwise registrant should be notified	No, due to constant change in malware	N/A	N/A	
64.	No, must notify registrant in all cases	No, not without consent of registrant, who should notify LEA	No remedies as no return. Seems a bit frustrated by the question	I will take that as a no. Suggests lessening the amount of personal data collected	Concerns about transparency and privacy. Issues with this being Internet Policing
65.	N/A	N/A	N/A	N/A	Kill it, this is so inappropriate – interesting stance
66.	No	No	No	No	Concerns about giving

					LEAs more rights and privacy issues
67.	No	No	N/A	No	Concerns about being spammed and personal data being available
68.	No	No	Yes, a refund	No, beyond our scope	Function of WG to find a balance between a valid request and the expectation of privacy
69.	N/A	N/A	No	No, as already legal avenues for IP infringement. Proposed changes go beyond this. No need for further framework	
70.	No, only if mandated by law	No only if mandated by law	No only by law	No, unnecessary	Recommends that the only parties using standardized request forms "are authorized by local authorities to do so."
71.	N/A	N/A	N/A	No, unnecessary, it will remove any protection under current laws and presume registrants to be guilty	Privacy concerns
72.	No	No	No	No	Erosion of privacy concerns
73.	No, provider is subject	No, there is no	No, should be in	No, any legitimate	

	to local laws and LEA can act only on authority under those laws	return after publication and may be the result of hacking. Publication may make this worse	the contract between provider and registrant and/or loss of accreditation	complaints can be filed through LEA	
74.	No, concerns about abuse by LEA	No	N/A	No – no-one should have this right, not even LEAs	Concerns about privacy and the laws governing privacy. Believes customer should always be notified/very strict rules around no notification.
75.	No, against civil rights	N/A	N/A	N/A	Concerns about civil rights and privacy; "American citizens have the right to face their accusers."
76.	No unless required to do so by law	No	None	No	
77.	No, it is a threat to privacy	No	No	No	Concerns about privacy and right to own opinion
78.	No	No	No	No	Existing legal systems are sufficient
79.	No, unless by court order	Yes but with a dispute period	No, once published then no return allowing all publications to be opposed	Yes, registrant to have right of appeal in case of unwarranted publishing	Providers not required to monitor content of websites. T&Cs to be specific
80.	No, only with court order	N/A	N/A	N/A	Notes that "Most privacy services will be run by people that

					understand when a request is pertinent to a dangerous situation and when it is simply abusive and refuse to service the request."
81	No	N/A		No	Customer MUST be notified when provider receives a publication or disclosure request from a third party.
82	No, unless required by law	No, unless appropriate legal documentation is provided	No, "except those as outlined in P/P service provider's contractual terms and conditions"	No	

SUMMARY & RECOMMENDATIONS

(1) Should it be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer?

In general, most of the comments are that it should not be mandatory to comply with express requests from law enforcement unless required by the applicable law (of either the requestor or the registrant). There was one suggestion that if this is not addressed by applicable law then a policy should be developed with LEA input. There was substantial support for the idea that registrants should always be notified but this was caveated that it may not be possible in some instances, e.g. abuse allegations. Two legal firms supported the idea that local law enforcement should be able to request no notification, but with the caveat that it would only apply for requests deemed to be valid. A few responses suggested the registrant should be notified regardless of request and to be able to defend or block the request in court. Another suggestion was to differentiate between local LEA requests and those from other jurisdictions. Another suggestion noted the difference between jurisdictions in which law enforcement may legally request a lack of notification (with a likely expectation that it will be respected), but it is not compulsory. A key concern was the erosion of privacy, with a few concerns about civil rights and freedom of speech.

SUB TEAM RECOMMENDATIONS: The general take-away appears to be that accredited P/P service providers should comply with express requests from LEA not to notify a customer where this is required by applicable law. The WG should consider whether to adopt this message explicitly. Given that a number of commenters did not zero in on the phrase "in the provider's jurisdiction", the WG may also wish to consider whether it should be mandatory for accredited P/P service providers to comply with express requests from LEA in other jurisdictions—those of the requestor or the registrant—not to notify a customer.

WG DISCUSSION/ACTION: Clarify in the Final Report that: (1) any and all WG recommendations on this topic are not intended to prevent providers from either adopting more stringent standards or from cooperating voluntarily with LEA; and (2) express LEA requests not to notify a customer are to be complied with where this is required by applicable law.

(2) Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity?

Roughly half of the commenters did not respond to this question. The general feeling among those who answered this question (39 out of 82) is that there should not be mandatory publication for these activities for a variety of reasons including but not limited to the fast rate of change in malware, possible effects on privacy, possibility of fake contact details, and the need for P/P providers to take reasonable steps to investigate and respond to complaints. It was also noted that any publication should be in accordance with applicable law. A few comments advocate publishing if illegal activity is established as doing so would be critical in helping to prevent abuse and protecting those using P/P services for legitimate purposes. ALAC for example observed that it would be appropriate when misuse of the DNS under the terms of the service and illegal activity is established, and also that P/P provider actions do not preclude other likely and more severe responses allowed by the RAA or in law. Several comments noted that they believed action was appropriate for these problems, but that Publication was not the appropriate action, and remedies for issues such as malware or viruses may more appropriately be taken up with the registrar or hosting provider, as these are content issues.

SUB TEAM RECOMMENDATIONS: Because the comments overall demonstrate a deference to contractual agreements (and terms of service) between the providers and their customers, and believe these to be enforceable mechanisms, contractual agreements should similarly control where the domain names are being used for activities that violate the terms of service, including for example malware/viruses. Therefore, the WG should consider whether to recommend that publication be mandatory for certain types of activity, a standard that would be reflected in the provider's terms and conditions and enforced accordingly. The WG may also consider what the appropriate evidentiary basis should be for abuse, as well as whether there may be remedies dictated by the terms and conditions other than publication to temper, and/or permit efficient investigation of, the alleged abuse.

WG DISCUSSION/ACTION: The responses seem to support the WG's Preliminary Recommendations #6 - #8 on provider terms of service. The WG is unlikely to recommend mandatory publication, as it was noted that providers generally and already have the discretion to terminate service for breach of their terms of service. This in effect would result in Publication. The WG noted further that there should be no restriction on providers being able to terminate service to a

customer on grounds stated in the terms of service, subject to any other specific limitation/recommendation by the WG. It is probably not possible to create a general policy that would in all cases prevent Publication via termination of service where the customer is ultimately shown to have been innocent (i.e. not in breach) - but as it finalizes its recommendations for the Final Report the WG may consider requiring that a provider first notify a customer before doing so, if the alleged ground for termination is malware.

(3) What (if any) should the remedies be for unwarranted Publication?

There are mixed comments on this question but in the main the sense was that there should be no extra remedies – several comments suggested that once publication has occurred there is no way to unpublish and therefore no penalty would suffice or that there are sufficient remedies under contract law. Many noted that this should be a matter between the privacy and proxy provider and registrant and dealt with in either the terms and conditions or under applicable law. Other comments stated that there should be a penalty, including but not limited to compensation (from publisher and ICANN), loss of accreditation (so ICANN compliance may be directly involved), a refund of the service fees. One noted that the state department or equivalent should be involved in cross-jurisdictional issues. Others seemed unsure as to remedies.

SUB TEAM RECOMMENDATIONS: The general take-away is that the contractual agreements between providers and their customers and relevant applicable laws control (and are sufficient) to remedy unwarranted publication. The WG should consider whether language specifying this sentiment should be included in the report, whether it is already inherent in the status quo, or whether the WG should consider additional remedies for unwarranted publication.

WG DISCUSSION/ACTION: The responses seem to support the WG's Preliminary Recommendations #6 - #8. Nonetheless, it would be useful to clarify the language in the Final Report to refer expressly to the possibility that this issue will in many cases be dealt with by the provider's terms of service and applicable law.

(4) Should a similar framework and/or considerations apply to requests made by third parties other than LEA and intellectual property rights-holders?

Roughly 50 out of 82 comments addressed this question. The majority (roughly 40 out of 50) of those who did were not in favour of a new framework for requests from third parties other than LEA and intellectual property rights-holders from a privacy perspective. That means roughly half of those who reviewed this questioned the necessity of a framework for third parties other than LEA or IP rights-holders, or thought it should be restricted/safeguarded. Many thought that the processes and any applicable law already in place are sufficient in this respect, the framework would be unnecessary, that third parties should be treated as complainants and should go through LEA, and any policy to be established should use examples already in use. Many thought

the framework in place for LEA requests was sufficient but some thought this was unnecessary too. [1]Some believe that local LEA requests should be treated differently to LEAs in other jurisdictions. [2]A couple of comments stated IP holders should not be allowed unless through a court order/local courts/independent adjudicator and that there are already legal avenues for IP infringement (such as going through LEA). [3]But some stated that disclosure may be permitted, subject to stricter procedures and safeguards. The registrant should also be informed of any non-LEA requests.

The Business Constituency thought Annex E could serve as a model for non-LEA requests, while others proposed that complaints should go to ICANN or proposed new bodies to mediate or authorize requests. Others noted that any form of Disclosure in this respect would have to be heavily safeguarded and would depend on whether the request was coming from LEA, IP holders or third parties, and on what was to be revealed. Some argued that requests would need be agreed by experts, or be extended specifically to expert groups already active. It was also thought the framework would help prevent and stop cybercrime.

SUB TEAM RECOMMENDATIONS: Although a number of those who responded questioned the necessity of a framework for third parties other than LEA or IP rightsholders, not many expressed why they thought it was unnecessary. We have deliberated related issues as a WG for some time, and several reasons advanced for other groups may be applicable here. Because many commenters were concerned with safeguarding privacy, our focus should remain on balancing privacy interests with other interests, and ensuring there are adequate safeguards in place in a framework for disclosure to third parties other than LEA and IP rightsholders. Moreover, there appears to be a level of trust of the community in the providers to investigate allegations of abuse or conduct that is against their terms of service, and to respond fairly to complaints. Because of the apparent deference to contractual agreements between providers and their customers, we should consider specifying in the report that certain types of activities are prohibited, or should be prohibited, by the terms of service and that any framework is designed to ensure consistent, restricted, and balanced way to address abuse complaints. Finally, the answer to this question may also to some extent depend on the framework established for LEA and IP rightsholders. Procedures for disclosure on grounds other than IP and LE could also come later after accreditation comes into force.

WG DISCUSSION/ACTION: Consider in light of recommendations from Sub Team 3. Sub Team 1 also notes that Blacknight Internet Solutions' comment included the suggestion 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." The Sub Team believes that while this suggestion is of relevant interest to its review of the sub-questions under this Question 2, the specific workings and procedures of ccTLDs may be more appropriately analysed by Sub Team 3. In this regard, Sub Team 1 notes that ICANN staff had previously prepared a summary of selected ccTLD practices around disclosure that may be useful.