**Privacy & Proxy Services Accreditation Issues (PPSAI) PDP Working Group**

**Public Comment Review Tool (Part 3)**

**19 August 2015**

For background and the general public comments received, please see <http://forum.icann.org/lists/comments-ppsai-initial-05may15/>. For a summary analysis of all the template responses received, please see the WG wiki space at: <https://community.icann.org/x/KIFCAw>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **16. Do you agree with the WG's recommendation concerning the relaying of electronic communications? Namely, that: (1) All communications required by the RAA and ICANN Consensus Policies must be forwarded; and (2) For all other electronic communications, P/P service providers may elect one of the following two options:i. Option #1: Forward all electronic requests received (including those received via emails and via web forms), but the provider may implement commercially reasonable safeguards (including CAPTCHA) to filter out spam and other forms of abusive communications, or Option #2: Forward all electronic requests received (including those received via emails and web forms) received from law enforcement authorities and third parties containing allegations of domain name abuse (i.e. illegal activities)? (3) Do you also agree that P/P service providers must publish and maintain a mechanism (e.g. designated email point of contact) for Requesters to contact to follow up on, or escalate, their original requests? (Section 1.3.1 Recommendation 16, Section 7.1 Category E)** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 29 template responders |  |  |
|  | No |  | 37 template responders |  |  |
|  | Yes with conditions (none specified) |  | 3 template responders |  |  |
|  | Privacy and proxy services should ensure that communication submitted to them should be properly forwarded to the registrant, but should not be responsible for adjudicating disputes over specific types of content or behavior on behalf of the registrant. |  | Google |  |  |
|  | Web.com believes that several of the WG's recommendations are unsupportable in their current form and are inconsistent with international data protection and privacy laws … we recommend that the WG revise its policy recommendations accordingly. |  | Web.com |  |  |
|  | The MPAA generally agrees that recommendations 16 and 17 outline a balanced and enforceable set of minimum standards associated with the relay of third party requests, but would like to highlight several issues:  Regarding the handling of electronic requests described in Option #1 of Recommendation 16 (p. 11), the accreditation standard must ensure safeguards that may filter out legitimate reports of abuse should not be considered commercially reasonable. |  | MPAA |  |  |
|  | Time Warner agrees with the recommendation of the Initial Report relating to the initial relay of electronic communications/allegations of illegal activity to customers of P/P Services (P/P Customers) … Any accreditation standards need to ensure that automated systems used to handle relays do not filter out legitimate reports of abuse … |  | Time Warner |  |  |
|  | Intermediaries, including privacy/proxy services, should not be required to assess the nature of content provided by third parties. |  | CDT/Open Technology Institute/PK |  |  |
|  | [G]enerally agree with recommendations 16 and 17 setting minimum standards for P/P Providers associated with the relay of third party requests.  Regarding recommendation 16, it was clear from the extensive discussions within the WG that most service providers would be expected to use automated systems to handle relays, and thus may use commercially reasonable safeguards such as CAPTCHA to filter out spam or other abusive communications. However, for smaller services such as those associated with certain specialized registrars, it could also be commercially reasonable to inspect each relay request manually as the filtering mechanism. IPC believes that option #1 should be interpreted flexibly, but must exclude any safeguard mechanism that routinely “filtered out” bona fide reports of domain name abuse, which would defeat the purpose of relay requirements. Such mechanisms should not be considered “commercially reasonable.” |  | IPC |  |  |
|  | [A]grees that P/P Providers should be required to either promptly forward to the P/P Customer all electronic communications that they receive (except for spam filtered out by commercially reasonable safeguards), or to promptly forward to the P/P Customer at least those electronic communications they receive that contain allegations of illegal activity such as trademark infringement. |  | INTA |  |  |
|  | We support the efforts of the working group to establish clear guidelines for “relaying” communication to the registrant (Recommendations 16 & 17. The IACC prefers Option #1, which would avoid any additional burden on the provider to act as an arbitrator to determine what constitutes “illegal activity.” |  | IACC |  |  |
|  | We support most of the “Relay” proposals of the PPSAI – proposals that would pass on communications from registries and registrars (such as renewal notices) and also legal communications such as “cease and desist” letters that attorneys may choose to send. |  | NCSG |  |  |
|  | We favor Option 2 as it allows filtering of unwanted messages such as purchase enquiries even if those do not qualify as spam or abusive communications. |  | Key Systems |  |  |
|  | Yes. The user of the privacy service should be able to indicate how they want communications and which communications (excluding RAA and ICANN communications). In addition, any captcha system should be required to be accessible to anyone regardless of ability to include the use of audio captcha and math captcha. the W3 web accessibility group could advise further on this point. |  | Reagan Lynch |  |  |
|  | Yes with conditions | There is no full security that using option #1 will guarantee there will not be abusive communication and this may be clearly stated in its agreements - reasonable safeguards shall be enough to the registrant. | Vanda Scartezini |  |  |
|  | Yes with conditions | In option #2: Only mail received from law enforcement authorities should be forwarded. No third parties. | Sebastian Brosser |  |  |
|  | Yes to (1), on (2) P/P providers and customers should have the option to elect which information should be forwarded; such scenarios should not be limited to these two options. |  | Donuts |  |  |
|  | Yes but with conditions - I completely disagree with Option #2 The very LAST thing you should be doing is giving the domain owner details of the person accusing the abuse. To a spammer a domain is disposable, what they LOVE to know is that an email is active, this increases the price they can sell the email for. The obvious middle ground here is Spamcop and Spamhaus When you report spam to Spamcop they resolve links determine who the spammer is. What is BAD is that some companies (even big companies like GoDaddy) ignore the abuse reports so all spamcop can do is record the information for stats. |  | J. Wilson |  |  |
|  | Yes but with conditions - Forwarding of electronic communications is important but privacy is more important. This must be considered when creating these policies else the internet becomes like George Orwell's novel 1984. |  | Dr. M. Klinefelter |  |  |
|  | Yes except the requirement that service providers have followup capability. Again, that should be up to the service provider. |  | Marc Schauber |  |  |
|  | Yes – but agree only with recommendation 1. Customers should have full transparency on third party requests for their identity or other information. |  | Sam |  |  |
|  | Yes – but for (2), P/P need to be compelled to use a safeguard against spam, not to be just an option. |  | Adrian Valeriu Ispas |  |  |
|  | Yes | I have no objection to receiving any requests from law enforcement about allegations. But this is interesting - what if my site is hacked and is now hosting say illegal material - I see this and delete the content refresh the server etc. Then am I going to be prosecuted for destroying evidence? Because - in the UK at least possession of 'child porn' is a strict liability offence. So if I observe files on there that shouldn't be there (content unknown) I am legally safe if I delete them without knowing their contents. If I find out or know what is in the files then this would potentially be evidence against me. Even the US government has been well and truly hacked so this is not outside the bounds of possibility. | Name withheld |  |  |
|  | Yes with conditions | P/P service providers shouldn't exist, but if they do, it shouldn't be up to them to participate in escalation. | Scott McClung |  |  |
|  | Yes with conditions | The WG should clarify the escalation mechanism. I believe the requester, not the customer, should bear any escalation fee. | Homer |  |  |
|  | Yes with conditions | SPAM filtering can not be allowed, spam complaints, containing spam being reported, will get filtered. | Gary Miller |  |  |
|  | Yes with conditions | Agreed on 1. Agreed on 2 if and ONLY if requests are made by a human (electronically, by voice, or by phone) who can clearly describe their need to communicate. Automated correspondence such as machine-generated notifications should be discarded. Disagreed on escalation mechanisms. | Andrew Merenbach |  |  |
|  | Yes with conditions | For Option #2, law enforcement authorities and third parties act on allegations of domain name abuse, whether justified or not, and forcing forwarding of electronic requests could create an avenue for harassment of individual clients of P/P service providers. | Adam Creighton |  |  |
|  | Yes with conditions | Option #2 with the exclusion of 3rd parties, and the right for registrars to filter commercial offers to the end user and person using the service. Allegations of illegal activities must follow the normal abuse procedure. | Arthur Zonnenberg |  |  |
|  | Yes with conditions | It should be the sole responsibility of the service provider to maintain contactability and no one else should be imposing this. | C. |  |  |
|  | Yes with conditions | I believe the general concept is reasonable here, but would benefit from refinement. OK as recommendation to providers; not yet OK as mandate for providers. | Jason Burns |  |  |
|  | No | Do not agree with law enforcement authority as defined. | Christopher |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | Option #1 and #2 are too limiting. P/P service providers should be given the flexibility to decide which level of filtering they wish to offer their customers. For example, a P/P service provider may block allegations of abuse that are not substantiated. | Cort Wee |  |  |
|  | No | Option #1 is preposterously broad and should be eliminated. Option #2, in speaking of third parties alleging any form of illegal activity, ignores the concept of due process. All I would have to do is file a form that says "he put a music file on his site" and I could pierce the P/P protection. The P/P provider must have the authority (under penalty of law, if abused) to protect common domain owners from vast third-party bots with canned "illegal activity" language. | Michael Ho |  |  |
|  | No | Seriously? You want to leave the courts out of this process? Are you on crack? | Stephen Black Wolf |  |  |
|  | No | This would destroy a legitimate safeguard that protects small business. | Noah Greenstein |  |  |
|  | No | We do not need a controlled list of privacy/proxy service providers at all. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | ---- you | Robin Hood |  |  |
|  | No | What communications should be relayed and how is between the P/P service and the user of that service. I do not support any measures imposing restrictions on this. | Finn Ellis |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |
|  | --- | I do not want spam in any case. | M.B. |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **17A. Do you agree with the WG's recommendation that: (1) all third party electronic requests alleging abuse by a P/P service customer will be promptly forwarded to the customer; and (2) a Requester will be promptly notified of a persistent failure of delivery that a P/P service provider becomes aware of? [In answering this question, please feel free to provide additional guidance to the WG as to what would constitute a "persistent delivery failure" beyond what is stated in the Initial Report](Section 1.3.1 Recommendation 17, Section 7.1 Category E)** | | | | | |
|  | **Comment[[1]](#footnote-1)** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 20 template responders |  |  |
|  | No |  | 25 template responders |  |  |
|  | Yes with conditions / Yes to one or some (no further comments) |  | 4 template responders |  |  |
|  | Web.com does not support recommendation 17 as currently written. Specifically, bullet one should clarify that "All" does not include spam or other forms of abusive communications as outlined in recommendation 16. |  | Web.com |  |  |
|  | The recommendations outlined in 17 (pp. 11-12) are critical to the accurate and timely relay of communication to the privacy and proxy customer from third parties. While we agree that the technical failure of electronic communications should not be equated with the failure of a customer to respond to a request, it is important that requesters be promptly notified of a persistent delivery failure when a P/P service provider becomes aware of it. |  | MPAA |  |  |
|  | Time Warner agrees with the recommendation of the Initial Report relating to … the notification of a “persistent delivery failure” ... Any accreditation standards need to ensure that automated systems used to handle relays do not filter out legitimate reports of abuse … |  | Time Warner |  |  |
|  | Recommendation 17 describes important details regarding the proper relay of requests from a third party (Requester) to a registrant via a proxy service. While we agree that the failure of “delivery” (i.e. a technical failure) of communication should not be equated with the failure of a customer to respond to a request, it is important that Requesters be promptly notified of a persistent delivery failure when a P/P Provider becomes aware of it. |  | IPC |  |  |
|  | INTA also agrees that P/P Providers should be required to either promptly forward to the P/P Customer all electronic communications that they receive (except for spam filtered out by commercially reasonable safeguards), or to promptly forward to the P/P Customer at least those electronic communications they receive that contain allegations of illegal activity such as trademark infringement. Once that initial relay is made, a P/P Provider should be required to promptly notify the trademark owner if it becomes aware of a “persistent delivery failure” and should perform a verification or re-verification (as applicable) of the P/P Customer’s email address at that time. INTA thus supports the Initial Report’s recommendations on “relay” as far as they go. But they should go farther. | Additional suggestions on relay incorporated into Sub Team 1 template | INTA |  |  |
|  | Instead of "All third party electronic requests alleging abuse by a P/P service customer will be promptly forwarded to the customer", we propose: "Provider will promptly upon receipt attempt to forward all substantiated third party electronic requests alleging abuse by a P/P service customer to the customer." |  | Key Systems |  |  |
|  | Yes | Persistent failure to me would be a failure of the message to be delivered after five attempts with one attempt made every 24 hours. At that point the privacy provider should initiate the verification procedures. I also think that the requestor should be notified after the fifth failure that the registrant cannot be contacted and then be given the protected Whois information so that they can follow up via postal mail or other contact methods. | Reagan Lynch |  |  |
|  | Yes | Promptly should be 30 to 60 days after initial attempt. You must provide adequate time and air on the side of fairness. Anything shorter could be the result of holidays, vacations, illness, etc. | Marc Schauber |  |  |
|  | Yes | The report states a reasonable definition of what represents persistent delivery failure. | Vanda Scartezini |  |  |
|  | Yes | Persistent delivery failure should not happen after only one method of communication fails. P/P providers should attempt to contact the registrant using at least two methods of communication, and they should allow the registrant a reasonably amount of time to reply. (Unless, for example, the email bounces or their phone line is disconnected.) | Nick O’Dell |  |  |
|  | Yes to only one - I would be concerned about veracious abuse allegations being reported over and over. For example Microsoft sent legal threats to MikeRoweSoft - belonging to Mike Rowe... that should be dismissed. |  | Name withheld |  |  |
|  | Agree with #1. #2, I would want a a long enough time definition of "persistent" to be sure it's not a transient failure of an email server. |  | Daniel Langer |  |  |
|  | Disagree with #1 - "Third-party allegation" is an unacceptably low bar and must be recast.  Agree with #2 - a properly vetted complaint should have an escalation path if delivery fails. |  | Michael Ho |  |  |
|  | Agreed to #1 provided these requests are made on a case-by-case basis by a human. Automated notifications of abuse should be discarded.  Disagreed on #2: if someone chooses to ignore communication they should be free to choose to do so. If the registration holder is in violation of the law, traditional means of enforcement should be used, modeled after United States due process and the concept of "innocent until proven guilty." When someone breaks laws they can be subject to arrest or a lawsuit, same as with other venues for committing crime. |  | Andrew Merenbach |  |  |
|  | #1 is OK.  #2 is unclear what counts as failure, and hence is prone to abuse. |  | Noah Greenstein |  |  |
|  | Only agree with #1 |  | Aaron Holmes |  |  |
|  | Yes with conditions | A persistant failure of delivery could be a bounced email for over 72 days, because if the email is on a domain that has expired then the user might recover the domain within that period. After that is goes to auction. | J. Wilson |  |  |
|  | Yes with conditions | Forwarding of electronic communications is important but privacy is more important. This must be considered when creating these policies else the internet becomes like George Orwell's novel 1984. | Dr. M. Klinefelter |  |  |
|  | Yes with conditions | "Persistent delivery failure" would include e.g. multiple emails bouncing, in which case telephoning or writing to the registrant would be appropriate. | Hugo Jobling |  |  |
|  | Yes with conditions | If the text is required to be sent together with the rest of the request to the customer | Alex Xu |  |  |
|  | Yes with conditions | The WG should clarify what a persistent delivery failure is. | Homer |  |  |
|  | Yes with conditions | I'd have to see some consensus on numbers of attempts and "a reasonable period of time" as mentioned, in order get an idea of how open to abuse it would be. | Thomas Smoonlock |  |  |
|  | Yes with conditions | Third party requests should be forwarded only if the customer has elected to have all requests forwarded. | Sebastian Brosser |  |  |
|  | Yes with conditions | "Persistent delivery failure" would include e.g. multiple emails bouncing, in which case telephoning or writing to the registrant would be appropriate. | Hugo Jobling |  |  |
|  | No | We do not need over reaches like what's being proposed. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | If included, this is not a privacy service anymore. Anybody alleging abuse is way too broad and intrusive. The feedback of delivery failure goes to the registrar or P/P service provider. They will find alternative means. It is not the right of the Requester to know so, nor should it be. | Arthur Zonnenberg |  |  |
|  | No | We disagree with these recommendations, as they are too broad and allow for abuse of the proposed system. The community has seen that, while P/P services may provide shelter for a certain number of registrants that abuse the domain name system, there also is proven abusive behavior on the part of self-designated (but not authoritative) "policing" entities. Instead, legitimate requests alleging abuse (as determined by P/P provider) may be forwarded. | Donuts |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | I think this opens up the opportunity for frivolous harassment of P/P service provider Clients. | Adam Creighton |  |  |
|  | No | OK as recommendation to providers, not OK as mandate to providers. Providers must have discretion to refuse requests, for example if the request facility itself is being abused. | Jason Burns |  |  |
|  | No | As above. The nature of relay service is between the P/P provider and its user, and it's for them to determine the conditions of that service. | Finn Ellis |  |  |
|  | No | Your days are numbered. | Robin Hood |  |  |
|  | No | If they're not getting through right now, the P/P provider is either incompetent or it's because they are screening vexatious emails that are known to be from bad actors. (1) would provide a hijack that forces emails to be delivered. | Anonymous Turtle |  |  |
|  | --- | Whatever definition is finally evolved it should not, in effect, provide a loophole which would allow malefactors materially to extend the period of their inappropriate activity. If all parts of the chain are made aware of the criticality of these processes then they will know the importance of responding promptly to them and the potential consequences of not so doing. | John Carr |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **17B. Do you agree with the WG's recommendation that when a P/P service provider becomes aware of a persistent delivery failure to a customer, that will trigger the provider’s obligation to perform a verification/re-verification (as applicable) of the customer’s email address(es), in accordance with the WG’s recommendation that customer data be validated and verified in a manner consistent with the WHOIS Accuracy Specification of the 2013 RAA? (Section 1.3.1 Recommendation 17, Section 7.1 Category E)** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 16 template responders |  |  |
|  | No |  | 36 template responders |  |  |
|  | Time Warner agrees with the recommendation of the Initial Report relating to … verification/re-verification … Any accreditation standards need to ensure that … in the event of a persistent delivery failure the P/P Service “must upon request forward a further form notice to its customer..”, without saddling the right holder or consumer with any additional cost. |  | Time Warner |  |  |
|  | Once that initial relay is made, a P/P Provider should be required to promptly notify the trademark owner if it becomes aware of a “persistent delivery failure” and should perform a verification or re-verification (as applicable) of the P/P Customer’s email address at that time. |  | INTA |  |  |
|  | Yes | Email and/or phone | Kelly Andersson |  |  |
|  | Yes | Sure, re-verification shall be a normal process when facing persistent delivery failure. | Vanda Scartezini |  |  |
|  | Yes, and I think full contact verification should take place not just of the email address. |  | Reagan Lynch |  |  |
|  | Yes If the appropriate amount of attempts occurred. |  | Dan M. |  |  |
|  | Yes | How many of these are we talking about? | Name withheld |  |  |
|  | Yes with conditions | A P/P service provider and a customer can communicate with each other via means other than those specified in the Initial Report, so the WG should not mandate any particular form of contact information. For example, a customer can log into a Web site of the P/P service provider to receive or send messages. | Homer |  |  |
|  | Yes with conditions | Subject to my prior conditions of legitimacy and attempt to reach postmaster@domain, the language seems reasonable. | Michael Ho |  |  |
|  | Yes with conditions | Provided the re-verification takes place no more than once during each year (term) of domain name registration, this makes sense. Otherwise these requests could become a denial-of-service in an attempt to garner a response. | Andrew Merenbach |  |  |
|  | Yes with conditions | Only due to delivery of authorized parties, not 3rd parties alleging abuse. Otherwise, this recommendation is open for abuse by 3rd parties suspecting a temporary e-mail failure and seizing the opportunity to disable the domain name. Efforts for P/P service provider within commercial reason. | Arthur Zonnenberg |  |  |
|  | Yes with conditions | Spam issues are a serious problem as described before. My registrant emails were all destroyed when I transferred away from Godaddy and godaddy lifted my privacy. Failure to respond is not lack of good will. Spam issues must be tackled and solved. Response forms may be one solution, instead of publishing emails. | Mario Hellmann |  |  |
|  | Yes with conditions | This should be solely the responsibility of the provider. | C. |  |  |
|  | Yes with conditions | As failure is not defined, this is prone to abuse. Needs clarification. | Noah Greenstein |  |  |
|  | Yes with conditions | Service provider to contact registrant for explanation prior to reverification. | Scott Jordan |  |  |
|  | No | ffs calm down with the millions of questions | John Doe |  |  |
|  | No | Absolutely not. It's up to the consumer to make sure they update their records, if necessary. | Marc Schauber |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | This would risk the privacy and safety of those who need it most, and provide an excuse for stealing domains. | Private |  |  |
|  | No | We disagree with this recommendation. It is the obligation of the registrar to validate a Whois record according to the terms of the 2013 RAA. The recommendation, as worded, opens the door to constant re-verification of a record based on failure of delivery that could be caused by multiple reasons (not related to an inaccurate Whois record). | Donuts |  |  |
|  | No | Stay out of the P/P business. Believe me, once my domain gets disabled, you \*will\* hear from me. | Aaron Dalton |  |  |
|  | No | In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | Email is not a guaranteed delivery mechanism! Allowing third parties to trigger verification and potentially cause suspension of registration is a denial-of-service mechanism with nontrivial chance of success. The continued operation of a website should not depend on the whims of the email provider's spam filter. | Jason Burns |  |  |
|  | No | Whois is a useless database that only serves to aid stalkers and those with malicious intent in discovering the personal data of a domain name registrant. | Stephen Black Wolf |  |  |
|  | No | Non applicable, as above | Finn Ellis |  |  |
|  | No | It's not clear what benefit this would provide. | Nick O’Dell |  |  |
|  | Not all domains have email |  | Joe |  |  |
|  | --- | Don’t know | M.B. |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **20A. Do you agree that privacy/proxy service customers should be notified prior to de-accreditation of a P/P service provider, to enable them to make alternative arrangements? If so, should this be when Compliance sends breach notices to the provider, as customers would then be put on notice (as is done for registrar de-accreditation)? (Section 1.3.1 Recommendation 20, Section 7.1 Category G)** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 45 template responders |  |  |
|  | No |  | 16 template responders |  |  |
|  | Where feasible, a customer should be able to choose its new P/P service provider in the event of de-accreditation of its existing provider. Separate to the domain registration itself, there should be a provision that the P/P cannot sell a customer's info, eg can't sell email addresses to a spammer. |  | Phil Crooker |  |  |
|  | Yes. A domain name owner should be notified at the time ICANN has determined to de-accredit a p/p. In addition, ICANN should provide up to three p/p providers for the customer to choose from and require that the p/p losing accreditation must post this information on its home page as well as on the ICANN website. |  | Reagan Lynch |  |  |
|  | Yes | Clearly, consumers must be given the option to find another p/p provider. | Marc Schauber |  |  |
|  | Yes | Notification is extremely important. | Dan M. |  |  |
|  | Yes | Individual registrants must be able to reasonably maintain their privacy regardless of the actions of the provider. If de-accreditation poses any risk of Publication or Disclosure, the registrant must be provided adequate recourse for maintaining privacy, since Publication and Disclosure cannot be undone. | Jason Burns |  |  |
|  | Yes provided the reasonable timeline for cure of the breach has been accommodated and is passed. |  | Donuts |  |  |
|  | Yes, this should be when the breach notices are submitted. I continue to disagree with the idea of accrediting P/P services. |  | Andrew Merenbach |  |  |
|  | Yes with conditions | I don't agree with the whole framework but the taking of property (de-accreditation) requires a high burden and sufficient transparency for the customers. | James Ford |  |  |
|  | Yes with conditions | There should be no accreditation of privacy service providers. | Private |  |  |
|  | Yes with conditions | This is ominous. Of course I would want to know of a P/P provider had its accreditation revoked, but it is unclear to me the circumstances under which ICANN would take such a brazen step. | Michael Ho |  |  |
|  | Yes with conditions | Kill the accreditation process. Kill it with fire. | Aaron Dalton |  |  |
|  | Yes with conditions | Notification should come from the P/P provider itself as soon as possible. | M.B. |  |  |
|  | Yes with conditions | Accreditation or de-accreditation should not negatively impact the service or the privacy of the customer information, and at no point should it be disclosed or subject to threat of disclosure by any third-party organization. | C. |  |  |
|  | Yes with conditions | Yes, but accreditation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue. | Lucas Stadler |  |  |
|  | Yes with conditions | Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes. | Finn Ellis |  |  |
|  | Yes with conditions | Customers should only be notified if there is a deaccreditation. Sending an email on notice of breach is a forceful move that's intended to put pressure on the P/P provider. The P/P provider is looking out for the interests of the customers in this case, not ICANN. | Anonymous Turtle |  |  |
|  | No | This requires accreditation, which is a steaming pile of cow excrement in itself. | Aaron Mason |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | Is not your business | D. Miedemma |  |  |
|  | No | 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 are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | No accreditation should be required. | Shane T. |  |  |
|  | No | No. That's a risk of hiding behind p/p. | Scott Jordan |  |  |
|  | No | I do not want to see an accreditation process come into existence. | Aaron Holmes |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **20B. Do you agree that other P/P service providers should also be notified, to enable interested providers to indicate if they wish to become the gaining P/P provider (as is done for registrar de-accreditation)? If so, should all notification(s) be published on the ICANN website (as is done for registrar de-accreditation)?** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 37 template responders |  |  |
|  | No |  | 26 template responders |  |  |
|  | Yes with conditions (none specified) |  | 3 template responders |  |  |
|  | Yes | Perhaps the initial registrant could at registration list a preferred provider so as not to receive 35 spam emails in the event of de-accreditation. | Kelly Andersson |  |  |
|  | Yes, agreed, and these notifications should be published. I continue to disagree with the idea of accrediting P/P services. |  | Andrew Merenbach |  |  |
|  | Yes with conditions | There should be no accreditation of privacy service providers. | Private |  |  |
|  | Yes with conditions | I think this is reasonable but it remains unclear how this could happen. | Michael Ho |  |  |
|  | Yes with conditions | ICANN should be less involved, so the second clause should be amended. | Noah Greenstein |  |  |
|  | Yes with conditions | Impending de-accreditation should not impinge on the registrant's privacy, including by providing third parties with mailing lists. Third-party solicitation should probably not be encouraged. | Jason Burns |  |  |
|  | Yes with conditions | Yes, but accreditation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue. | Lucas Stadler |  |  |
|  | This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain. |  | D. Miedemma |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | Yes, agreed, and these notifications should be published. I continue to disagree with the idea of accrediting P/P services. | Aaron Dalton |  |  |
|  | No | That would entail releasing customers' information. | M.B. |  |  |
|  | No | I believe this would provide a "chilling effect" to the industry and to this particular vertical market. | Adam Creighton |  |  |
|  | No | 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 are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | No accreditation should be required. | Shane T. |  |  |
|  | No | I do not want to see an accreditation process come into existence. | Aaron Holmes |  |  |
|  | No | This makes it too easy for a problematic accredited P/P provider to insert itself everywhere. The customer should be notified and have to research it. | Anonymous Turtle |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **20C. Do you agree that a de-accredited P/P service provider should have the opportunity to find a gaining provider to work with (as sometimes occurs with registrar de-accreditation)?** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 48 template responders |  |  |
|  | No |  | 19 template responders |  |  |
|  | Yes, agreed, and these notifications should be published. I continue to disagree with the idea of accrediting P/P services. |  | Andrew Merenbach |  |  |
|  | Yes with conditions | Much depends on the circumstances leading up to de-accreditation. It may be more appropriate that the de-accredited service provider be given a list of options rather than allowing it to "find" another service provider with motivations similar to its own. | Tim Kramer |  |  |
|  | Yes with conditions | There should be no accreditation of privacy service providers. | Private |  |  |
|  | Yes with conditions | I think this is reasonable but it remains unclear how this could happen. | Michael Ho |  |  |
|  | Yes with conditions | If this were enforced, there needs to be some oversight to ensure there is not a usury scenario occurring that is artificially / maliciously forcing accredited P/P service providers out of business to the benefit of a gaining provider. | Adam Creighton |  |  |
|  | Yes with conditions | Accreditation or de-accreditation should not negatively impact the service or the privacy of the customer information, and at no point should it be disclosed or subject to threat of disclosure by any third-party organization that the customer does not wish to disclose that information to. | C. |  |  |
|  | Yes with conditions | Yes, but accreditation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue. | Lucas Stadler |  |  |
|  | Yes with conditions | Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes. | Finn Ellis |  |  |
|  | No | ICANN should make the determination of the gaining provider to eliminate the possibility that a de-accredited privacy/proxy provider would select an affiliated entity. | Terri Stumme |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | Kill the accreditation process. Kill it with fire. | Aaron Dalton |  |  |
|  | No | 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 are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | No accreditation should be required. | Shane T. |  |  |
|  | No | I do not want to see an accreditation process come into existence. | Aaron Holmes |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **20D. Do you agree that a “graduated response” approach to de-accreditation should be explored, i.e. a set series of breach notices (e.g. up to three) with escalating sanctions, with the final recourse being de-accreditation?** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 40 template responders |  |  |
|  | No |  | 21 template responders |  |  |
|  | Yes – maximum of 3 |  | Kelly Andersson |  |  |
|  | Yes - As long as it is a large adequate series of breach notices. |  | Dan M. |  |  |
|  | Yes with conditions | Why up to three? What does baseball have to do with the internet and privacy? 3 strikes and you are? Unaccredited amazing. | Gabriel de Luca |  |  |
|  | Yes with conditions | I don't agree with the framework in the first place. | James Ford |  |  |
|  | Yes with conditions | There should be no accreditation of privacy service providers. | Private |  |  |
|  | Yes with conditions | The WG should explore allowing more than three series of breach notices. | Homer |  |  |
|  | Yes with conditions | As long as the process does not linger. | Gary Miller |  |  |
|  | Yes with conditions | I think this is reasonable but it remains unclear how this could happen. | Michael Ho |  |  |
|  | Yes with conditions | No new territory or conditions for de-accreditation should be defined here. I continue to disagree with the idea of accrediting P/P services. | Andrew Merenbach |  |  |
|  | Yes with conditions | That local authority law is not infringed upon by this de-accreditation process. | Arthur Zonnenberg |  |  |
|  | Yes with conditions | Yes, but accreditation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue. | Lucas Stadler |  |  |
|  | Yes with conditions | Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes. | Finn Ellis |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information | TS |  |  |
|  | No | Kill the accreditation process. Kill it with fire. | Aaron Dalton |  |  |
|  | No | 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 are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | No accreditation should be required. | Shane T. |  |  |
|  | No | I do not want to see an accreditation process come into existence. | Aaron Holmes |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **20E. Do you agree that, where feasible, a customer should be able to choose its new P/P service provider in the event of de-accreditation of its existing provider?** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 45 template responders |  |  |
|  | No |  | 16 template responders |  |  |
|  | Yes with conditions (none specified) |  | 8 template responders |  |  |
|  | Yes with no further cost to the user, in the same way that if you transfer a domain with 3 years to run those three years are honored. |  | J. Wilson |  |  |
|  | Yes | Seamless anonymity is absolutely crucial. Anonymity must never be lifted without giving a chance to move over to another anonymity provider | Mario Hellman |  |  |
|  | Yes | Not just feasible but ALWAYS. | Adrian Valeriu Ispas |  |  |
|  | Yes, they should be notified. |  | Dan M. |  |  |
|  | Yes with conditions | This should be able to be setup prior to even the event of starting use with the first P/P. Thereby allowing the customer to have their information with a P/P service they trust. Not just the next one on the list. And not after their information was turned over automatically to the next P/P service behind the one being unaccredited. | Gabriel de Luca |  |  |
|  | Yes with conditions | Customers should be given sufficient time to change their privacy provider to ensure that at no time is private information leaked. | Hugo Jobling |  |  |
|  | Yes with conditions | I don't agree with the framework in the first place. | James Ford |  |  |
|  | Yes with conditions | I think this is reasonable but it remains unclear how this could happen. | Michael Ho |  |  |
|  | Yes with conditions | I continue to disagree with the idea of accrediting P/P services. | Andrew Merenbach |  |  |
|  | Yes with conditions | Though the customer's identity should be protected in the event of switching P/P service provider (per the language elsewhere in the recommendations). | Adam Creighton |  |  |
|  | Yes with conditions | Within the arrangements made by parties. | Arthur Zonnenberg |  |  |
|  | Yes with conditions | Yes, but accreditation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue. | Lucas Stadler |  |  |
|  | Yes with conditions | Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes. | Finn Ellis |  |  |
|  | Yes with conditions | The customer should also be able to choose a non-accredited provider. | Anonymous Turtle |  |  |
|  | Yes with conditions | There should be no accreditation of privacy service providers. | Private |  |  |
|  | No | 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 are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | No accreditation should be required. | Shane T. |  |  |
|  | No | I do not want to see an accreditation process come into existence. | Aaron Holmes |  |  |
|  | This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain. |  | D. Miedemma |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **20F. Do you agree that the next review of the IRTP should include an analysis of the impact on P/P service customers, to ensure that adequate safeguards are in place as regards P/P service protection when domain names are transferred pursuant to an IRTP process?** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 49 template responders |  |  |
|  | No |  | 22 template responders |  |  |
|  | Yes | Due process per the law of the domain owner's country should be required before revealing information. The WHOIS database is unnecessary in the first place. It should be taken down. | TS |  |  |
|  | Yes | Though I question where the cost of the analysis of the impact where will be borne, and whether this will unduly burden P/P service providers (which will be passed on to Clients). | Adam Creighton |  |  |
|  | Yes | I continue to disagree with the idea of accrediting P/P services. | Andrew Merenbach |  |  |
|  | Yes | I believe that the current language of these recommendations is more or less opening a can of worms. Please consider the impact on the customers of these proxy/privacy customers, or at least make these recommendations or guidelines that do not negatively impact their privacy and their ability to express their speech freely on the web. | C. |  |  |
|  | Yes | The needs of end users do not appear to be a goal of the current recommendations. I would be very interested to review one where they were. | Finn Ellis |  |  |
|  | Yes | There should be no accreditation of privacy service providers or mechanism for violating the privacy of users. | Private |  |  |
|  | Yes with conditions | I don't agree with the framework in the first place. | James Ford |  |  |
|  | No | No P/P protection should exist at all. | Gary Miller |  |  |
|  | No | No. The IRTP is neither defined nor linked here, so it is impossible to agree with this statement. | Michael Ho |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | 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 are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain. |  | D. Miedemma |  |  |
|  | --- | All I care about is being spammed. If our email is publicly available someone will write 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. | Ian McNeil |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **20G. Please provide any suggestions you may have on a possible compliance framework that may facilitate the effectiveness of the de-accreditation process. (Section 1.3.1 Recommendation 20, Section 7.1 Category G)** | | | | | |
|  | **Comment** | **Additional Comments** | **Commenter** | **WG Response** | **WG Action** |
|  | I don’t think that P/P providers need accreditation |  | Liam |  |  |
|  | Launch an initial trial of selected providers? |  | Kelly Andersson |  |  |
|  | Utilization of iCANN’s current compliance program framework is a start; however, greater attention to enforcement, more transparency in the decision-making process and final determinations made by ICANN is needed. |  | Terri Stumme |  |  |
|  | Kinda needs accreditation to exist. |  | Aaron Mason |  |  |
|  | Don't make P/P services jump through these loops. This is an international issue. It should not be something that a USA company can inflict upon a Europe company. This entire Recommendation is just scary for the future of the internet. |  | Gabriel de Luca |  |  |
|  | Scrap this whole proposal. |  | James Ford |  |  |
|  | If accreditation is required, de-accreditation should only occur because of a failure to keep P/P information private, IE the P/P service disclosing information should be the only reason for de-accreditation, and P/P services should generally be prohibited from disclosing personal information or storing it long term. |  | Not your business |  |  |
|  | YOU ARE ONLY TROUBLING GOOD-FAITH USERS. THOSE WITH ILL INTENT WILL EASILY CIRCUMVENT THESE RULES! |  | TS |  |  |
|  | Do not force accreditation on providers, in the first place. |  | Shantanu Gupta |  |  |
|  | Whenever a private company handles an accreditation, that's a bad thing. |  | Christopher Smith |  |  |
|  | You lie, you die. |  | Gary Miller |  |  |
|  | There should be no de-accreditation process whatsoever. |  | Adam Miller |  |  |
|  | De-accreditation of a P/P provider should have a public comment period as it will have far more stakeholders than just ICANN, the provider, the requesters, and the registrants of the requested domains. |  | Byunghoon Choi |  |  |
|  | De-accreditation needs to be a consequence of misbehavior, not an arbitrary threat. Currently it appears to be the latter. Whatever framework is defined, it must be as narrow and specific as possible, avoiding the "things we think of later" kind of language seen before, |  | Michael Ho |  |  |
|  | Respectfully, I continue to disagree with the idea of accrediting P/P services. |  | Andrew Merenbach |  |  |
|  | Abolish accreditation. Else force it upon us and we'll hasten our technological workarounds and moving away from this bullshit, anyway. |  | Jawala |  |  |
|  | Kill the accreditation process. Kill it with fire. |  | Aaron Dalton |  |  |
|  | All I care about is being spammed. If our email is publicly available someone will write 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. |  | Ian McNeil |  |  |
|  | To not use a separate framework for this, or go beyond regular de-accreditation. |  | Arthur Zonnenberg |  |  |
|  | Yes, but accreditation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue. |  | Lucas Stadler |  |  |
|  | No accreditation should be required. |  | Shane T. |  |  |
|  | I do not want to see an accreditation process come into existence. |  | Aaron Holmes |  |  |
|  | There should be no accreditation of privacy service providers. |  | Private |  |  |

1. Some of the more general comments noted under Recommendation 16, above, also seem intended to apply to this Recommendation 17; in some cases this was stated expressly. [↑](#footnote-ref-1)