**PPSAI – Category E - RELAY of complaints to the privacy/proxy customer**

**Question 1 – What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers?**

**Background information relevant to this question:**

*GNSO's Terms of Reference for a proposed Privacy & Proxy Relay & Reveal Study (dating from 2010):*

For many domains, Registered Name Holders can be reached directly at addresses obtained from WHOIS. However, for Privacy/Proxy-registered domains, Registered Name Holders or third party licensees cannot be reached directly via WHOIS- published addresses. Instead, ***communication relay requests*** may be sent to the Privacy/Proxy service provider published in WHOIS, or attempted using addresses obtained from other sources, websites or communications associated with the domain.

*Whois Review Team Final Report*

In considering the process to regulate and oversee privacy/proxy service providers, consideration should be given to the following objectives:

(…)

* Adopting agreed standardized relay and reveal processes and timeframes; (these should be clearly published, and pro-actively advised to potential users of these services so they can make informed choices based on their individual circumstances);

**Information from the Whois Studies**

*WHOIS Proxy/Privacy Reveal & Relay Feasibility Survey*

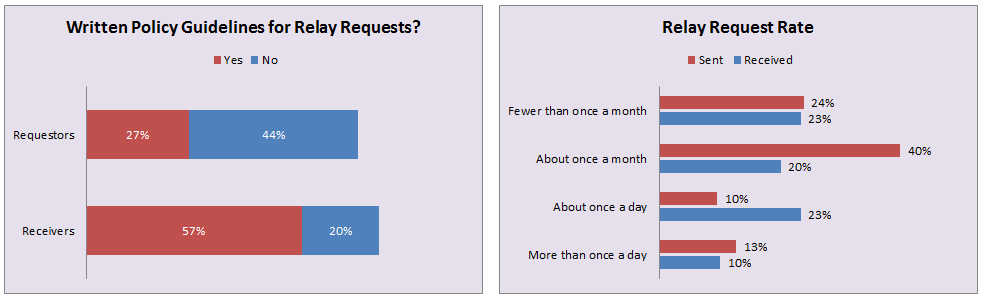
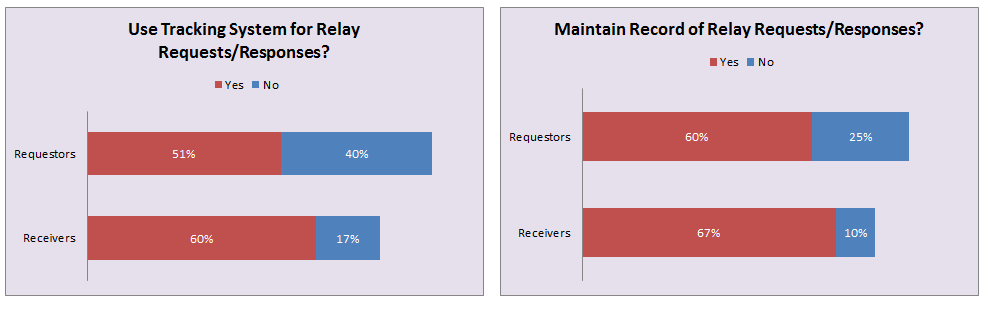
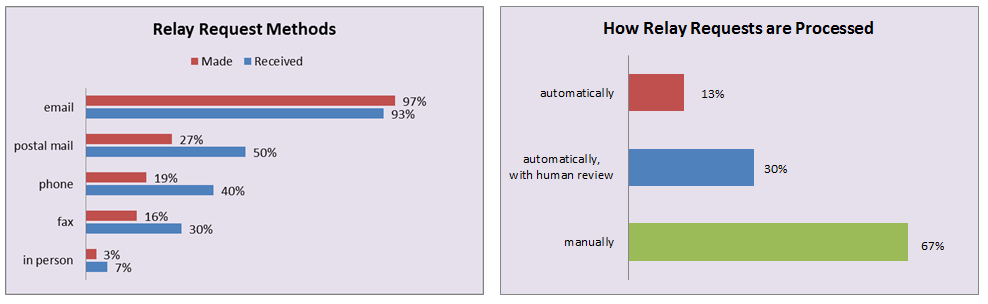
In some cases, privacy and proxy service providers publish email and postal addresses in WHOIS which can be used to relay communications to the actual domain name holder: i.e., domainname@ privacy-or-proxy-provider. Some of these providers may require court orders or other legal instruments before they will provide information to those making requests.

(…)

4.2 Relay Handling

For many domains, Registered Name Holders can be reached directly at addresses obtained from WHOIS. However, for Privacy- or Proxy-registered domains, Registered Name Holders or third party licensees cannot be reached directly via WHOIS-published addresses. Instead, communication with the Registered Name Holder may be attempted by sending a request to the Privacy or Proxy service provider published in WHOIS to relay the message to the Registered Name Holder or third party licensee. Communication may also be attempted using addresses obtained from other sources, websites, or communications associated with the domain.

37% of survey respondents reported experience sending communication relay requests. 18% reported experience receiving and/or responding to them.



4.2.2. Interviewee observations

The information obtained from interviews was consistent with the results of the online survey. Most requests were submitted and processed electronically. Interviewees were vague about the request rates they handled, saying it varied: some months were quiet and others were busy. Law enforcement said that information was hard to obtain because they have no central clearinghouse handling requests and records are stored across all sectors of the justice system. All of the interviewees said that the details of actual requests and responses were unlikely to be available to a full study. Both those making the requests and those processing them have concerns about identifying domain names or registrants, except when that information is already in the public domain: for example in court records or UDRP transcripts.

Processes for responding to requests appear to be ad-hoc and performed manually on a caseby-case basis. Responders said that they automatically co-operate with local law enforcement but have trouble authenticating requests from overseas. Those initiating requests expressed dissatisfaction with providers’ responsiveness. It is not clear if the reported inconsistency between those on the supply and demand side of relay and reveal requests is caused by structural problems or process/communications failures.

4.2.3 Implications for a Full Study

60% of relay request senders maintain records, and 51% use tracking systems to do so; for relay request receivers, the numbers are similar (67% and 60%). However, it is unlikely that this information would be made available to a full study in a way that would identify individual

domain or registrant names. These data would be aggregated or anonymized.

**Other Information**

*Information relating to relay from sample of P/P Terms & Conditions as collected by ICANN Staff upon the request of the WG*

|  |  |
| --- | --- |
| **Whoisproxy.com (affiliated registrar: KeySystems)** | Any email sent to the automatically generated temporary anonymous individual email address will be redirected to the email address provided by the registrant. The service provider is not obligated to contact the registrant via another method should his email address become non-functional. In order to protect registrant from spam the generated email address will only work for a period of 14 days after the whois query was made. |
| **1 & 1 Internet** | You hereby authorize 1&1 to receive, sort, open, forward, and destroy any and all mail sent to 1&1 on your behalf in its sole discretion. Third class and "junk" mail will be discarded upon receipt or returned to the sender unopened. First-class mail and mail received via certified mail or courier, including but not limited to Federal Express, United Parcel Services, and similar services, will be opened and all such mail that can be scanned will be scanned and sent to you via the e-mail address associated with the 1&1 account for the Private Domain Name. You acknowledge that you will have five (5) calendar days from the date such mail is sent to you via e-mail to request in. writing that a copy of such scanned mail be forwarded to you via postal mail. You acknowledge that unless you direct us otherwise in writing within such five (5) calendar day period, all such mail will be destroyed five (5) calendar days after a scanned copy is sent to you via e-mail. All mail that is unable to be scanned will be forwarded to you at your expense at the postal address associated with the account for the applicable domain name. Messages received at the e-mail address posted in the public WHOIS database for your Private Domain Name will be forwarded to the e-mail address associated with your account name or to another e-mail address, in accordance with the preferences you set in the 1&1 Control Panel. |
| **Domains by Proxy (Affiliated Registrar: GoDaddy.com)** | a. Correspondence Forwarding Inasmuch as DBP's name, postal address and phone number will be listed in the Whois directory, You agree DBP will review and forward communications addressed to Your domain name that are received via email, certified or traceable courier mail (such as UPS, FedEx, or DHL), or first class U.S. postal mail. You specifically acknowledge DBP will not forward to You first class postal mail (other than legal notices), "junk" mail or other unsolicited communications (whether delivered through email, fax, postal mail or telephone), and You further authorize DBP to either discard all such communications or return all such communications to sender unopened. You agree to waive any and all claims arising from Your failure to receive communications directed to Your domain name but not forwarded to You by DBP.  b. Email Forwarding The Whois directory requires an email address for every purchased domain name registration. When You purchase a private domain registration, DBP creates a private email address for that domain name, "@domainsbyproxy.com". Thereafter, when messages are sent to that private email address, DBP handles them according to the email preference You selected for that particular domain name. You have three (3) email preferences from which to choose. You can elect to:   Have all of the messages forwarded;  Have all of the messages filtered for Spam and then forwarded; or  Have none of the messages forwarded.  As with all communications, You agree to waive any and all claims arising from Your failure to receive email directed to Your domain name but not forwarded to You by DBP.  c. Notifications Regarding Correspondence and Your Obligation to Respond When DBP receives certified or traceable courier mail or legal notices addressed to Your domain name, in most cases, DBP will attempt to forward the mail to you via email. If You do not respond to the DBP email and/or the correspondence DBP has received regarding Your domain name registration concerns a dispute of any kind or otherwise requires immediate disposition, DBP may immediately reveal Your identity and/or cancel the DBP private registration service regarding either the domain name registration(s) in question. This means the Whois directory will revert to displaying Your name, postal address, email address and phone number that you provided to DBP. |
| **Whois Privacy Service (Affiliated Registrar: Register.ca)** | Communications received with respect to a particular domain name registration will be handled as follows: (i) We will forward to you or a Contact all correspondence received by registered mail or traceable courier. This information may be opened, scanned and emailed to you or your Contact.. Regular postal mail will be discarded or returned to sender at our discretion. (ii) Email correspondence will be replied with the instructions to use the Whois Privacy Service registrant contact form available online. The submitted form will be forwarded to the registrant contact email address as they appear in our records. (iii) We will only be responsible for forwarding communications where our details have appeared in the whois and when your Whois Information is accurate, complete and up to date. |
| **DomainDiscreet.com (affiliated register: register.com)** | You agree that Register.com may review all emails, faxes, voice messages, certified or traceable courier mail (such as UPS, FedEx, or DHL), or first class U.S. postal mail ("Communications") sent to the Private Registration Addresses associated with your Private Registration Domain except first class postal mail or email, fax, postal mail or telephone communications which appear, in Regsiter.com' sole discretion, to be unsolicited Communications which offer or advertise the sale of goods or services or which solicit charitable contributions, or Communications which appear to arise from your having used the Private Registration Services as a general mail forwarding service (as further referenced above). Without limiting the foregoing, Register.com may review all other Communications sent to the Private Registration Addresses.  When you order Private Registration Services, Register.com creates a random and unique email address for your domain, using the suffix "@domaindiscreet.com". Thereafter, when messages are sent to the email address listed in the Private Registration Address, Register.com forwards such messages to the email address you listed in Personal WHOIS Data. If the email address you listed in the Personal WHOIS Data becomes non-functioning or if email to such address bounces, Register.com is not obligated to attempt to contact you through other means. |
| **My Private Registration (affiliated registrar: Melbourne IT)** | 3.3. Melbourne IT will process any correspondence (including Communications) and telephone calls received regarding the Relevant Domain Name as described below. You must promptly respond to all communications from Melbourne IT (as contemplated below) and at a minimum, in accordance with the time frames specified below. 3.3.1 Email: Melbourne IT will use all reasonable efforts to filter the email for Junk Mail. Any sender of an email that is not otherwise filtered out by Melbourne IT as Junk Mail will be directed to complete a form. If this form is not validly completed by the sender (in Melbourne IT"s sole discretion), you will not be notified of receipt of the email. If the form is validly completed by the sender (in Melbourne IT"s sole discretion), and provided that the sender completes the form in a timely manner, the email message of the sender will be forwarded by Melbourne IT to the administrative contact (as specified in your Contact Details) of the Relevant Domain Name within 3 business days of receipt. If (for whatever reason), the email address of such administrative contact is undeliverable, Melbourne IT will not be required to contact you through any other medium. 3.3.2 Postal: Melbourne IT will sort and open all postal mail. Any postal mail that is not a Communication will be destroyed by Melbourne IT. In addition, Melbourne IT will destroy any Communication that it determines (in its sole discretion) is or could be Junk Mail. Melbourne IT will use all reasonable commercial efforts to scan any reasonable sized Communication that is not Junk Mail and forward the scanned Communication to the email address of the administrative contact (as specified in your Contact Details) of the Relevant Domain Name within 3 business days of receipt. If (for whatever reason), the email address of such administrative contact is undeliverable, Melbourne IT will not be required to contact you through any other medium. The administrative contact will have 5 business days to confirm to Melbourne IT that it wishes to obtain a physical copy of the scanned Communication. If the administrative contact confirms that it wishes to receive a physical copy of the scanned Communication, a physical copy of the Communication will be sent to such administrative contact at the administrative contact"s expense, or, if the physical copy of the scanned Communication is a legal notice or Uniform Dispute Resolution Policy notice or correspondence, at Melbourne IT"s expense. You acknowledge that any scanned Communication forwarded to the administrative contact at the administrative contact"s expense will require the payment of that expense prior to it being provided to the administrative contact. If the administrative contact fails to respond to Melbourne IT within 5 business days or if such email address is undeliverable, Melbourne IT reserves the right to destroy the Communication following the expiration of 30 days from its receipt by Melbourne IT. In addition, if any Communication is unable to be scanned by Melbourne IT, Melbourne IT will use all reasonable commercial efforts to forward that Communication to the administrative contact (as specified in your Contact Details) of the Relevant Domain Name by mail. 3.3.3 Telephone: If a telephone call is received by Melbourne IT, the caller will be informed about how to contact the administrative contact of the Relevant Domain Name |
| **Whois Privacy Service (affiliated registrar: above.com)** | By subscribing to the Privacy Service, you authorize and direct Above.com Pty Ltd to process communications directed to you at the contact information displayed in the public WHOIS database as follows: - E-Mail Address. Messages received at the e-mail address posted in the public WHOIS database will be forwarded to the domain contact email address provided in your Above.com Domain Registrar account. This forwarding address is not filtered in any way, so we suggest a level of spam email filtering at the destination email address. - Postal Address. You hereby authorize Above.com Pty Ltd to receive, sort, open, and destroy any and all mail sent to the address posted in the public WHOIS database at its sole discretion. Above.com Pty Ltd may in its sole discretion destroy all third class and "junk" mail upon receipt and will either discard all such other communications received or return the same to the sender unopened. No postal mail will be forwarded to you. - Phone/Fax. The telephone and fax numbers posted in the public WHOIS database of the applicable domain name are answered and monitored by Above.com Pty Ltd. Third parties attempting to contact you using either of these means are informed that the domain name owner does not wish to receive communication in this manner and prefers e-mail. No messages or faxes will be forwarded to you. |

|  |  |  |  |
| --- | --- | --- | --- |
| **What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers?** | **Who** | **WG Response/Discussion** | **Recommended Action (if any)** |
| Relay should be as broad as is practical, only allowing non-relay based on "normal" procedures currently in use for filtering spam, junk mail, etc. | Withheld | The WG noted that there is no single uniform practice across different providers, e.g. some do not apply any filters except for spam; some allow customers to select the option to relay all communications; others require a requestor to reply to a correct email address within 24 hours. The WG generally agreed that P/P providers should continue to be able to provide safeguards to prevent abuse (e.g. against spurious, harassing or irrelevant complaints). The WG also agreed that a policy not to forward any communications (i.e. no relay) would not satisfy P/P accreditation standards. At a minimum, all registrant communications required by the RAA should be relayed.  Some WG members recommend that providers should forward all allegations of malicious/illegal activity except where this is not permitted by law; i.e. the presumption would be to relay, subject to reasonable safeguards which a P/P provider may implement (e.g. against spam and other forms of abuse). Others suggested making relay mandatory for certain types of communications (e.g. requests from law enforcement authorities or notices of UDRP proceedings).  The WG agreed that email communications are not reliable or perfect (e.g. there is no guarantee it will be read). The WG agreed, however, that it will be impractical to develop mandatory recommendations for telephone requests but has not yet agreed on how to deal with other forms of communication (e.g. hard copy letters).  Several WG members suggested placing a limit on the number of times that the same complaint can be relayed, but noted that the requestor may need to declare that there has been no response to prior communications in each case.  The WG discussed whether or not a P/P provider should be obliged to notify a requestor when a relayed communication is returned as undeliverable (as distinguished from “not received” or “no response”, neither of which may be known to the provider). The WG is considering recommending that a provider notify a requestor in a situation where the provider actually knows that a communication was undeliverable (ie a similar standard to the “knowingly” language used in the 2013 RAA).  The WG is also discussing whether to recommend that a provider should use commercially reasonable efforts to relay or implement commercially reasonable safeguards. In addition, the WG is discussing the question of charging a reasonable fee for relaying certain types of communications (e.g. postal mail which carries a charge for forwarding). This could be recommended as a best practice instead.  Further Notes: The WG noted at this stage that it may be relevant to consider when the process should move from relay to reveal; and some WG members suggested that a reveal request should not be conditioned on there first having been a relay request. |  |
| The baseline minimum standardized relay and reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers include:  For the relay process:  1 - All bona fide queries should be relayed upon request.  2 - The time standards for relaying and for subsequent reiterations of relay.  3 - Escalation in cases where customer cannot be reached through relay. | Keith Kupferschmid |  |
| If an intellectual property owner notifies a PP Service Provider in writing that the domain name subject to the privacy/proxy service (PPS) is the subject of an allegation of an intellectual property violation (or more formal dispute resolution or legal proceeding in a court or other legal body of competent jurisdiction), the PP Service Provider must RELAY notice of the proceeding to the PP Customer within 24 hours. | Jim Bikoff, David Heasley, Griffin Barnett, Valeriya  Sherman / Silverberg, Goldman & Bikoff, LLP |  |
| (1) All bona fide queries, regardless of geographic source, including all allegations of illegal activity, should be relayed upon request (subject to reasonable safeguards against abuse, e.g., CAPTCHA?). (2) Time standards for relaying (and for subsequent reiterations of relay). (3) Limitation on changes during relay period, for prevent cyberflight. (4) Escalation (to reveal and/or publication) in cases where customer cannot be reached (or does not acknowledge) through relay within set time limits. | IPC |  |
| Requests and demands for relay can be generated by spam or electronic means as easily as anything else. We support the imposition of reasonable efforts by proxy/privacy service providers to ensure that the requests being relayed are genuine, in good faith and not repetitive. | NCSG |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
|  | **What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers?** |
| **WG Preliminary Conclusion** |  |
| **Should the same conclusion apply to proxy services & privacy services? If not, please explain why.** |  |