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

**Public Comment Review Tool Version 1 Part 1**

**20 July 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>.

**I. GENERAL STATEMENTS/COMMENTS ON OVERARCHING PRINCIPLES[[1]](#footnote-1):**

TBA

**II. DEFINITIONS, PROVIDER STATUS, LABELING:**

| **#** | **Recommendation / Comment** | **Additional Comments/Notes** | **Who / What** | **WG Response** | **WG Action** |
| --- | --- | --- | --- | --- | --- |
| **1. Do you agree or disagree with the WG’s recommended definitions for the following terms: Disclosure, Publication, Person, Law Enforcement Authority, Relay, Requester (Section 1.3.1 Recommendation 1)?** | | | | | |
|  | Support |  | BC |  |  |
|  | Respects desire to use ICANN’s definition of LEA |  | ISPCP |  |  |
|  | No issues |  | Blacknight |  |  |
|  | Would welcome clarification as to exactly which organizations constitute P/P providers |  | Com Laude |  |  |
|  | Some have interpreted these definitions to extend to entities such as lawyers and law firms that register domain names on behalf of clients as an incidental part of larger and broader legal representation of their clients … While we do not think the WG intended such a sweeping requirement, IPC urges it to clarify that the standards only apply to those providers who specialize in the provision of such services and for which it is a primary business offering. |  | IPC |  |  |
|  | Agree with all | Note: This row represents all the template responses that answered the question without providing further comment | 58 out of 144 individual respondents to the WG question template |  |  |
|  | Agree with some | See Note above | 6 out of 144 |  |  |
|  | Agree with none | See Note above | 50 out of 144 template responses |  |  |
|  | Agree with some | Private proxy registration makes it exceedingly difficult, time-consuming, and cost-prohibitive to pursue a copyright infringement claim. BUT – for individual private “bloggers” with a “personal” website, eliminating private registration exposes millions of part-time hobbyist individuals to invasion of privacy and has a chilling effect on their online publication goals and pursuits. | Kelly Andersson (individual) |  |  |
|  | Disagree with: A) ICANN should publish and maintain a publicly accessible list of all accredited P/P service providers, with all appropriate contact information. Registrars should provide a web link to P/P services run by them or their Affiliates, and P/P service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program. No. ICANN should not publish such a list. ‘Commercial activities’ is too broad, to vague, and to static. My own domains have in the past, and in the future may continue to switch between commercial and non-commercial. B) Should registrants of domain names associated with commercial activities and which are used for online financial transactions be prohibited from using, or continuing to use, P/P services? If so, why, and if not, why not? No. Consumers are able to determine which domains do provide this information, and choose who to conduct business with. ICANN should be a ‘Good Housekeeping Seal’ not a police force. |  | Michael Cariaso (individual) |  |  |
|  | Agree with some; disagree with disclosure of contact information. Identity theft is rampant and by disclosing contact information will only add to the problem. |  | Dan Balla |  |  |
|  | Agree with none | Protect our privacy. The burden for small business owners to provide their home address to the public is crazy! This proposal is narrow minded, and does not take into consideration the small players. | Luis (individual) |  |  |
|  | Agree with some | What kind of survey does NOT allow me to DISAGREE I do not think ICANN should change ANYTHING, except: 1. To insist that GoDaddy provide authorized 3rd party WHOIS services with all WHOIS information rather than a link to their site. For example in the link below WHO.IS are unable to publish the complete information and the user is FORCED to go to GoDaddy. http://www.who.is/whois/oxcars.com I also think that ALL WHOIS providers should protect the data from bots by masking the email address with a long graphic, it is not sufficient to put a capcha as there are automated capacha systems What is wrong is that some of the services, specifically Domains by Proxy, Melbourne IT and the one in Panama, do NOT properly respond when you tell them that the domain has been used for spamming. I think they should simply cease providing the privacy service if Spamcop and Spamhaus have sufficient human reports of spam (not automated or ticks, a proper copy of header and email reported to said companies). | J Wilson (individual) |  |  |
|  | Agree with none | You've made this public comment form too complicated and neglected to show the sections you are referring to as part of the question. | Marc Schauber (individual) |  |  |
|  | Agree with none | The internet has become too much of an important utility for the world. You cannot start now to only care about the interests of a few anti piracy groups. There are way too many other groups that are also not even pirates who need to have privacy. Please for the love of god leave it to the individual countries and local laws to deal with this stuff. Your fatcat, anti piracy totalitarians are not the only ones on the block with an interest. It shouldn’t be your job. Please just stay out of it and remain neutral. | Anon (individual) |  |  |
|  | Agree with some | I am contented with the WG dealing with some of the chartered questions. But I disagree with their assessment and proposed resolution involving, "provider obligations in relation to "relay" and "reveal" procedures to handle requests for the disclosure of a privacy/proxy customer's identity and contact details." There should be no instances except under a sanctioned court order that anyone's private information is made public to any form. It violates due process, is blatant privacy infringement, and endangers millions of domain registrars and domain owners by enabling personal information to be available not only unnecessarily but also irrelevantly pertaining to their website or business. It is both directly and indirectly harmful and dangerous. | Dan M (individual) |  |  |
|  | Agree with none | ICANN itself is hypocritical on the definitions: Nor does ICANN not follow it's own rules on WHOIS entires. Person seems to have changed meaning so it doesn't mean person anymore - it can be 'domain administrator' ICANS own whois (on http://whois.icann.org/en/lookup?name=icann.org ) Name: Domain Administrator Organization: ICANN Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US Phone: +1.4242171313 from https://www.icann.org/en/system/files/files/approved-with-specs-27jun13-en.pdf p6 Registration Directory Whois Specification Registry Registrant ID: 5372808-ERL3 Registrant Name: EXAMPLE REGISTRANT4 Registrant Organization: EXAMPLE ORGANIZATION Registrant Street: 123 EXAMPLE STREET Registrant City: ANYTOWN Registrant State/Province: AP5 Registrant Postal Code: A1A1A16 Registrant Country: AA Registrant Phone: +1.5555551212 Registrant Phone Ext: 12347 Registrant Fax: +1.5555551213 Registrant Fax Ext: 4321 Registrant Email: EMAIL@EXAMPLE.TLD Registry Admin ID: 5372809-ERL8 1 Data element may be deleted, provided that if the data element is used, it must appear at this location. 2 Note: all applicable statuses must be displayed in the Whois output. 3 May be left blank if not available from Registry. 4 For the Registrant, Admin and Tech contact fields requiring a “Name” or “Organization”, the output must include either the name or organization (or both, if available). Note point #4 well - ICANN's entry for registrant, admin and technical contact is set to "Domain Administrator" That is is neither a person nor an organization (or both) - and certainly is not the contact for all three. So ICANN want to inflict rules upon the rest of us that they don't even do themselves. | Name withheld (individual) |  |  |
|  | Agree with none | I oppose the current proposals to change the privacy disclosure to what ICANN is is proposing. If we are paying for privacy then that is what we should get, privacy period. | Sperry Russ (individual) |  |  |
|  | Agree with some | Disagree with quasi-governments being considered law enforcement authority. | Christopher (individual) |  |  |
|  | Agree with none | KEEP WHOIS PRIVACY SERVICES ALIVE. Do NOT kill online privacy! Respect being anonymous! | John Doe (individual) |  |  |
|  | Agree with some - Law enforcement requests should come with judicial warrants. |  | James Ford (individual) |  |  |
|  | Agree with none | I don't believe that you should have to disclose your personal identity to the whole world just to get a domain name for your blog or other personal website. And I don't believe that there should be a means of forcing the disclosure of personal identity without a court process. Or that Whois records should include personally identifiable information. Or that domain registrars should be required to obtain personally identifying information from customers. If someone wants to buy a domain with bitcoin, and not identify themselves beyond an email like "someguy@example.com" it should more than sufficient. Frankly, I don't think Whois makes any sense. There should be some kind of DNS record for domain contact that just lists an email address and the rest of Whois ought to be just completely killed off. | Not your business (individual) |  |  |
|  | Agree with none | A privacy provider should be allowed to refuse disclosure except when required by compulsory legal process (warrant, subpoena, court order, or other binding legal process it is required to comply with by the jurisdiction in which it operates.) It should be allowed to refuse any requests by law enforcement to not notify the customer of the disclosure whenever those requests are not legally obligatory. Members of the public deserve the full protection of their privacy available under the law and it is wrong for ICANN to try to mandate less privacy protections than the law itself provides. | Simon Kissane (individual) |  |  |
|  | Agree with none | If you handle registrant privacy, freedom, and information like a police state, you lose any moral ground. People will not trust you, and you will force behavior that will make new industries and services based on avoiding illegal and unethical practices by your company and those you work with/for. Your reputation is on the line. If people do not want to be tracked or evaluated by unelected private companies, they have every moral and ethical right to do so. The free market will remain free. Freedom and privacy will win. The police state will be navigated around at all costs. You are either for freedom and privacy or against it. There is not middle ground. | Christopher Smith (individual) |  |  |
|  | Agree with none | With regards to private and public domain registration services. With the rise of digital organizations that are dedicated to causing havoc and mischief, a system that allows almost any individual with a nicely formatted letter, and or convincingly spoofed email, to reveal critically private information for individuals without a legal department would be devastating to home businesses and those that use the domain name system in a more professional than private manner. | Matthew R. Steno (individual) |  |  |
|  | Agree with none | I especially disagree with the following: 1) Mandatory disclosure to law enforcement: I can only see this being abused. 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. This is a feature, not a bug. If the LEA has a court order, then an impartial judge has decided that the officer isn't being abusive. 2) I disagree with ICANN dictating policy based on the content of the website in question. While I understand that for a long time, .com and .org were separate based on whether the organization registering them was a non-profit, that barrier has long fallen. The beauty of the internet is how people can use it without being stuffed into little boxes set created by someone else. 3) This policy severely compromises the ability of anyone who needs privacy or simply wants privacy to speak their mind. Government dissidents, members of LGBT communities overseas, anyone speaking truth to power or refusing to hide will be uncovered worldwide unless they happen to be a member of a corporation that has front office. The impact is disproportionately on individuals rather than companies. | Anonymous Turtle (individual) |  |  |
|  | Agree with none | Go ---- yourself | Robin Hood (individual; representing humans) |  |  |
|  | Agree with some | Don't dignify the assertion that corporations and other commercial organizations are people. | Finn Ellis (individual) |  |  |
|  | Agree with none | There should be no back door requirements to disclose information to any outside party. It should be wholly up to the provider of the service to follow the law as written when disclosing a users information. It should not be based on accreditation standards. | Jason Weinberg (individual) |  |  |
|  | Agree with some | I disagree with the definition of Law Enforcement Authority (hereafter LEA) as being too vague and requiring too much interpretation. Providing and interpreting a definition of LEA is outside of ICANN's scope and area of expertise. It is my opinion that rather than provide, maintain and interpret a definition of LEA, ICANN should instead make a reference to a list, compilation of lists or some other collection defined and maintained by some other authority or authorities that specialize in that subject matter. | Gregory Antonellis (individual) |  |  |
|  | Agree with none | Stop trying to break a system that is working fine already. | John Stetson (individual) |  |  |
|  | Agree with none | 1) Lack of privacy is life threatening. Even Europe and Canada have hate speech laws that outlaw basic free speech. Not even to mention the majority of undemocratic countries. Free private speech is an overriding good. 2) All emails I ever published on whois are spammed to death to the point of being useless. If someone notifies me, I will not notice. Private registration mostly gets respected by spammers. Spam is extremely serious as it disrupts normal channels of communication. 3) Even commercial providers can have an interest in provacy. They might be selling books, or sex toys. Or gay literature in countries where such endeavor carries a death penalty. 4) if it ain't broke, don't fix it. Leave as is. | Mario Heilmann |  |  |
|  | Agree with none | I own a woman-owned home-based business in the video game industry. I am also the Executive Director of 501c(3) non-profit professional organization for women working in video games. Women in my industry have been the target of death threats, rape threats, threats to their families and homes by people with access to home addresses through domain name registration. I have had domain names for my business and my non-profit registered to my address since 2005. It is imperative that criminals and the insane do not have access to my home address through ICANN. The FBI has been following my colleagues to protect them from potential murder and rape due to these threats. Do not be a part of the disclosure of personally identifying information that could lead to the worst kinds of personal crime and death. The liability for ICANN is huge. | Belinda van Sickle (individual) |  |  |
|  | Agree with some | I do not know about all the provisions and recommendations. I only know that I am utterly opposed to my information being available on the Internet to anyone who has access to a computer! Please maintain the privacy of the individual/businessowner who opts for privacy!!! | M.B. (individual) |  |  |
|  | Agree with some | The definition for "law enforcement authority" is insanely broad. What does a "quasi-governmental" authority even look like? And while we're on the topic, "publication" is problematic because I see no reason for a public WHOIS database anyway. | Aaron Dalton (individual) |  |  |
|  | Agree with some | This seems fine in general, though I worry about the breadth of "other similar" in the definition of "Law Enforcement Authority" being extended to cover private parties with only thin connections to legitimate government action. | Kat Walsh (individual) |  |  |
|  | Agree with some | While the other definitions are reasonable, the definition of "Law Enforcement Authority" fails to define "or similar authorities designated from time to time"; it also fails to define "jurisdiction" as to level (in the United States, local, state or federal; presumably any level of government can designate any authority for the purpose of this definition. | Michael Ho (individual) |  |  |
|  | Agree with all | Clear statements. No need to rewrite. | Vanda Scartezini (At Large, commenting individually) |  |  |
| **2. Do you agree with the WG’s recommendation that privacy and proxy services should be treated the same way for the purpose of the accreditation process? (Section 1.3.1 Recommendation 2, and Section 7.1, Category A)?** | | | | | |
|  | Yes |  | BC + 48 template responders |  |  |
|  | No |  | 62 template responders |  |  |
|  | No | Hypothetical example: Website A has posted without permission content owned by the owner/manager of Website B. The Website B owner should be able to contact the owner of Website A without too much fuss. Registration services (private and proxy) should be required to contact the owner of Website A within a short period, at no charge, with the complaint from Website B, and should be required to provide a response from A to B within a short period (say 5 business days). If Website A does not respond, then registrar provides contact info directly to Website B owner. | Kelly Andersson |  |  |
|  | Yes | What is critical here is that proxy services do not become a service for spammers. To this end, they should be required to provide owner information to Spamhaus and/or Spamcop in the event that there are more than 10 EXPLICIT user reports of spam, i.e that a human reported the item as Spam via the said services. | J Wilson |  |  |
|  | Yes | You've made this public comment form too complicated and neglected to show the sections you are referring to as part of the question. No idea how to answer this. | Marc Schauber |  |  |
|  | No | No if you accredit it you will want to publish it. I do not want any of my details published. I am willing to publish a contact email address that will be monitored - and if it receives much spam then we know that ICANN was responsible for it. | Name withheld |  |  |
|  | No | Reducing privacy on the open internet will reduce the individual content being produced and distributed. This limit of speech is unacceptable and will drive people to the dark net. | James Ford |  |  |
|  | No | I don't think it should be ICANN's business what someone is using a domain for and I don't think ICANN should be in the business of "accrediting" a domain. The only question should be "is it already in use?" If it's not, then it shouldn't matter who's using it. Likewise, I don't think privacy and proxy services should have to be accredited. (Though if ICANN insists on trying to do such things it's not clear to me that there's a difference between a "privacy" and "proxy" service.) | Not your business |  |  |
|  | No | My privacy and of my clients is not guaranteed nor safe at all under ICANN rules. | D. Miedema |  |  |
|  | No | This is going to end badly for you. | Robin Hood |  |  |
|  | No | They provide different services for different purposes, and deserve to be treated separately. | Finn Ellis |  |  |
|  | No | No accreditation should be required. | Shane T. |  |  |
|  | Yes with reservations | With reservations: this should be approached on a recommendation-by-recommendation basis, not imposed as policy, as the contractual implications are different. | Jason Burns |  |  |
|  | 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 | I do not believe that imposing these requirements where it should be the responsibility of the domain registrars is in the interest of the majority who may be affected should these recommendations come to pass, and this may create more problems where there weren't any previously. | C. |  |  |
|  | No | Putting too much demand onto domain registrants will cause bloat, cost, .... Publication of contact data is required by certain countries (Germany) and should not be demanded by ICANN for all countires. Again: privacy is an important good. Protection against harassment by government, extremists, terrorists, and spammers is an overriding concern. | Mario Heilmann |  |  |
|  | No | A proxy is a 3rd identifiable party. A privacy is a non existent party that provides a similar service. But not equal. There are legal differences in liability for example. | Arthur Zonnenberg |  |  |
|  | -- | 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 |  |  |
|  | No | Accreditation in and of itself is a nonstarter. The process should be killed. | Aaron Dalton |  |  |
|  | Yes | There are many legitimate reasons to need privacy and proxy services, such as operating home-based businesses or publishing politically contentious material, and this should not be used as a means to discriminate. | Kat Walsh |  |  |
|  | No | I disagree with this statement on a technicality: Neither term has been defined at this point in the document. | Michael Ho |  |  |
|  | Yes | With one delimiter: Since ICANN's authority is by appointment from the Federal Government, it could be viewed as a Government agency and might be subject to PII requirements under the Privacy Act. As an individual, I have some concern that the Privacy Act was included as part of the discussion (anywhere in the document). | Tim Kramer |  |  |
|  | No | Keep the Whois privacy please. | Pedro Valles |  |  |
|  | Yes | Accreditation process provides a guarantee to registrants that registrars are following correct processes and are responsible to the services they are providing. P/P services has similar relevance than other services in the Domain Name space and as such, similar guarantee, provided by the accreditation process shall be in place. | Vanda Scartezini |  |  |
| **3. Do you agree with the WG’s recommendation that: (1) the status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether proxy/privacy services are available to the registrant; (2) privacy and proxy services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals; and (3) privacy and proxy registrations should not be limited to private individuals who use their domains for non-commercial purposes? (Section 1.3.1 Recommendation 3, Section 7.1 Category C)?** | | | | | |
|  | Yes |  | Internet Commerce Association (ICA) + 70 template responders |  |  |
|  | No |  | 20 template responders |  |  |
|  | Privacy and proxy services should be available to all types of registrants, regardless of whether the registrant engages in any kind of commercial activity. |  | Google |  |  |
|  | A Privacy/Proxy framework that draws a distinction Between “Commercial” and “Non-Commercial” registrants would be inappropriate and inadministrable. We strongly support the continued availability of privacy/proxy services for non-commercial organizations, commercial organizations, and individuals. |  | CDT/ONI/PK |  |  |
|  | The mere fact that a domain name is registered by a commercial entity or by anyone conducting commercial activity should not preclude the use of P/P Services. | Note further comment on WG’s open question on this point (1.3.3). | International Trademark Association (INTA) |  |  |
|  | Agrees with the consensus view of the PPSAI WG that proxy and privacy registrations services should be available to all who seek them and use them for legal purposes |  | NCSG |  |  |
|  | Proxy usage should be barred for any registered shared private companies or gov. institution, same of course for Proxy service. When permitted, proxy service should be strictly controlled and allow fast access to Law Enforcement, Security companies, Official CERTs (like ones registered at First or Terena). |  | Julien T. |  |  |
|  | Yes to all | Additional provision: Any registrant with more than 3 complaints about copyright infringement (or other illegal actions on their website) should be considered/reviewed for loss of proxy/private registration privileges. After review by a qualified panel, this consideration could be extended by such panel to include 3 complaints in 10 years. | Kelly Andersson |  |  |
|  | Yes to some. Don't agree with disclosure of private individual's information. Therefore, you cannot treat them the same as an organization. |  | Dan Balla |  |  |
|  | No to all. Any person (includes natural and legal persons, as well as organizations and entities) registering a domain name that will be utilized to market products or merchandise to be sold to the general public for profit should not be permitted to utilize proxy/privacy services, nor should any person registering a domain name utilized for transactional purposes (a website where payment processing occurs via credit card or any other accepted form of payment). |  | Terri Stumme |  |  |
|  | Yes to all. | The consequences of publicly showing private information of small internet business are very dangerous. Competitors are capable of anything to take down a successful entrepreneur. This information will be use for abuse and actionable harm. There must be a way to protect small business owners who work at home. Not having access to privacy/ Proxy service would be devastating. Not a good idea. This measure would put their safety and their family' safety in danger. | Roxana (individual) |  |  |
|  | Yes to some | In simple terms I think the WHOIS privacy data should stay how it is now, i.e. published unless WHOIS privacy is privided by the Domain Registrar. The changes you are proposing will increase spam, remove privacy, expose commercially sensitive information and potentially wreck genuine businesses. 1. YES and it should not even be recorded whether it is an individual or organisation because this is commercially sensitive information, otherwise you help spammers who can garner that data and sent targetted spam. 2. YES, this is critical to avoid spam, retain privacy and protect commercially sensitive information 3. Yes privacy and proxy registrations should NOT be limited to private individuals who use their domains for non-commercial purposes? Once your details are out there they are sold and shared on black hat forums. Publishing the name of a domain owner without WHOIS privacy will result in a massive increase in SPAM, you will be helping the spammers. As a result of this domain owners will get more spam. This is commercially sensitive information, sites like webboar re-publish this information, consider Amber Jalink, a Canadian woman who helps local businesses, this link identifies the customers whose domains she manages http://www.webboar.com/whois-name/YW1iZXIgamFsaW5rIA== They already did this in Canada which is why her commercially sensitive information (the names of her customers) is now freely available on the above link. If you want to know the owner of an office building you have to pay for each entry in the register and the information is copyright so cannot be re-published and you don't then get the name and address of every other building they own. Well that is what happens if you publish the owner of a domain. It also affects the standing of the domain owners from Google who has already shown itself as abusive as far as data collection is concerned (Google Streetview cars breaking past home routers, stealing documents from PC's and indexing that information, plus publishing the details of routers to remove privacy with Apps like Waze.) The real villains here are the spammers, the solution to spammers is for the FTC to FOLLOW THE MONEY, every spam email has a link, that link can be traced with sites like http://tools.pingdom.com/ the link then shows the affiliate reference. What the FTC need to do is simply bring in an obligation of companies like Leadpages, Clickbank, JVZoo, WarriorForum and anyone else who pays out to provide the financial information of who they are paying to the likes of Spamhaus and Spamcop who can then provide it with evidence to the FTC for prosecution. | J Wilson |  |  |
|  | Yes to all | This is no different than our right to list or not list a phone number and/or address in a phone book. This is private information that is available to every single person who has access to the internet. You cannot allow the desires and money of a few organizations with a very narrow view of the world to dictate the privacy for billions of people. These same companies have a legal process they can go through to get their desired information. Just because that is time consuming and costly doesn't mean you can take away the right to privacy for all other organizations, companies and individuals. | Marc Schauber |  |  |
|  | No to all | I feel that the "Privacy and Proxy Services" as currently available should not be permitted. These facilities were apparently created as a new mechanism for registrars to charge for services, and NOT to protect privacy. If the registrars wanted to provide privacy, they wouldn't be charging for this. Disallow the services in full. | David Garfield |  |  |
|  | No to all | Privacy and proxy registrations should be available to the registrant regardless of their use or status. It should not be compartmentalized dependent on use and given exceptions under specific circumstances. | Dan M |  |  |
|  | Yes to all | I think that ICANN is the wrong level to deal with the issues: it should be a matter for national law, particularly as that allows differing definitions of commercial and differing levels of required disclosure appropriate local business practices. In almost all cases it will be possible to enforce this at national level | Graeme Pietersz |  |  |
|  | No to all | It's not fair to individuals, bloggers and small businesses that have their home address listed for their domain. Large corporations and bigger companies with brick and mortar addresses have the luxury of not having their personal information listed. Security and safety: Let's say I'm a blogger and I make money from my site. I'm guessing this would mean commercial. But I happen to blog about anti muslim type stuff. If my address were revealed this would put my life, my wife and kids life and even my dogs life in harms way, not to mention my property. According to the law, I have a right to feel safe and secure in my own home without distress. I'm not a lawyer but this new proposal seems like it would put certain peoples safety in harms way. And to be clear I don't blog about anti muslim stuff, it was just an example. Plus, we pay for this service. So the executives at ICANN came up with the brilliant idea of "hey, let's cut this so our revenues decrease." Any other corporation in the world would fire the people who came up with this idea. Jus sayin. | Kevin Szprychel |  |  |
|  | Yes to all | ICANN itself does not publish it's own people's names in it's own whois entry! http://whois.icann.org/en/lookup?name=icann.org So why should anyone else? Furthermore - my Limited Company (1 person) is correctly registered where I live and operate - even here, the government's own company registrar does not list my companies contact details for anyone to browse - it does not even publish contact details. Merely the registration number, and that my firms registration is still live and when the registration was first made. So if that is good enough for the government it should be good enough to merely hold a domain name - which is a very small subset of running a company. | Name withheld |  |  |
|  | Yes to some | I do not agree with the above statements due to the notes that accompany them on the actual document which are not provided here. | Christopher |  |  |
|  | Yes to some: (3) privacy and proxy registrations should not be limited to private individuals who use their domains for non-commercial purposes. |  | Gabriel de Luca |  |  |
|  | Yes to all | Privacy should be the default. Not the pay-to-play opt in option. | Not your business |  |  |
|  | Yes to some | Privacy is essential in the decentralized miasma that is the Internet. Limiting who can utilize these services would devastate the state of e-commerce and other legal online venues. | Matthew R. Steno |  |  |
|  | No to all | If you try to force your will on the people, the people will respond with violence. | Robin Hood |  |  |
|  | No to all | Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good. | Scott Jordan |  |  |
|  | Yes to all | Privacy and proxy services should be available to domain registrants regardless of the nature and use of their domains. There are several reasons for this, of which the most obvious is that one person might control a domain which is used commercially and another which is used privately; it is ridiculous to suppose that privacy could be kept on one but not the other. | Finn Ellis |  |  |
|  | Yes to some | Disagree with 1. Agree with 2 and 3. Privacy and proxy services should remain available to all under all conditions. | Shane T. |  |  |
|  | Yes to some | 1 and 2 | Nicolai Pogadi |  |  |
|  | Yes to all | It is important to uphold all possible privacy protections that are currently made available to users, small and large, by the privacy and proxy service organizations. Without this, people would receive a lot more spam and would also be subject to the whims and fancies of anyone who finds a site objectionable. | Anand S |  |  |
|  | Yes to all | I think I agree unless there is something I don't understand. Privacy is of the utmost importance to me as an individual owner and business owner of domain names. | M.B. |  |  |
|  | Yes to some | Disagree strongly with 1 - agree with 2, no opinion on 3 | Lucien Parsons |  |  |
|  | -- | 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 |  |  |
|  | Yes to all | Yes. Both private individuals and commercial organizations need privacy to allow for free speech, ability to conduct business, and ability to be safe from harassment and abuse. All parties should be entitled to the use of privacy services, but a particular consideration is that the line between private activity and commercial activity online is often blurry: for example, small home-based businesses or individual artists and writers may be considered "commercial" but have economic and privacy concerns similar to individuals. Meanwhile, many "noncommercial" activities, such as large charities, are run by nonprofits with resources and legal infrastructure comparable to large corporations, and the impact of their activity online is also no different. | Kat Walsh |  |  |
|  | Yes to all | Domain name registrants place great trust in ICANN and its accredited providers. With respect to the members of the ICANN WG, I implore you to please not abuse this trust with the weasel-words and commerce-trumps-personal-privacy attitude of corporate and intellectual property interests. | Andrew Merenbach |  |  |
|  | Yes to some | I disagree that an individual should be treated the same as a commercial or non-commercial organisation. The reason for this is that any staff member or representative of an organisation is able to go home at night and be safe. An individual or sole-trader only has their home address to give; and this opens them up immediately to serious personal risk and harrassment outside the nine to five business hours, as their telephone number will be published. If someone has a problem with a service, then they should go through the propper channels. ie. legal or oversight body. To do otherwise is to expose a family home to harassment and possible physical abuse. ie. things like hate speach should be brought before the courts rather than putting bricks through windows and petrol through letterboxes. | Michelle Knight |  |  |
|  | Yes to some | In some cases, it may be advantageous for the registrar to require a "public" interface with an organization (e.g., Public Affairs Officer or similar). Such could be required without exposing individuals' PII (e.g., use of a role or title, with an email address, phone number, or physical mailing address). | Tim Kramer |  |  |
|  | Yes to all | Keep the Whois privacy please. | Pedro Valles |  |  |
|  | No to all | I value my privacy. 'Commercial' definition way too vague. | Alisa Harris |  |  |
|  | Yes to some | Does my site constitute commercial purposes? No. You tell me! A blog that has ads, does that count? What about I sell physical goods over the phone and ship them to buyers and use a website strictly to deliver invoices and allow payment online? Does that count? | Justin Steele |  |  |
|  | Yes to some | The status of a registrant as a commercial organization, non-commercial organization, or individual should be the driving factor in whether proxy/privacy services are available to the registrant. | Dylan Henderson |  |  |
|  | Yes to all | There is no reason to discriminate the statues of registrant. whatever they are, that shall have identical rights. P/P services is a right shall be available to any registrant. | Vanda Scartezini |  |  |
|  | Yes to all | P/P should be banned. | Gary Miller |  |  |
| **4. Do you agree with the WG’s recommendation that domain names registered using a privacy or proxy service should be labeled as such in Whois? (Section 1.3.1 Recommendation 4, Section 7.1 Category B-1)?** | | | | | |
|  | Agree, and add that the "clear labeling" should be easily machine-parsable. We would consider this a negative indicator when evaluating business legitimacy. |  | John Nagle/Sitetruth |  |  |
|  | Yes |  | 55 template responders |  |  |
|  | No |  | 51 template responders |  |  |
|  | No | Not sure I understand this one ... if I look up a domain with Whois I can see if it’s private (??) | Kelly Andersson |  |  |
|  | No | No need, it is pretty obvious if it says Privacy Protected or Domains by Proxy | J Wilson |  |  |
|  | Yes | I believe, labeling private or proxy registrations to clearly show they are being kept private is fine. However, revealing the company providing that is providing the service is the first step to ending that privacy. In the interests of privacy, I therefore strongly recommend the proxy not be named. | Dr M Klinefelter |  |  |
|  | Yes | They already are. There is no confusion and these companies that have spent a ton of money to get this common practice eliminated, should be told to turn around and attempt to pay for influence elsewhere. | Marc Schauber |  |  |
|  | No | Absolutely not. WHOIS information is made public or private when the domain is registered, it should not be modified at free will, it's unfair and unjust. | Dan M |  |  |
|  | Yes | I prefer that very limited information is published in whois. Limited to a contact email is quite sufficient. | Name withheld |  |  |
|  | No | Do not understand the need to label domain names as registered via privacy or proxy services. | Christopher |  |  |
|  | No | I do not think privacy services should be regulated. There is already a market for these services and market forces will drive the best to the top and the users of those services to advertise their use themselves. Furthermore most normal internet users don't know how to use Whois so it is worthless to list there anyway. | James Ford |  |  |
|  | No | I've already stated my position that Whois in its current incarnation should not exist. All it does is create risk for those who need privacy and enable bad state actors like China and Turkey. All that should be required for getting a domain is a minimal method of contact (an email or similar) and all Whois should disclose is that that email. | Not your business |  |  |
|  | No | The only advantage I see is determining whether a given email address is reachable, but labeling it has many more repercussions. Anything handling domains might discriminate on this field, e.g. search engines may rank anonymous domains lower and SSL/TLS certificate authorities might reject these domains. It probably ends up in discrimination of domains somewhere. Crooks can use fake info because they are willing to break the law to achieve it; everyone else who wishes their personally identifiable information to be private (only available to the registrar itself, which authorities can reach) gets discriminated by such a policy. | NYB |  |  |
|  | Not really in favor, neither against |  | D. Miedema |  |  |
|  | No | You don’t get to decide | Robin Hood |  |  |
|  | Yes | Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good. | Scott Jordan |  |  |
|  | Yes | No strong opinion but this seems appropriate. | Finn Ellis |  |  |
|  | No | This would create an atmosphere of contempt for those wishing to remain anonymous online. It is a constitutional right to be anonymous when one wants to. These services should appear identical to any other non private service. More importantly many healthcare organizations use these services to transmit protected health information. Any attempt to violate this security could be seen as a violation of HIPAA under the security and privacy rules. | Jason Weinberg |  |  |
|  | No | This is clearly an additional burden on everyone involved in WHOIS maintenance, including registrars and registrants, and should therefore not be included unless clearly necessary for the good functioning of the service. In fact, the opposite is true: the WHOIS system provides contact information, not legal ownership information, and thus the legal relationship of the provided contact to the domain registrant is irrelevant. | Jason Burns |  |  |
|  | 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 | An extra label is not necessary, as long as contact information is correct. | Arthur Zonnenberg |  |  |
|  | ?? | Don’t understand | M.B. |  |  |
|  | No | I believe that when one wants to start a website, there should be no need to give up private information at all, but it should especially not be available to the general public. | Gabby Taylor |  |  |
|  | -- | 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 |  |  |
|  | No | There is no reason to make this discrimination. Marking this in WHOIS would give a signal to those looking for contact information that the registrant feels they need extra privacy--this may increase the likelihood that potential harassers and abusers will look for the information that is being hidden, and to use the publication of that information as an attack. | Kat Walsh |  |  |
|  | Yes | Provided no personally-identifiable (or personally-correlatable) information is exposed, I would agree. If two domains registered privately to the same individual would have the same identifier simply because it's the same individual, I'd say No. | Andrew Merenbach |  |  |
|  | Yes | This is not a change from today, where anyone with a pulse can tell. | Michael Ho |  |  |
|  | Yes | Keep the Whois privacy please. | Pedro Valles |  |  |
|  | No | No point. | Alisa Harris |  |  |
|  | Yes | Must be clear to registrant and other as Law Enforcement Agent that the registrant has opted to be unders P/P services, and for such this shall be stated at Whois platform. | Vanda Scartezini |  |  |
|  | No | We disagree with the WG's recommendation. Privacy and proxy services are designed to ensure a level of privacy that benefits the end user, and a designation such as this removes that benefit. | Donuts |  |  |
|  | Yes | I see nothing wrong with that recommendation. In fact most of the bigger proxy services seem to have the word "proxy" (or "privacy") somewhere in there name already. So why not making such a label mandatory? | Stefan Grunder |  |  |

**III. VALIDATION & VERIFICATION, RIGHTS & RESPONSIBILITIES, TERMS OF SERVICE, STANDARD FORMS, PROVIDER LISTING:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **5. Do you agree with the WG's recommendation that: (1) privacy/proxy customer data is to be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Specification of the 2013 RAA; and (2) in the cases where a privacy/proxy service provider is Affiliated with a registrar (as defined by the 2013 RAA), and validation and verification of the customer data has been carried out by the registrar, re-verification by the privacy/proxy service provider of the same, identical, information should not be required? (Section 1.3.1 Recommendation 5, Section 7.1 Category B-2)?** | | | | | | |
|  | | Yes |  | 51 template responders |  |  |
|  | | No |  | 49 template responders |  |  |
|  | | Yes | Based on the ability to contact the registrant as currently required concerning contact details being maintained. | James |  |  |
|  | | No | I believe the 2nd condition is true however, in the interests of privacy and the smooth running of the internet I don't believe ICANN should begin policing. If perhaps I misunderstood some parts of the WHOIS Accuracy Program Specification of the RAA 2013 and policing isn't the intention. My intent is to say that privacy is a human right that should not be infringed in the interests a few companies. | Dr M Klinefelter |  |  |
|  | | No | Not only is this overly burdensome which will force an increase in already high registry costs, but it's anti capitalism. I don't have to give my personal data and have it verified when I subscribe to online services or at restaurants or brick and mortar stores. That process is wholly unfair, unless the registrant is claiming to be a registered business or non-profit. In those cases automated online lookups could be done. | Marc Schauber |  |  |
|  | | No | Whether or not customer data is verified and the manner in which it is verified should be left to the discretion of the privacy/proxy service. | Josh Hancock |  |  |
|  | | No | There is no need to validate users if they already have an ongoing commercial relationship. There is no need to have accurate information in whois. | Name withheld |  |  |
|  | | No | This defeats the purpose of having the privacy provider. | James Ford |  |  |
|  | | No | Point two I suppose I agree with given that point one is required, but as previously stated I don't think date should be validated or verified. The identity of a domain's owner should not be part of the domain system. Anything else is likely to put freedom of speech at risk by forcing those who wish to express themselves anonymously to go through a gatekeeper who can censor their speech. | Not your business |  |  |
|  | | No | WHOIS Accuracy Specification is overly onerous. | Simon Kissane |  |  |
|  | | I disagree with (1) but agree with (2). |  | R Poss |  |  |
|  | | No | With regard to (1), no. Whois Accuracy as specified by 2013 RAA does not need to be applied to P/P providers. | Nick O’Dell |  |  |
|  | | Yes | Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good. | Scott Jordan |  |  |
|  | | Yes | No strong opinion, this is acceptable | Finn Ellis |  |  |
|  | | No | To validate privacy customer data would negate the entire purpose of the customer using the privacy service. This would destroy an entire industry. It would also open up secure data such as protected health information in transmission and could cause violations of the HIPAA privacy rule. | Jason Weinberg |  |  |
|  | | No | Requiring the adoption of a whois verfication and sharing standard like this would do little to hamper those who intend not to provide legitimate or meaningful information to the whois system with intent of malice, especially outside North America and Europe. Those seeking to to acquire a domain registration anonymously for legitimate purposes such as companies looking to preemptively prevent domain squatting without making their association to a domain visible to their competition (a company doesn't want it's competitors to know that a proxy service acting on it's behalf purchased myexamplemarketingcampaign.com or mypotentialnewwidgetname.com) will be driven to 3rd parties (already a common practice, as seen with the release of .xxx TLDs) creating needless hassle/friction/cost. The additional cost/hassle would disproportionately impact individuals with legitimate motives for desiring anonymity (owning something like mybeerblog.something isn't something most people would want showing up on a pre-employment background check). | Gregory Antonellis |  |  |
|  | | No | (1): I believe that the WHOIS Accuracy Specification is fundamentally misguided, and should be demoted to a recommended practice rather than a requirement. For example, email is not a guaranteed delivery mechanism, so it is inappropriate to depend on email as a primary contact, and perhaps even inappropriate to mandate in contact information. The current Specification assumes otherwise for all of these. (2): No objection. | Jason Burns |  |  |
|  | | 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 | Re: Recommendation 1: Third-party handling and verification of customer data defeats the entire purpose of the privacy/proxy service, which I believe should be a relationship only between the service provider and the customer, and I'm certain there are many others who agree with this sentiment. From my understanding, the current low standards for disclosure will do more harm than good to individuals, may very well open them up to harm and harassment from "doxxers" and other unscrupulous people who may want to silence their critics physically or otherwise. The current language of this document places the metaphorical keys in the hands of “Law enforcement authority” as liberally defined by the GNSO Initial Report document in Section 1.3.1 Recommendation 1, which more or less the door for privileged special interest organizations to encroach on the individual right to privacy. | C. |  |  |
|  | | No | Spam issues can cause failure to re-verify. Spam needs to be solved. Actually, it is easier to verify anonymous data than public email data. I think Godaddy should be prohibited from demanding privacy protection to be removed before changing domain registrars. Never should privacy be lifted, this should be illegal. I did have a good reachable private email address, and during domain registrar transfer this email became known and spammed. This issues MUST be solved. Court orders may be an exception. Destroying a bona fide honest email address caused extreme hardship and made normal contact impossible. It also makes me weary to provide good spam free email contact to the Anonymizer service Godaddy (and maybe others) does this to prevent registrar changes. They hold their domain holders hostage. | Marik Heilmann |  |  |
|  | | No | From the Netherlands and 10 Dutch ICANN accredited registrars, we have several objections to the WHOIS Accuracy Specification of the 2013 RAA. We do agree that re-verification should not be required on identical data. | Arthur Zonnenberg |  |  |
|  | | -- | Please keep my information private and unavailable to anyone that I have not authorized to have it!! | 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 |  |  |
|  | | No | The WHOIS accuracy specification is fundamentally flawed. | Aaron Dalton |  |  |
|  | | No | I cannot trust or evaluate this because it incorporates excessive language by reference. | Michael Ho |  |  |
|  | | Yes | With at least one of the registrars that I've employed, re-verification has been a nuisance. | Tim Kramer |  |  |
|  | | No | This proposal only makes sense if there is a very high level of certainty that the original data were accurate and there has been no material change of circumstances since. | Children’s Charities Coalition on Internet Safety |  |  |
|  | | No | The WHOIS Accuracy Program is useless (criminals will still use fake data) and harmful (it makes registrants vulnerable to phishing attacks). | Sebastian Broussier |  |  |
|  | | Yes | Both statements follow a correct logic. | Vanda Scartezini |  |  |
|  | | Yes | A corrupt registrar will just run a corrupt P/P service. | Gary Miller |  |  |
|  | | No |  | Homer |  |  |
| **6. Do you agree with the WG's recommendation that: (1) all rights, responsibilities and obligations of registrants, privacy/proxy service customers and service providers need to be clearly communicated in the privacy/proxy registration agreement, including a provider’s obligations in managing those rights and responsibilities and any specific requirements applying to transfers and renewals of a domain name; and (2) all privacy/proxy service providers must disclose to their customers the conditions under which the service may be terminated in the event of a transfer of the domain name, and how requests for transfers of a domain name are handled? (Section 1.3.1 Recommendation 6, Section 7.1 Category B-3)?** | | | | | | |
|  | | Yes |  | 83 template responders |  |  |
|  | | No |  | 29 template responders |  |  |
|  | | Yes with conditions (but none specified and no comment added) |  | 2 template responders |  |  |
|  | | Yes | Um, obvious. Come on... if it's not clear and in the contract, it doesn't exist, period! | Marc Schauber |  |  |
|  | | Yes | Yes, they absolutely have to be clearly communicated, nothing should be done behind closed doors, from what I am understanding this to say. | Dan M |  |  |
|  | | Yes with conditions | I do not entirely agree with everything. A good compromise would be to apply this to privacy services provided by registrars (most of them) but do not attempt to prevent other parties from providing such services standalone. | Graeme Pietersz |  |  |
|  | | Yes with conditions | As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order. | Not your business |  |  |
|  | | Yes with conditions | 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 | Not something that should be under ICANN regulation | D. Miedema |  |  |
|  | | No | I disagree with this part the most. As an individual, I simply don't want my personal information to be readily available to the Internet at large, and I don't want privacy companies to have to disclose that information so easily. Nor do I want the additional bureaucratic overhead to result in additional costs for me. | Aaron Holmes |  |  |
|  | | Yes | Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good. | Scott Jordan |  |  |
|  | | No | Since a providers disclosure of customer information may violate the privacy and security rule under HIPAA. It would be a gross violation of federal law to enforce service provider to disclose customers. This could lead to hacking attacks or other security violations. | Jason Weinberg |  |  |
|  | | 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 |  |  |
|  | | Yes with conditions | In the case of a transfer, the service cannot be guaranteed or forced. If a reseller does not offer the service, a client transferring to that reseller in the market cannot force the reseller via any ICANN policy or contract. | Arthur Zonnenberg |  |  |
|  | | -- | 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 |  |  |
|  | | Yes with conditions | Since ICANN is a Government-appointed entity, I would suspect most that most, if not all, provisions of the Privacy Act would apply. (The Privacy Act is not even referenced in the Report.) It's always been a point of concern that many registrars treat privacy as an "opt in" measure and leverage it as a vehicle for profit. | Tim Kramer |  |  |
|  | | Yes | Domain registrars have done bad job of disclosing restrictions on transfer of private domains. Either, rules should be amended to allow transfer of private domains, or registrars should be mandated to disclose upfront that domains may not be transferred without having privacy turned off in large print, not hidden in the find print of the end user agreement. | Byunghoon Choi |  |  |
|  | | Yes | P/P services are additional services to whom decided to make such choice. hence, all obligations and responsibilities and rights for both sides shall be clearly stated at the signed agreement. Basic services supported by RAA will continue to be valid and the interface between Registrar and P/P Service Provider shall also be clear into the P/P agreement with registrant. Disclosure, Publication, termination, transfer or renew shall also be include in such agreement. | Vanda Scartezini |  |  |
| **7. Do you agree with the WG's recommendation that accredited P/P service providers must include on their websites, and in all Publication and Disclosure-related policies and documents, a link to either a standardized request form or an equivalent list of specific criteria that the provider requires in order to determine whether or not to comply with third party requests, such as for the Disclosure or Publication of customer identity or contact details? (Section 1.3.1 Recommendation 7, Section 7.1 Category F)?** | | | | | | |
|  | | No |  | 41 template responders |  |  |
|  | | Yes |  | 51 template responders |  |  |
|  | | No | This will be abused, the only people who should be able to request disclosure should be: FTC Spamhaus Spamcop Court Order. | J Wilson |  |  |
|  | | Yes, but I believe local country laws may be held higher than these policies when appropriate. |  | Dr M Klinefelter |  |  |
|  | | -- | Publication and disclosure requests will be abused by third parties. | Sam |  |  |
|  | | Yes | They should also be emailing and contacting current customers in the circumstances this occurs. It is misleading to just put a link in a standardized document or form on their website. | Dan M |  |  |
|  | | Yes with conditions | I have no objection to law enforcement seeking such information - I have no choice anyway. All others can contact me through my websites email or my whois entry email. There is no reason whatsoever that anyone should be given my name, home phone number and home address. | Name withheld |  |  |
|  | | No | Privacy or proxy services should not be required to provide personal info. | Christopher |  |  |
|  | | No | This should not be regulated. A law enforcement entity will know how to get in touch and the requirements to request private information (valid court order) | James Ford |  |  |
|  | | Yes with conditions | As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order. | Not your business |  |  |
|  | | 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 |  |  |
|  | | Yes with conditions | The former only if it clearly lists which items are required (i.e. the latter). | Alex Xu |  |  |
|  | | Yes | If the recommendation as a whole passes, yes, but I do not think it should pass. | Anonymous Turtle |  |  |
|  | | Yes, but in addition to a standard process for requesting disclosure/publication, there also needs to be a standard process for opposing disclosure/publication. |  | Nick O’Dell |  |  |
|  | | Yes | Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good. | Scott Jordan |  |  |
|  | | 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 |  |  |
|  | | Yes with conditions | Where the only parties using said form are authorized by local authorities to do so. Quasi-governmental or similar is too vague, not in line with privacy law, and unacceptable. | Arthur Zonnenberg |  |  |
|  | | Yes with conditions | Clients of accredited P/P service providers need to be protected in the event of frivolous litigation requests to P/P service providers, directed at the P/P service provider's client(s). | Adam Creighton |  |  |
|  | |  | The decision should be mine alone, as the information is mine alone. | 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 |  |  |
|  | | Yes with conditions | The accreditation program is a fundamental issue. It should not exist! | Aaron Dalton |  |  |
|  | | Yes | Commercial organisations that run from listed buildings should actually, in my personal opinion, not be granted the right to be protected. This service is currently being abused by spammers operating as, "marketing companies," who are then impossible to trace in order to report to authorities. Rule of thumb - persons name, allow the option to be protected. Business name, not protected. | Michelle Knight |  |  |
|  | | Yes with conditions | It's probably a good idea to include a limitation of "in accordance with the registrar's host/parent country". | Tim Kramer |  |  |
|  | | No | There is no need for more burdenous regulation. This is what the court system is designed for. | Gladys Portales |  |  |
|  | | No | Private should mean PRIVATE - not "Private until further notice". | Dylan Henderson |  |  |
|  | | Yes | Transparence is key. Make it available to customer at their website or at other way where registrant will access to make its option is fundamental. I would not enphazise "all publication". being complete under the link provided at the P/P Services Provider, look suffice for me. | Vanda Scartezini |  |  |
|  | | Yes | If the request for disclosure of any personal data, identity or contact details does not come with a valid and legal court order, any such request must be forwarded to the registrant to enable them to object. Since a court order cannot be sent through any online request form, no such request must be complied with without first notifying the registrant and allowing them to object. And no such request must be granted without following some very strict and clear rules which the registrant must have agreed with at some point (usually during the registration of the domain). | Stefan Grunder |  |  |
|  | | Yes | But of course the P/P providers will just ignore requests. | Gary Miller |  |  |
| **8. Do you agree that the following additional provisions regarding Disclosure and Publication should be included in the Terms of Service: (1) clarification of when there is a reference to Publication requests (and their consequences) and when to Disclosure requests (and their consequences); (2) explanation of the meaning and consequences of Publication; (3) the specific grounds upon which a customer’s details may be Disclosed or Published or service suspended or terminated; and (4) clarification as to whether or not a customer: (i) will be notified when a provider receives a Publication or Disclosure request from a third party; and (ii) in the case of Publication, whether the customer may opt to cancel its domain registration prior to and in lieu of Publication or Disclosure? (Section 1.3.1 Recommendation 8, Section 7.1 Category F)?** | | | | | | |
|  | Yes | |  | 62 template responders |  |  |
|  | No | |  | 24 template responders |  |  |
|  | Yes to some (but none listed and no comments) | |  |  |  |  |
|  | Yes, but Customer MUST be notified when provider receives a publication or disclosure request from a third party | |  | John Lawrence |  |  |
|  | Yes, esp (3) & (4) | |  | Kelly Andersson |  |  |
|  | Yes | | I also think that disclosure should only be made to valid requestors and law enforcement agencies or consumer protection groups via some form of secured email communication system and not in the whois database itself. | Reagan Lynch |  |  |
|  | Yes | | These are the ICANN's recommended best practices for P/P providers. Again I don't feel it's ICANN's place to police these policies. | Dr M Klinefelter |  |  |
|  | Yes | | Customers must have full transparency on the conditions under which their information may be published or disclosed. There should be almost no such conditions. | Sam |  |  |
|  | Yes (see comment) | | Yes, also contacting the customer, again, is important. | Dan M |  |  |
|  | Yes with conditions | | As above - not all privacy providers need by accredited, only those combining registrar and privacy services. | Graeme Pietersz |  |  |
|  | No | | I have no objection to law enforcement seeking such information - I have no choice anyway. There is no reason whatsoever that any servie provider should disclose my name, home phone number and home address. They may pass along email communications that I may chose to answer. | Name withheld |  |  |
|  | No | | Do not agree with the reasons for or the persons able to request personal information from privacy or proxy services. | Christopher |  |  |
|  | No | | These are good recommendations but shouldn't be mandatory and privacy services should adopt them voluntarily. | James Ford |  |  |
|  | Yes with conditions | | As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order. | Not your business |  |  |
|  | 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 |  |  |
|  | Yes to some | | Customers should always receive notification unless prohibited by law. | Alex Xu |  |  |
|  | Yes to some: Disclosure and delay for responsive litigation must be mandatory in all circumstances. Disclosure should be prohibited except when legally ordered. | |  | Private |  |  |
|  | Yes to some | | (2), (3), (4) seem reasonable. (1) seems like unnecessary busywork. | Nick O’Dell |  |  |
|  | Yes | | Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good. | Scott Jordan |  |  |
|  | Yes to some | | I disagree with 4.i, a customer should always be notified. Recent news have shown that law enforcement entities tend to misuse the powers they are granted, or not even that, in some cases. There should be very strict rules around not notifying a customer. 4.ii should also be an option for a customer. In general, it must remain possible (and encouraged) for privacy and proxy providers to provide the strongest guarantees they can make. The process currently works, and an accreditation process that would harm existing providers (and their customers) is unacceptable. | Lucas Stadler |  |  |
|  | 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 | | Not until these policies have been improved and approved. | Arthur Zonnenberg |  |  |
|  | Yes to some | | For (4)(ii), I am concerned about frivolous litigious attacks from disconnected legal entities representing IP owners, and individuals needing to cancel their domain registration prior to and in lieu of Publication or Disclosure, because they are fearful of or cannot afford litigious engagement. I see this process being abused by IP rights holders looking to inappropriately expand their brand presence via domain registration. | Adam Creighton |  |  |
|  | -- | | They should not be giving out my information in any case unless I have authorized it or they have a legitimate subpoena from law enforcement. | M.B. |  |  |
|  | Yes with conditions | | If the Registrar's criteria has been met, the Disclosure and/or Publication of the WHOIS data to a non-law enforcement third-party should be limited to the equivalent of a Public Records search. For example, in the United States you can search the public business records of the California Secretary of State. A search for Google Inc. discloses the entity name and mailing address. But it does not expose the private email address or phone numbers of the business owner or it's employees. In addition to the basic contact information the public business records search includes the "Agent for Service of Process" which is the legal representative of the entity. I assert the ICANN P/P Service Regulations should adopt a similar policy directing Registrar's to only disclose basic contact information and "Agent for Service of Process" contact information to a non-law enforcement third-party. | Reid Baker |  |  |
|  | -- | | 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 |  |  |
|  | Yes with conditions | | Terms of Service are already impenetrable. If you are insistent on an "accurate" WHOIS database, then the only thing you should do is verify that the contact information a P/P provider gives is accurate. Other than that, stay the hell out of the industry. You have no role to play there. | Aaron Dalton |  |  |
|  | Yes with conditions | | I would much rather that providers notify customers/registrants of \*ALL\* Publication or Disclosure requests, making clarification as to whether a customer will be notified irrelevant. | Jawala |  |  |
|  | Yes | | This, in my view shall be clearly stated - all those - at the link provided by P/P provider as stated above. | Vanda Scartezini |  |  |
|  | Yes to some | | 4(ii) should not be allowed | Gary Miller |  |  |
| **9. Do you agree that the following should be recommended as "best practices" for P/P service providers: (1) they should facilitate and not obstruct the transfer, renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the Expired Registration Recovery Policy and transfers to another registrar; (2) they should use commercially reasonable efforts to avoid the need to disclose underlying customer data in the process of renewing, transferring or restoring a domain name; and (3) they should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved online location) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication? (Section 1.3.1 Recommendation 9, Section 7.1 Category B-3)?** | | | | | | |
|  | Support recommendation that providers should facilitate the transfer, renewal and restoration of domain names | |  | Google |  |  |
|  | Yes to some (no comments) | |  | 2 template responders |  |  |
|  | Yes with conditions (none specified) | |  | 1 template responder |  |  |
|  | No | |  | 22 template responders |  |  |
|  | Yes | |  | 66 template responders |  |  |
|  | Yes | | If the privacy service is apart of a registrar then it should be made clear that by transferring away from that registrar privacy service will be deactivated and contact information will be made public. The losing registrar should not be obligated to keep the contact data private. If a third-party privacy service is used then the privacy should remain in place. | Reagan Lynch |  |  |
|  | Yes | | To this end, WHOIS privacy should extend when the domain has expired and until released. Many registrars remove the service in the grace period and even redirect the domain to a page where the registrar makes money displaying ads. | J Wilson |  |  |
|  | Yes with conditions - These and all rules, laws, regulations, clauses, etc must be written so an average person can 100% understand them. No legalese, no jargon meant to fool readers and no loopholes for big companies to gain access to data without prior notification and an appeal process before any personal data would be shared with anyone, regardless of how much money they spend trying to buy these rules that they want. | |  | Marc Schauber |  |  |
|  | Yes (see comment) | | I don't like the word, "commercially reasonable", disclosure should be made aware to the customer at all times unless it is a legal court order or warrant. | Dan M |  |  |
|  | Yes to some. I don't see (3) as needed. I agree with (1), but not with (2), because a P/P service should NEVER disclose the data, not to make only "commercially reasonable efforts". | |  | Adrian Valeriu Ispas |  |  |
|  | Yes to some – on (3) I think Google will assist more than ICANN will. | |  | Name withheld |  |  |
|  | Yes to some – for (3) they should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved online location) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication? | |  | Gabriel de Luca |  |  |
|  | Yes to some | | Advertising ICANN shouldn’t be a best practice | James Ford |  |  |
|  | Yes with conditions | | As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order. | Not your business |  |  |
|  | 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 |  |  |
|  | Yes with conditions | | I don't understand why a P/P provider would intentionally obstruct these procedures when ordered by their customer. If this means that ordinarily, the customer would have to notify the P/P provider before initiating the action, and this item would mean disclosure of information not ordinarily transferred, I object. | Anonymous Turtle |  |  |
|  | Yes to some | | (1) and (2) seem like clear wins. (3) is unnecessary given Section 1.3.1 Recommendation 8, Section 7.1 Category F, subpoint 2 | Nick O’Dell |  |  |
|  | Yes | | We need a higher standard than "commercially reasonable." Your profit is not worth someone's privacy. Explanatory language should be in terms that are accessible to anyone the policy is going to affect, including those who may not be highly literate in English or any language. | Finn Ellis |  |  |
|  | 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 |  |  |
|  | Yes | | Absolutely. Privacy protection must be mandatory until the end of transfer to another registrar. Registrar's requirement to remove privacy (Godaddy) is extreme hardship, dangerous, and defeats the entire purpose of privacy. | Mario Heilmann |  |  |
|  | No | | Privacy can be an obstruction for transfer if either party does not offer the service. The P/P service provider should not decide or make efforts on whether said privacy is to be upheld or not. If a legitimate and legal need to disclosure is submitted, it must be executed. The distinction between Disclosure and Publication is ripe for abuse by those parties requesting Disclosure in bulk. Parties should not generally be allowed, unless they are local authority binded by law. | Arthur Zonnenberg |  |  |
|  | -- | | My information should be protected at all times! | 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 |  |  |
|  | No | | Get the hell out of the P/P business. Beyond ensuring they themselves provide accurate contact information, there is nothing more I as an individual want you to do about P/P services! | Aaron Dalton |  |  |
|  | Yes to some | | Agree to 1 and 2. Disagree with 3: the authoritative definitions and meanings should be codified upon accreditation. Putting them on a separate Web site means that they can be changed without approval of the registrar. | Andrew Merenbach |  |  |
|  | Yes with conditions | | 1. "or other ICANN-approved online location" puts an undue burden on the P/P provider to know where your link is at all times, even after you move it. 2. The authoritative definitions must form part of a document such as you provide and must not be subject to arbitrary future change, which is easy to do with a link-in-motion. | Michael Ho |  |  |
|  | Yes | | As I have state, in my view conditions under RAA, and best practices followed by accredited registrars shall remain valid for those registrants that have opted to have P/P services. As such, P/P services provider shall offer conditions stated in 1 and 2, allowing registrants to understand what they as entitle to and which are their rights and obligations. | Vanda Scartezini |  |  |
|  | Yes with conditions | | For (3), where the working group definitions are used. | Donuts |  |  |
|  | Yes to some | | (2) is in contradiction to (1) | Gary Miller |  |  |

1. This is the first part of the Public Comment Review Tool for the PPSAI WG. As more collation is completed, other Parts will be prepared and circulated for the WG’s review and deliberations. [↑](#footnote-ref-1)