Privacy/Proxy Service Provider Accreditation
Law Enforcement Authority Framework: Requirements and Recommendations [Draft Discussion Document]

Summary: In its Helsinki Communique (June 2016), the Governmental Advisory Committee advised the ICANN Board to ensure that GAC concerns are effectively addressed in the implementation phase of the Privacy/Proxy Service Provider Accreditation Program to the greatest extent possible. The GAC advised that its input and feedback should be sought out as necessary in developing a proposed implementation plan, including through participation of the GAC Public Safety Working Group (PSWG) on the Implementation Review Team (IRT). In response, the ICANN Board has directed the ICANN organization to continue to encourage dialogue between the IRT and the PSWG to address GAC concerns during implementation, to the extent that so doing is consistent with Policy Recommendations.

Proposed Process: ICANN recommends that the PSWG designate a working group to develop a strawman proposal, in consultation with an IRT sub-team, for a framework for Privacy and Proxy Service providers to follow when receiving a request for disclosure or relay from an entity that falls within to-be-defined scope of "law enforcement authority."

Requested Timeline: This strawman should be completed and distributed to the IRT subteam for discussion before ICANN58. This will provide time for face-to-face discussion about the proposed framework between the PSWG and the IRT at ICANN58.

- Mid-January 2017—kickoff meeting with PSWG
- Jan-Feb 2017—GAC PSWG develops strawman proposal
- Feb 2017-strawman distributed to IRT subteam for discussion
- March 2017—F2F discussion about strawman at ICANN58

Guiding Principles: This framework should be consistent with the Final Recommendations of the PDP Working Group. The framework proposed by the PSWG for discussion within the IRT may not contradict any of the Final Recommendations. A list of relevant recommendations from the PDP working group is included in Annex A of this document. If the PSWG wishes to re-raise a Policy issue that has already been examined during the PDP WG deliberations or raise a new Policy issue, it must use a process other than this IRT to do so. This IRT is only authorized to implement requirements that are consistent with the Final Recommendations developed by the GNSO PDP process.

ICANN recommends that the PSWG consult the elements of the IP disclosure framework, included as Annex B, and strive to follow a similar overall model so that Privacy and Proxy Service providers can use the same channels for processing these requests (even if the requirements differ for each).

For example, it is expected that Privacy and Proxy Service providers will have the option to use a standard information request form for all third-party requests (to be developed during implementation). As a result, this framework should propose to utilize that channel.

This framework should contain:

- A definition of how law enforcement authorities will qualify for this process, with the understanding that this may need to be geographically-limited;
- A process for PP service providers' acceptance of these requests from LEA (please attempt to work within the processes currently being designed—for example, "law enforcement" could be one of the options on the PP service provider's standard "information request" form, that will be created via the IRT process);
- Requested timelines required for PP provider to respond to LEA requests;
- A description of the information a qualifying LEA entity must submit to support its request to the PP provider (for example, see PICS list (see specification 11); this could form the basis of a list of alleged misconduct that could qualify for PP action under the LEA framework); and
- A process for resolving disputes arising from this framework (for example, the IP framework in Annex B includes a provision that requires third-party requesters to agree "to submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or rights holder's knowing misuse of information disclosed to it in response to its request.")

ANNEX A: Final PDP Recommendations Relevant to LEA Framework/Abuse Reporting

Final Report available at: https://gnso.icann.org/en/issues/raa/ppsai-final-07dec15-en.pdf

Definition: "Law Enforcement Authority" means law enforcement, consumer protection, quasigovernmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the privacy or proxy service provider is established or maintains a physical office. This definition is based on Section 3.18.2 of the 2013 Registrar Accreditation Agreement, which provision spells out a registrar's obligation to maintain a point of contact for, and to review reports received from, law enforcement authorities14; as such, the WG notes that its recommendation for a definition of "law enforcement authority" in the context of privacy and proxy service accreditation should also be updated to the extent that, and if and when, the corresponding definition in the RAA is modified. (See final report, p. 8)

Regarding the relay of Electronic Communications (See Final Report, p. 13-14): At a minimum, Privacy and Proxy Service providers must relay all electronic requests received (including those received via emails and web forms) from law enforcement authorities containing allegations of domain name abuse (i.e. illegal activity).

In all cases, Privacy and Proxy Service providers must publish and maintain a mechanism (e.g. designated email point of contact) for Requesters to contact to follow up on or escalate their original requests.

Regarding the confidentiality of LEA requests: Based on input received, the WG recommends that accredited P/P service providers should comply with express requests from LEA not to notify a customer where this is required by applicable law. However, this recommendation is not intended to prevent providers from either voluntarily adopting more stringent standards or from cooperating with LEA (See Final Report p.16).

Regarding any future LEA framework: In the event that a Disclosure Framework is eventually developed for LEA requests, the WG recommends that the Framework expressly include requirements under which at a minimum: (a) the Requester agrees to comply with all applicable data protection laws and to use any information disclosed to it solely for the purpose to determine whether further action on the issue is warranted, to contact the customer, or in a legal proceeding concerning the issue for which the request was made; and (b) exempts Disclosure where the customer has provided, or the P/P service provider has found, specific information, facts, and/or circumstances showing that Disclosure will endanger the safety of the customer. (See Final Report p. 16).

ANNEX B: Illustrative Disclosure Framework Applicable to Intellectual Property Rights-Holder Disclosure Requests

By facilitating direct communication among Requesters, Providers, and Customers, this policy serves the public interest and seeks to balance the interests of concerned parties. It aims to give Requesters a higher degree of certainty and predictability as to if, when, and how they can obtain disclosure; to give Providers flexibility and discretion to act on requests for disclosure and not require that disclosure automatically follow any given request; and to include reasonable safeguards and procedures to protect the legitimate interests and legal rights of Customers of Providers. At an appropriate time after implementation of these accreditation standards and periodically thereafter, the Working Group recommends a review to determine whether these three objectives have been met and fairly balanced, as further described in Recommendation #19 of the Working Group's Final Report.

Policy Scope:

The following procedures were developed by the Working Group to apply to requests made by intellectual property rights-holders or their authorized representatives. The WG has not developed a similarly detailed process for other types of Requesters, e.g. law enforcement authorities or consumer protection agencies.

Given the balance that this Policy attempts to strike, evidence of the use of high-volume, automated electronic processes for sending Requests or responses to Requests (without human review) to the systems of Requesters, Providers, or Customers in performing any of the steps in the processes outlined in this Policy shall create a rebuttable presumption of non-compliance with this Policy.

I. Provider Process for Intake of Requests

- Provider will establish and publish a point of contact for submitting complaints that registration or use of a domain name for which the Provider provides privacy/proxy services infringes copyright or trademark rights of the Requester. The point of contact shall enable all the following information (in II below) to be submitted electronically, whether via email, through a web submission form, or similar means. Telephonic point of contact may also be provided.
- Nothing in this document prevents a Provider from implementing measures to optimize or manage access to the Request submission process. This could include:
  i. Requiring Requesters to register themselves and/or their organizations with Provider.
  ii. ii. Authenticating complaint submissions as originating from a registered Requester (e.g., log- in, use of pre-identified e-mail address).

iii. Assessing a nominal cost-recovery fee for processing complaint submissions, or to maintain Requester account so long as this does not serve as an unreasonable barrier to access to the process.
iv. Qualifying Requesters meeting certain reliable criteria as "trusted Requesters" whose requests would be subject to a streamlined process.
v. Revoking or blocking Requester access to the submission tool for egregious abuse of the tool or system, including submission of frivolous, vexatious, or harassing requests, or numerous Requests that are identical, i.e., that concern the same domain name, the same intellectual property, and the same Requester.

- Nothing in this document prevents Providers from sharing information with one another regarding Requesters who have been revoked or blocked from their systems or who have engaged in misconduct under this Policy, including frivolous or harassing requests.
- Nothing in this document prevents a Provider from adopting and implementing policies to publish the contact details of Customers in WHOIS, or to terminate privacy/proxy service to a Customer, for breach of Service Provider's published Terms of Service, or on other grounds stated in the published Terms of Service, even if the criteria outlined in this document for a Request have not been met.

II. Request templates for Disclosure

A. Where a domain name allegedly infringes a trademark

Requester provides to Provider verifiable evidence of wrongdoing, including:

1) The domain name that allegedly infringes the trademark;

2) Evidence of previous use of a relay function (compliant with the relevant section of accreditation standards regarding Relay) to attempt to contact the Customer regarding the subject matter of the request, if any, and of any responses thereto, if any;

3) Full name, physical address, email address, and telephone number of the trademark holder, and for legal entities, the country where incorporated or organized;

4) Authorized legal contact for trademark holder and his/her name, title, law firm, if outside counsel, physical address, email address and telephone number for contact purposes;

5) The trademark, the trademark registration number (if applicable), links to the national trademark register where the mark is registered (or a representative sample of such registers in the case of an internationally registered mark), showing that the registration is currently in force (if applicable), and the date of first use and/or of application and registration of the mark; and

6) A good faith statement, either under penalty of perjury or notarized or accompanied by sworn statement ("Versicherung an Eides statt"), from either the trademark holder or an authorized representative of the trademark holder, that:

a) Provides a basis for reasonably believing that the use of the trademark in the domain name

i. allegedly infringes the trademark holder's rights; and

ii. is not defensible.

b) States that Requester will comply with all applicable data protection laws while retaining Customer's contact details and will use Customer's contact details only:

i. to determine where further action is warranted to resolve the issue;

ii. to attempt to contact Customer regarding the issue; and/or

iii. in a legal proceeding concerning the issue; and

c) Agrees that the Requester and trademark holder will submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or trademark holder's knowing misuse of information disclosed to it in response to its request.

7) Where the signatory is not the rights holder, he/she must attest that he/she is an authorized representative of the rights holder, capable and qualified to evaluate and address the matters involved in this request, and having the authority to make the representations and claims on behalf of the rights holder in the request, including the authority to bind the rights holder to the limitations on the use of Customer data once disclosed.

8) Where the signatory is not the rights holder, an officer of the rights holder (if a corporate entity) or an attorney of the rights holder, and the Provider has a reasonable basis to believe that the Requester is unauthorized to act on behalf of the rights holder or seeks to verify a new or unknown Requester, the Provider may request, and the Requester shall provide, sufficient proof of authorization.

B. Domain name resolves to website where copyright is allegedly infringed

Requester provides to Provider verifiable evidence of wrongdoing, including:

1) The exact URL where the allegedly infringing work or infringing activity is located, or a representative sample of where such work or activity is located;

2) Evidence of previous use of a relay function (compliant with the relevant section of accreditation standards regarding Relay) to attempt to contact the Customer with

regard to the subject matter of the request, if any, and of any responses thereto, if any. Requesters are also encouraged (but not required under this Policy) to provide evidence of previous attempts to contact the web host or the domain name registrar with regard to the subject matter of the request, if any, and of any responses thereto, if any;

3) Full name, physical address, email address, and telephone number of the copyright holder; and for legal entities, the country where incorporated or organized;

4) Authorized legal contact for the copyright holder and his/her name, law firm, if outside counsel, physical address, email address and telephone number for contact purposes;

5) Information reasonably sufficient to identify the copyrighted work, which may include, where applicable, the copyright registration number, and the country where the copyright is registered;

6) If possible, the exact URL where the original content is located (if online content) or where the claim can be verified; and

7) A good faith statement, either under penalty of perjury or notarized or accompanied by sworn statement ("Versicherung an Eides statt"), from either the copyright holder or an authorized representative of the copyright holder, that:

   a) Provides a basis for reasonably believing that the use of the copyright content on the website
      i. infringes the copyright holder's rights; and
      ii. is not defensible.

   b) Provides a basis for reasonably believing that the copyright protection extends to the locale the website targets

   c) States that Requester will comply with all applicable data protection laws while retaining Customer's contact details and will use Customer's contact details only:
      i. to determine whether further action is warranted to resolve the issue;
      ii. to attempt to contact Customer regarding the issue; and/or
      iii. in a legal proceeding concerning the issue; and

   d) Agrees that the Requester and the copyright holder will submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or copyright holder's knowing misuse of information disclosed to it in response to its request.

8) Where the signatory is not the rights holder, he/she must attest that he/she is an authorized representative of the rights holder, capable and qualified to evaluate and address the matters involved in this request, and having the authority to make the representations and claims on behalf of the rights holder in the request, including the authority to bind the rights holder to the limitations on the use of Customer data once disclosed.
9) Where the signatory is not the rights holder, an officer of the rights holder (if a corporate entity) or an attorney of the rights holder, and the Provider has a reasonable basis to believe that the Requester is unauthorized to act on behalf of the rights holder or seeks to verify a new or unknown Requester, the Provider may request, and the Requester shall provide, sufficient proof of authorization.

C. Domain name resolves to website where trademark is allegedly infringed

Requester provides to Provider verifiable evidence of wrongdoing, including:

1) The exact URL where the allegedly infringing content is located;

2) Evidence of previous use of a relay function (compliant with the relevant section of accreditation standards regarding Relay) to attempt to contact the Customer with regard to the subject matter of the request, if any, and of any responses thereto, if any. Requesters are also encouraged (but not required under this Policy) to provide evidence of previous attempts to contact the web host or the domain name registrar with regard to the subject matter of the request, if any, and of any responses thereto, if any;

3) Full name, physical address, email address, and telephone number of the trademark holder; and for legal entities, the country where incorporated or organized;

4) Authorized legal contact for the trademark holder and his/her name, law firm, if outside counsel, physical address, email address and telephone number for contact purposes;

5) The trademark, the trademark registration number (if applicable), links to the national trademark register where the mark is registered (or a representative sample of such registers in the case of an internationally registered mark), showing that the registration is currently in force (if applicable), and the date of first use and/or of application and registration of the mark; and

6) A good faith statement, either under penalty of perjury or notarized or accompanied by sworn statement (“Versicherung an Eides statt”), from either the trademark holder or an authorized representative of the trademark holder, that:

a) Provides a reasonable basis for believing that the use of the trademark on the website

i. infringes the trademark holder's rights; and

ii. is not defensible.

b) States that Requester will comply with all applicable data protection laws while retaining Customer's contact details and will use Customer's contact details only:

i. to determine whether further action is warranted to resolve the issue;

ii. to attempt to contact Customer regarding the issue; and/or

iii. in a legal proceeding concerning the issue; and

c) Agrees that the Requester and the trademark holder will submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or the trademark holder's knowing misuse of information disclosed to it in response to its request.

7) Where the signatory is not the rights holder, he/she must attest that he/she is an authorized representative of the rights holder, capable and qualified to evaluate and address the matters involved in this request, and having the authority to make the representations and claims on behalf of the rights holder in the request, including the authority to bind the rights holder to the limitations on the use of Customer data once disclosed.

8) Where the signatory is not the rights holder, an officer of the rights holder (if a corporate entity) or an attorney of the rights holder, and the Provider has a reasonable basis to believe that the Requester is unauthorized to act on behalf of the rights holder or seeks to verify a new or unknown Requester, the Provider may request, and the Requester shall provide, sufficient proof of authorization.

III. Provider Action on Request

Upon receipt of the verifiable evidence of wrongdoing set forth above in writing, Provider will take reasonable and prompt steps to investigate and respond appropriately to the request for disclosure, as follows:

A. Promptly notify the Customer about the complaint and disclosure request and request that the Customer respond to Provider within 15 calendar days. Provider shall advise the Customer that if the Customer believes there are legitimate reason(s) to object to disclosure, the Customer must disclose these reasons to the Provider and authorize the Provider to communicate such reason(s) to the Requester (so long as doing so will not endanger the safety of the Customer, as outlined in Section III(c)(vi)); and

B. Within 5 business days after receiving the Customer's response, or within 2 business days after the time for Customer's response has passed, Provider shall take one of the following actions:

   i. Disclose to Requester using secure communication channels the contact information it has for Customer that would ordinarily appear in the publicly accessible WHOIS for nonproxy/privacy registration; or
   ii. State to Requester in writing or by electronic communication its specific reasons for refusing to disclose.
   In exceptional circumstances, if Provider requires additional time to respond to the Requester, Provider shall inform the Requester of the cause of the delay, and state a new date by which it will provide its response under this Section.

C. Disclosure can be reasonably refused, for reasons consistent with the general policy stated herein, including without limitation any of the following:

   i. the Provider has already published Customer contact details in WHOIS as the result of termination of privacy/proxy service;
   ii. the Customer has objected to the disclosure and has provided a basis for reasonably believing (i) that it is not infringing the Requester's claimed intellectual property rights, and/or (ii) that its use of the claimed intellectual property is defensible;
   iii. the Provider has a basis for reasonably believing (i) that the Customer is not infringing the Requester's claimed intellectual property rights, and/or (ii) that the Customer's use of the claimed intellectual property is defensible;
   iv. the Customer has surrendered its domain name registration in lieu of disclosure, if the Provider offers its Customers this option;
   v. the Customer has provided, or the Provider has found, specific information, facts and/or circumstances showing that the Requester's trademark or copyright complaint is a pretext for obtaining the Customer's contact details by effecting removal of the privacy/proxy service for some other purpose unrelated to addressing the alleged infringement described in the Request;
   vi. the Customer has provided, or the Provider has found, specific information, facts, and/or circumstances showing that disclosure to the Requester will endanger the safety of the Customer; or
   vii. the Requester failed to provide to the Provider the verifiable evidence of wrongdoing outlined in Section II.

D. Disclosure cannot be refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to disclose be solely based on the fact that the Request is founded on alleged intellectual property infringement in content on a website associated with the domain name.

E. For all refusals made in accordance with the policy and requirements herein, Provider must accept and give due consideration to Requester's requests for reconsideration of the refusal to disclose.

F. A recommended mechanism for resolving disputes in which a Provider is alleged to have made a wrongful disclosure based on a Requester having provided false information is outlined in Annex 1 below.

Annex 1 To Disclosure Framework: Resolving Disputes Arising From Disclosures Made As A Result Of Allegedly Improper Requests

Notes:
For the avoidance of doubt, this option is not intended to preclude any party from seeking other available remedies at law.

Under these standards, disclosure is wrongful only when it is effected by the Requester having made knowingly false representations to the Provider. Disclosure is not wrongful if the Requester had a good faith basis for seeking disclosure at the time the Request was submitted to the Provider.

Under these standards, misuse occurs only when a Requester knowingly uses Customer contact information disclosed to it by a Service Provider for a purpose other than one of the specific purposes for which it had agreed to use such information (as listed in Section II.A(6), II.B(7), and II.C(6) of the Policy).

Jurisdiction:
In making a submission to request disclosure of a Customer's contact information, the Requester and the rights holder agrees to submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) where it is incorporated (or of its home address, if an individual), AND (2) where the Provider specifies on its request form, solely for disputes arising from alleged improper disclosures caused by knowingly false statements made by the Requester, or from Requester's and/or rights holder's knowing misuse of information disclosed to it in response to its request.