DRAFT: Privacy & Proxy Services Implementation Review Team - GAC Public Safety Working Group Disclosure Framework

Purpose:

This document sets out draft principles developed by representatives of the Governmental Advisory Committee (GAC) working group on Public Safety (PSWG), and endorsed by the GAC, regarding the policy implementation for the processing of disclosure requests by accredited Privacy and Proxy Service providers, in accordance with the GNSO Final Report on Privacy & Proxy Services Accreditation Issues Policy Development Process. While the focus of this document is "Disclosure," as defined in the Privacy and Proxy Service Provider Accreditation Agreement (PPAA), this will not preclude LEA requests for other data held by Providers as pertinent to an investigation where issued as a properly submitted request using the appropriate legal processes."

Commented [AB1]: Note: Redline edit proposed in light of discussion during IRT-PSWG meeting at ICANN59.

This disclosure framework will provide guidance to the Privacy and Proxy Services Implementation Review Team during the development of policy in response to the final report and related GAC advice on this matter.

1. Definition of terms

1.1. The "Requestor": Law enforcement, consumer protection, quasi-governmental 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;[1]

1.2. The "Provider": The entity who provides the Privacy and / or Proxy service;

1.3. The "Customer": The subscriber of the Privacy or Proxy service;

1.4. The "Requested Information": The data asked for by the Requestor. This

[1] *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 authorities 14; 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).*

must be detailed in the request submission., ~~and may include, but is not limited to: Customer registration data directory service records; contact data including email addresses, usernames, contact telephone numbers residential addresses and any other subscriber number or identity; billing and payment information including bank account numbers, billing records, credit and debit card details; verification documents; account access data including session times, duration and associated IP addresses.~~

1.5. The "Priority Level": The urgency with which the disclosure request should be actioned. Disclosure requests may be categorized as "high priority" or "standard priority." "High priority" requests are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure or child exploitation.

Commented [AB2]: Rationale: Redline proposed based on definition of "disclosure" (see Final Report p. 8), "the reveal of a person's (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details to a third party Requester without Publication in the WHOIS system."

Redline was discussed at ICANN 59 and appeared to be acceptable, coupled with new redline edit in the introduction re: other legal processes for information beyond "Disclosure."

Commented [AB3]: Rationale: Redline proposed to clarify specific criteria for a request to qualify as "high priority." This was discussed at ICANN59 and appeared to be acceptable edit.

2. Minimum requirements for disclosure request submissions

2.1. As a minimum standard for acceptance, disclosure request submissions must contain:

2.1.1. Domain name or URL involved;
2.1.2. Deciding authority (~~i.e~~e.g.~~.~~ prosecutor, judge, police authority) behind this request and source of legal authority for request;
2.1.3. Details of Requested Information;
2.1.4. Priority Level, including detail about threat type and justification for Priority Level, and / or suggested deadline for response;
2.1.5. Instructions regarding timeline requirements for customer notification;
2.1.6. Requestor contact details, including instructions for identity verification;
2.1.7. Any details otherwise required by national or international law.
~~2.1.7.~~2.1.8. A verification statement (e.g. all provided information is true and correct).

2.2. To assist the Provider, further additional information may include:

2.2.1. Evidence of earlier contact (attempts), if any, and if deemed relevant by the Requestor;
2.2.2. Requestor contact details for the customer;
2.2.3. Reference to applicable national or international law(s), ICANN regulation(s);
2.2.4. Details of decision to order disclosure of information.

Commented [AB4]: Rationale: Redline proposed to provide additional examples and make clear that this is a non-exclusive list of deciding authorities.

Commented [AB5]: Rationale: Redline proposed to add legal rationale/source of authority for LEA request.

3. Receipt Process

3.1. Pre-Request:

3.1.1. The Provider will establish and maintain a designated Requestor point of contact for submitting disclosure requests. ~~These details~~The designated contact will be published on the Provider website.

3.1.2.

~~3.1.3. Where no website exists, the Provider will publish these details in registration data directory service records.~~

Commented [AB6]: Note: This was discussed at ICANN59 and on the 11 July call. It was agreed that there should be a way for LEA to contact the Provider from the Provider's website, but that the contact does not have to be an email address (could be a form, telephone number or any other means).

The Final Report, p. 62, noted with respect to abuse reports that the IRT should "consider alternative abuse report options other than publishing an email address on a website and in WHOIS output (to address increasing volumes of spam)."

The IRT is asked for feedback on this edit and whether any additional text should be added.

3.2. Receipt Process:

3.2.1. Within ~~24 hours~~two business days (in the Provider's jurisdiction) of the disclosure request been submitted, the Provider will review the request, and confirm it has been received and contains the relevant information required to meet the minimum standard for acceptance. If the request does not meet the minimum standard, the Provider will notify the Requestor.

Commented [AB7]: Rationale: Redline proposed in light of IRT conclusion that 24 hours is too short a window. This proposal would accommodate holidays/weekends.

This was discussed on the 11 July IRT call.

3.2.2. Where the Requestor is not known to the Provider, the Provider will verify the identity of the Requestor.

4. Provider response actions (two-tier prioriti~~z~~sation)

4.1. Prioriti~~z~~sation:

4.1.1. Upon completion of the Receipt Process, the Provider will action in accordance with 4.2 and 4.3 the disclosure request in accordance with the Priority Level. High Priority requests can include an imminent

Commented [AB8]: Rationale: Redline proposed to clarify the meaning of "actioned."

threat to life, serious bodily injury, critical infrastructure or child exploitation.

4.1.2. Where a disclosure request has been categorized as High Priority, this must be actioned within 24 hours. The Requestor will detail the threat type and justification for Priority Level.

4.1.3. For all other disclosure requests not identified as High Priority, the Provider should seek to action these in accordance with the deadline identified in the request. If the Provider cannot adhere to this deadline, the Provider should notify the Requestor and provide a reasonable timeframe for response.

4.2. Disclosure:

4.2.1. Within the appropriate timeframe consistent with the Priority Level, the Provider will disclose to Requestor using a secure mechanism the Requested Information it holds against the account.

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

4.2.2.1. The Requestor failed to provide to information to meet the minimum standard for acceptance as outlined in Section 2;

4.2.2.2. If disclosure would lead to a contravention of national or international law;

4.2.2.3. where the customer has provided, or ~~or~~ the Provider has found, specific information, facts, and/or circumstances showing that disclosure will endanger the safety of the customer.

4.2.3. If disclosure is refused, the Provider must state to the Requestor in writing or by electronic communication its specific reasons for refusing to disclose. This must be completed prior to any Customer Notification, irrespective of the reason for refusal;

4.2.4. In exceptional circumstances, if the Provider requires additional time to respond to the Requestor, the Provider shall inform the Requestor of the cause of the delay, and agree with the Requestor a new date by which it will provide its response under this Section.

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

4.3. Customer Notification:

4.3.1. The Provider will notify the Customer of the disclosure request in accordance with its published Terms of Service and the timeframe identified by the Requestor.

4.3.2. The Provider may voluntarily set a generic timeframe for Customer Notification (for example 90 days), which can be extended at the behest of the Requestor. Details of any generic timeframe must be published on the Provider website, and the Requestor must always be informed in advance of any time limit being implemented or changed.

4.3.3. The Provider must notify the Requestor at least three working days before Customer Notification takes place.

Commented [AB9]: Rationale: This redline is being proposed because the Policy Recommendations do not require customer notification—the Provider must simply spell out whatever processes it follows for notifications in its terms of service.

This was discussed with Nick Shorey on 11 July IRT call.

5. Issues of Non-response / non-compliance with LEA requests

5.1. In cases of the Requestor receiving no response from the Provider, or non-compliance with disclosure requests within contractually defined or mutually agreed timelines, the issue may be escalated to ICANN in accordance with existing compliance mechanisms, or other appropriate legal mechanisms available within the jurisdiction in which the privacy or proxy service Provider is established or maintains a physical office.

6. Additional guidance

6.1. The Provider may voluntarily action disclosure requests from non-designated government authorities in accordance with the processes detailed within this document,–where such action does not conflict with national or international law(s).

6.2. A Requestor must 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 legal proceeding concerning the issue for which the request was made.

6.3. Customer notification should take place at the earliest opportunity, unless such disclosure would pose a risk to operational sensitivity; safety of individuals; or is prohibited by law or court order. Such circumstances must be detailed in the disclosure request.