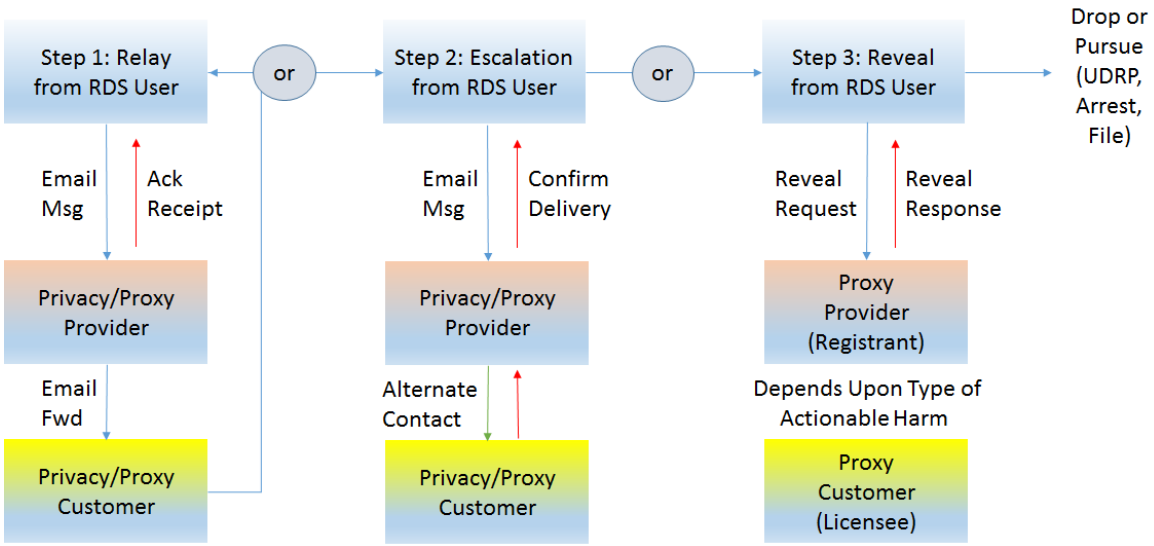
ANNEX H: MODEL AND PRINCIPLES FOR RELAY AND REVEAL

As noted in Section VI(b), the EWG recommends accredited Privacy and Proxy Services be required to relay all email received by the forwarding email address. The goal is to provide accredited Privacy/Proxy customers and RDS users who might want to contact them with a standard, always-available, near real-time communication path.

In addition, the EWG recommends requiring accredited proxy services respond to reveal requests in a timely manner (further details below). The goal is to provide users experiencing serious problems with proxy-registered domains with a standard, always-available, efficient process to seek effective problem resolution.

When analyzing these user needs, the EWG noted another shortfall in today's practices: the absence of a readily-available, efficient escalation method when communication fails. Many users jump quickly to reveal because they have no other recourse. The EWG recommends introducing an escalation process which might be less costly to all parties and reduce the number of problems that lead to more costly and time-consuming reveal requests. This three-step process is illustrated below:



Step 1: Relay

a) The RDS user requests contact data for a domain, retrieving:

- The Registrant's Contact ID (i.e., the Privacy Customer or Proxy Provider's Contact ID)

- Contact IDs for all mandatory Purpose-Based Contacts (PBCs) and published PBC addresses (including email addresses)

- An indication the domain registration was done via Privacy/Proxy Service, and

- Name and address of the accredited Privacy or Proxy Service Provider, provided as a Privacy/Proxy Provider PBC, which includes a published Relay Escalation and Reveal form URLs.

b) The RDS user, noting that this is an accredited Privacy/Proxy registration, attempts to email the Privacy/Proxy customer at the forwarding address. Providers might optionally let customers supply more forwarding addresses (e.g., phone, SMS, postal).

c) The accredited Privacy/Proxy provider must be required to forward and acknowledge receipt of the relayed message (e.g., email acknowledgement to all messages received for the forwarding email address). A negative acknowledgement might be returned for error cases (e.g., no such mailbox), and acknowledgements to the same sender might be limited by a threshold to deter relay abuse.

d) The RDS user receiving the acknowledgement now has confirmation that the message was relayed to the Privacy/Proxy customer. However, the customer may choose not to reply or may discard the relayed message without reading it (e.g., treat as spam).

Step 2: Escalation

The RDS user tires of waiting for the accredited Privacy/Proxy customer to respond and decides to escalate the previously-attempted contact by:

a) Visiting the website of the accredited Privacy or Proxy Service identified in Step 1 and completing an escalation form that contains:

- The RDS user's identity (possibly re-using an RDS query credential)

- The RDS user's reason for contact (could be a pull-down list of defined reasons)

- The Privacy/Proxy-registered domain name

- An uploaded message to be relayed to the customer (possibly encrypted?)

- Timestamp of when relay was first attempted

b) The accredited Privacy/Proxy Provider must be required to try to contact the customer directly, possibly using contact information and/or methods inaccessible to

the RDS user, returning a "delivery confirmation" within N*[42] days. Here again, negative confirms would be returned for error cases (e.g., unauthenticated user, timeout) and submissions could be logged and limited by a threshold to deter abuse.

c) The RDS user receiving the confirmation now has documented proof that the message was delivered to the Privacy/Proxy customer. The customer may still choose not to reply, but escalation must help overcome basic communication failures without requiring reveals.

Step 3: Reveal (only applies to proxy-registered domains)

The RDS user times out waiting for the accredited Proxy customer (licensee) to respond and decides the problem is significant enough to pursue criminal or civil action by:

a) Visiting the website or calling or mailing the accredited Proxy Service Provider identified in Step 1 and submitting a reveal request that contains:

- The RDS user's identity
- The RDS user's reason for contact (narrowly limited to actionable harms)
- The Proxy Provider-registered domain name
- Documentation of harm (trademark registration information, allegations of abuse)
- Timestamp of when relay/escalation was attempted (case number from escalation?)

b) The accredited Proxy Provider must be required to investigate and take appropriate action (see d), returning a "reveal response" within N*[43] days. Reveal requests could be logged and limited to actionable harms alleged by RDS users with standing,[44] to deter abuse.

---

[42] * The timeout might depend on authenticated identity and stated reason for contact. For example, 1 day for law enforcement/OpSec investigating a crime/abuse; 7 days for brand owners investigating TM infringement; 7 days for Internet consumers trying to reach online merchants.

[43] * The timeout might depend on requestor and stated reason for contact. Law enforcement might go directly to Step 3 (Reveal) for time-sensitive investigations. Time frames and efforts for Step 2 must be low enough to discourage others from jumping directly to Step 3.

[44] ** Any user requesting a reveal must demonstrate they are (or represent) a party suffering actionable harm. For example, brand holders or their agents alleging TM infringement might show they own domain name(s) similar to the proxy-registered domain. Further thought is needed to map types of users to types of harms. See GoDaddy's list of proxy-registered domain complaint form options as example.

c) The accredited Proxy Provider, given documentation with which to assess the case, might:

- Notify and transfer the domain to the customer (that is, discontinue proxy service)
- Temporarily suspend the domain during a criminal investigation
- Reveal to the user the identity/contact of a licensee engaged in unlawful activity
- Reject the reveal – positively affirming the Proxy's liability for further domain use.

A policy must be developed here to detail what constitutes sufficient documentation and when the licensee must be notified. In addition, there will need to be clear policies regarding the impact of local law and factors to be considered. All of the above happens today, without any oversight, policy guidance or consequences for rejecting/ignoring reveal.

d) The RDS user receiving the reveal response now has the information needed to drop the matter or pursue legal/civil action. For example, trademark infringement might lead to filing a UDRP, while a law enforcement criminal investigation might lead to a suspect's apprehension. If the reveal is rejected (or timely response is not received), the RDS user may also now choose to pursue legal/civil action against the accredited Proxy.

Note that the processes described above do not address when a proxy or privacy registration must be "unmasked" to the public rather than simply "revealed" to the requestor.

These suggested models and processes must be further refined by the GNSO PPSAI WG, based upon their consideration of ICANN community needs and informed by best practices identified by responses to the EWG's on-line survey of Privacy and Proxy Service Providers.