**Findings**

Privacy and proxy services have arisen to fill an ICANN policy vacuum. These services are clearly meeting a market demand, and it is equally clear that these services are complicating the WHOIS landscape.

Privacy and proxy services can be used to address legitimate legal, noncommercial and commercial interests. For example,

**Individuals – who prefer not to have their personal data published on the Internet as part of a WHOIS record.**

**Organizations – as religious, political or ethnic minority, or sharing controversial moral or sexual information.**

**Companies –** for upcoming mergers, new product or service names, new movie names, or other product launches

However, ICANN’s current lack of any clear and consistent rules with regards to privacy and proxy services[[1]](#footnote-1) has resulted in unpredictable outcomes for stakeholders. In terms of the review team’s scope:

* Law enforcement shared its concern over the abuse of proxy services by criminals seeking to hide, companies defrauding customers, and parties attacking the security of the Internet including by botnets and malware [can we do a fact-based statement here, perhaps a quote from the Report? Many stakeholders identified the unregulated environment in which they operate as a major underlying problem [from our Report, chapter 6]
* [quick KK note: that consumers of p/p services generally DO have some idea how their data is treated because they sign an agreement with the p/p service; it is the community as a whole that does not know how p/p handle the data]; and
* the current use of privacy and proxy services raises questions about whether ICANN is meeting its AoC commitments relating to ‘timely, unrestricted and public access’ to WHOIS data.

**[**The Review Team considers that,

* with appropriate regulation and oversight, privacy and proxy services appear capable of addressing stakeholder needs.**]**

**Recommendation**

The Review Team recommends that ICANN should initiate processes to regulate and oversee privacy and proxy service providers.

ICANN should develop these processes in consultation with all interested stakeholders.

This work should take note of the studies of existing practices used by proxy/privacy service providers now taking place within the GNSO. .

The review team considers that one possible approach to achieving this would be to establish, through the appropriate means, an accreditation system for all proxy/privacy service providers. As part of this process, ICANN should consider the merits (if any) of establishing or maintaining a distinction between privacy and proxy services. [let’s footnote the two definitions, privacy and proxy services. Do we want the other definitions that are footnoted in Recommendation 14?]

The goal of this process should be to provide clear, consistent and enforceable requirements for the operation of these services consistent with national laws, and to strike an appropriate balance between stakeholders with competing but legitimate interests. At a minimum, this would include privacy, data protection, law enforcement, the industry around law enforcement and the human rights community.

ICANN could, for example, use a mix of incentives and graduated sanctions to encourage proxy/privacy service providers to become accredited, and to ensure that registrars do not knowingly accept registrations from unaccredited providers.

ICANN could develop a graduated and enforceable series of penalties for proxy/privacy service providers who violate the requirements, with a clear path to de-accreditation for repeat, serial or otherwise serious breaches.

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

* Clearly labeling WHOIS entries to indicate that registrations have been made by a privacy or proxy service
* Providing full WHOIS contact details, which are contactable and responsive
* Adopting agreed standardized relay and reveal processes and timeframes (these should be clearly published, and pro-actively advised to potential users of these service so they can make informed choices based on their individual circumstances)
* Registrars should disclose their relationship with any proxy/privacy service provider
* Maintaining dedicated abuse points of contact for each provider
* Conducting periodic due diligence checks on customer contact information
* Maintaining the privacy and integrity of registrations in the event that major problems arise with a privacy/proxy provider

**[** Finally, for the avoidance of doubt, the WHOIS policy, referred to in Recommendation 1 above, could include an affirmative statement that clarifies that ICANN regards the registered name holder in the WHOIS data to be the entity that obtains all rights and assumes all responsibility for the domain name and its manner of use. [KK: did we adopt this earlier? If not, this may be a consensus-breaker. Is there another, more neutral way to phrase it? Tx!] **]**

1. Working definitions of Privacy and Proxy Services:

Privacy Service a service that provides the Registrant Name and a subset of other information (possibly null set) but consistent across ICANN

Proxy Service a relationship in which the registrant is acting on behalf of another. The WHOIS data is that of the agent and the agent alone obtains all rights and assumes all responsibility for the domain name and its manner of use. [↑](#footnote-ref-1)