Appendix I: Comparative review of registries and WHOIS data publication

In order to inform our understanding of peer standards we examined how privacy services are treated by other registries including ccTLDs and gTLDs. In addition we compared the approaches adopted by other registries in relation to publication of contact data on the WHOIS and stakeholder views in response to the Final report of the ICANN WHOIS Policy Review Team.

1. Privacy services: an International comparison

Figure 1

Privacy Service?	Domain Extension	Registry	Notes
Yes - Registry operated	. fr, .re, .pm, .yt, .wf, .tf	Afnic	Afnic - Privacy service introduced in December 2011. Applied by default and Registrants can opt-out.
	.ca	CIRA	CIRA – Privacy service enabled by default for individual Registrants, who can disable.
	.nl	SIDN	SIDN – Privacy service requests are considered on a individual basis by the Registry
Yes - Registrar operated	.com, .net	Verisign	
	.org	PIR	
No enhanced privacy options.	.us	Neustar	Registrants do not have the option to keep their details private.
	.de	DENIC	Registrant and Technical Contact postal addresses must be disclosed. Phone number and email addresses are not disclosed.
	.au	AuDA	Registrant name and a contact email address must be published. No postal address is published as per Australian legislation.
	.nz	Domain Name Commission	Registrants must accept *'that the details in the register ... are available to all as a matter of public record'.*[1]

2. WHOIS data publication: an International comparison

[1] http://dnc.org.nz/story/faq-registrants

Registries and registrars are able to offer either a thin or a thick WHOIS. For gTLDs these are defined as:

- A thin WHOIS discloses a limited set of data fields sufficient to identify the registrar, the status of the registration, and the creation and expiration dates of each registration.
- A thick WHOIS publishes additional registrant data elements including contact information for the registrant and administrative and technical contacts.

We examined 22 country code Top Level Domain Registries (ccTLDs) to ascertain whether a thin or thick WHOIS was provided.

The research indicates that the majority of registries provide a thick WHOIS.

Figure 2

	Thin WHOIS	Thick WHOIS
ccTLDs	4	18
gTLDs	2	4
Totals	**6**	**22**

It should be noted that under the new gTLD registry agreement registry operators must enable free public access to registrant data by providing a thick WHOIS Query tool.[2]

3. WHOIS data publication: Review of the final report of the ICANN WHOIS Policy Review Team

Nominet commissioned Shepherd and Wedderburn LLP to review the final report[3] from the ICANN WHOIS Policy Review team (PRT) published in 2012. Since its publication the debate on WHOIS has continued, however it was useful to review the key arguments put forward by stakeholders to the PRT both in favour and against disclosure of personal information on the WHOIS and the recommendations specifically relating to data access and privacy and proxy services within the gTLD space. The key points are summarised below.

The PRT report identified three key reasons for stakeholders to use privacy and proxy services including:

- Individuals who do not wish to disclose their personal contact information on the WHOIS
- Organisations such as religious groups who may wish to use the domain name for a website publishing potentially controversial views
- Businesses who wish to protect commercially confidential information

Arguments in favour of disclosure of information on the WHOIS

[2] p60 of the new gTLD Registry Agreement
[3] https://www.icann.org/en/system/files/files/final-report-11may12-en.pdf

Law enforcement and IP rights stakeholders expressed views that privacy and proxy services are used by criminals to hide their contact details. They state that the lack of access to accurate registrant contact data frequently impedes investigations and increases the cost to business of protecting their IP rights. This can be further exacerbated by a lack of cooperation from the privacy or proxy service operator in complying with requests to release the intended registrant data. In addition comments reflected the public interest argument that registrant data should be published for public access and the fact that data is made available in other databases supports arguments in favour of disclosure on the WHOIS.

Arguments against disclosure of information on the WHOIS

Business stakeholders put forward the view that non-disclosure of contact details through the use of a privacy service could be useful and necessary for companies wishing to protect commercially confidential information such as details of a new product. Law enforcement suggested that non-disclosure may be necessary in cases where disclosure is likely to put the registrant at risk of harm. Others, including those representing the views of non-commercial stakeholders, stated that enabling registrants to hide their registration details may encourage the provision of accurate data. In addition their view was that generally registrants object to the indiscriminate public access to their contact data rather than the provision of the data to a trusted source.

Recommendations of the Policy Review Team

A key recommendation was for ICANN to explore developing an accreditation system to regulate and oversee privacy and proxy services with any system taking the following objectives into consideration:

- Clearly labelling WHOIS entries to indicate that registrations have been made by a privacy or proxy service;
- Providing full WHOIS contact details for the privacy/proxy service provider, which are contactable and responsive;
- Adopting agreed standardised relay and reveal processes and timeframes; (these should be clearly published, and pro-actively advised to potential users of these services 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;
- Providing clear and unambiguous guidance on the rights and responsibilities of registered name holders, and how those should be managed in the privacy/proxy environment.