Appendix J: Review of international discussions

We continue to monitor the work of the ICANN Expert Working Group (EWG) on Registry Directory Services and the Working Group on Privacy and Proxy Services Accreditation Programme so we can understand the international environment, drivers of the discussions and the potential impact of those discussions on Nominet's registrars that are also ICANN Accredited In our view, many of the concerns raised in the gTLD space are not comparable to the .uk space – such as the matter of publication of email addresses and phone numbers, spam, and the use of privacy services for criminality. Therefore our proposal for consultation does not mirror exactly the gTLD approach. Our continued monitoring of developments within the gTLD space will enable Nominet to develop responsive and relevant policies for .uk that do not adversely impact on its ability to compete within the market.

1. *The Expert Working Group (EWG) on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*

The remit of the EWG was to "re-examine and define the purpose of collecting and maintaining gTLD registration data, consider how to safeguard the data, and propose a next generation solution that will better serve the needs of the global internet"[1] The group released a final report in June 2014, which they considered to be the first step in response to the Board's commissioning of the work. The EWG stated that the overarching problem of the current WHOIS system are the characteristics of entirely public data that is available and accessible anonymously, where registrants cannot provide contemporary alternate data or have control over who may access the data, and that contacts cannot prevent inaccurate or fraudulent use. The group unanimously recommended that the current WHOIS model be replaced with a centralised WHOIS that provides access to validated registration data for a specific purpose.

The recommendations focus on the concept of 'purpose driven access' and 'purpose based contact' to minimise the volume and type of data that is publicly available. It is proposed that the centralised WHOIS would contain 'Purpose based contact IDs,' the date and level to which the contact data was validated; and other optional elements such as whether data is that of a privacy or proxy service or a business. Such purpose based contacts would then require the collection of what could be considered a large amount of additional data including Admin, Tech and Contact Data, Abuse, Legal, Proxy and Business Contact Data.

WHOIS users would be able to access a limited amount of public data recorded for the registration. Access to the balance of the data would be granted to authenticated requestors (subject to their level of authentication) and for permissible purposes only (listed in Fig. 12). The RDS would be responsible for the collection, validation and disclosure of the data and accessing the gated information would most likely attract a fee.

The EWG proposed that contact data could contain third party information authorised for use by the domain holder or forwarded by a privacy service or a 'purpose based contact'. They have also suggested that this approach would allow for the improvement of data quality by protecting phone numbers and addresses however more consideration would need to be given as to whether there is the potential for legal issues to arise when proxies are used from different jurisdictions. In

[1] https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf p6

our view, the proposal may attract criticism from stakeholders such as Government, Law Enforcement and the IP rights community who may object to having access to registrant data restricted in this way.

The EWG's report also discusses data protection principles and that their proposals 'should be able to apply local law'. However, the Data Protection representative on the EWG has issued a minority view that does not agree with the group's findings.

The suggested 'Permissable Purposes' set out in the report[2] are outlined in the table below:

Figure 1 Suggested 'Permissable Purposes'

Purpose	Includes tasks such as…
Domain Name Control	Creating, managing and monitoring a Registrant's own domain name (DN), including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant's own contact information.
Personal Data Protection	Identifying the accredited Privacy/Proxy Provider or Secure Protected Credential Approver associated with a DN and reporting abuse, requesting reveal, or otherwise contacting that Provider.
Technical Issue Resolution	Working to resolve technical issues associated with domain name use, including email delivery issues, DNS resolution failures, and website functional issues, by contacting technical staff responsible for handling these issues.
Domain Name Certification	Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name needing to confirm that the DN is registered to the certificate subject.
Individual Internet Use	Identifying the organization using a domain name to instil consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them.
Business Domain Name Purchase or Sale	Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research.
Academic/Public-Interest DNS Research	Academic public-interest research studies about domain names published in the RDS, including public information about the Registrant and designated contacts, the domain name's history and status, and DNs registered by a given Registrant.
Legal Actions	Investigating possible fraudulent use of a Registrant's name or address by other domain names, investigating possible trademark infringement, contacting a Registrant/Licensee's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed.
Regulatory and Contractual Enforcement	Tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits.
Criminal Investigation & DNS Abuse Mitigation	Reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation.

[2] https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf p8-9

DNS Transparency	Querying the registration data made public by Registrants to satisfy a wide variety of needs to inform the general public.

The EWG also makes recommendations on "Privacy Principles"[3] in relation to how the Registry Directory Service could take into account the use of privacy and proxy services.

- In addition to the privacy afforded by compliance with data protection laws, the RDS ecosystem must accommodate needs for privacy by including:
    - An accredited Privacy/Proxy Service for general personal data protection and adherence to local privacy law; and
    - An accredited Secure Protected Credentials Service for persons at risk, and in instances where free-speech rights may be denied or speakers persecuted.
- There must be accreditation for Privacy/Proxy service providers and rules regarding the provision and use of accredited Privacy/Proxy services.
- Outside of domain names registered via accredited Privacy/Proxy services, all Registrants must assume responsibility for the domain names they register.
- ICANN must investigate the development of a single, harmonized privacy policy which governs RDS activities in a comprehensive manner.

2. Privacy & Proxy Services Accreditation Issues Working Group

The working group has been established to address outstanding issues related to Privacy & Proxy Services that were not addressed through the introduction of the 2013 Registrar Accreditation Agreement. A full list of the issues can be accessed in the staff briefing paper published on 16 September 2013[4].

The working group is focused on exploring the policy questions relating to privacy and proxy services and developing recommendations regarding the obligations ICANN-accredited privacy/proxy service providers could be required to adopt which originally included:

- Standard Service Practices – what should they be and are there any other contractual obligations in relation to termination.
- Baseline standard relay and reveal processes.
- Access to customer data: under what circumstances should customer data be made available and to whom.
- Data re-validation.
- Rights and responsibilities of privacy/proxy service customers.
- Transparency – should domains using privacy/proxy services be identified as such and what contact information should be published on the WHOIS?
- Enforcement and compliance.
- Should privacy/proxy services be available for use by all types of registrant?

The group will aim to publish initial recommendations in March 2015 with their final report published at the end of June. At the time of writing it is understood that agreement has been reached on a number of areas including:

- No distinction, in principle, between privacy and proxy services

[3] https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf p96
[4] http://gnso.icann.org/en/issues/raa/negotiations-conclusion-16sep13-en.pdf p15-19

- Abuse reporting mechanism
- Relay of electronic communications
- Reveal of customer identity/contact details

3. Continued monitoring

The proposals from the EWG, if adopted as they have been drafted, could fundamentally change the availability of data in the WHOIS so that it is 'gated'.

Nominet will continue to monitor carefully the development of the ICANN policies in the areas of both privacy and proxy services and WHOIS and assess the potential impact on our own work within .uk. This will include the activities set out in the WHOIS Roadmap of Activities planned for 2015.[5]

[5] https://www.icann.org/news/announcement-2-2014-12-15-enPage B-1