Initial Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service

STATUS OF THIS DOCUMENT

This is an initial report from the Expert Working Group on gTLD Directory Services (EWG) providing draft recommendations for a next generation gTLD Registration Directory Service (the "RDS") to replace the current WHOIS system.

I. EXECUTIVE SUMMARY

The Expert Working Group on gTLD Directory Services (EWG) was formed by ICANN's CEO, Fadi Chehadé, at the request of ICANN's Board, to help resolve the nearly decade-long deadlock within the ICANN community on how to replace the current WHOIS system, which is widely regarded as "broken." The EWG's mandate is to reexamine and define the purpose of collecting and maintaining gTLD directory services, consider how to safeguard the data, and propose a next generation solution that will better serve the needs of the global Internet community. The group started with a tabula rasa, exploring and questioning fundamental assumptions about the purposes, uses, collection, maintenance and provision of registration data, as well as accuracy, access, and privacy needs, and the stakeholders involved in gTLD directory services. After working through a broad array of use cases, and the myriad of issues they raised, the EWG concluded that today's WHOIS model—giving every user the same anonymous public access to (too often inaccurate) gTLD registration data—should be abandoned. Instead, the EWG recommends a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.

The EWG recommends that permissible purposes include the following:

- Domain Name Control
- Domain Name Research
- Personal Data Protection
- Legal Actions
- Technical Issue Resolution
- Regulatory/Contract Enforcement
- Domain Name Purchase/Sale
- Individual Internet Use
- Abuse Mitigation
- Internet Services Provision

The EWG considered the breadth of stakeholders involved in collecting, storing, disclosing and using gTLD registration data, mapped to associated purposes. Areas of common need were then identified and taken into consideration as the EWG developed principles and features to guide the design of a next generation registration data service (RDS).

This led the EWG to consider several system designs and agree on a new registration data service model to collect, use, and disclose accurate individual data elements for various purposes. Each player in the RDS eco-system has different needs for data, different risks, and potentially different responsibilities. Historically, most of these responsibilities were transferred to the Registrars, whose primary goal was to provide working domain names to paying customers. As the Internet ecosystem becomes more complex, and with the introduction of hundreds of new gTLDs, it is likely that new players will be required to take on some of the many responsibilities that come with satisfying such a broad range of registration purposes.

The following figure illustrates the EWG's recommended model for a next generation RDS that could potentially incorporate many of the principles discussed in this report. **Key elements of this Aggregated RDS (ARDS) model include:**

- ARDS serves as an aggregated repository that contains a non-authoritative copy of all of the collected data elements
- Each gTLD registry remains the authoritative source of the data
- Requestors (users who wish to obtain gTLD registration data from the system) apply for access credentials to the ARDS
- Registrars/Registries are relieved of obligations to provide Port 43 access or other public access requirements
- In most cases, the ARDS provides access to cached registration data that is copied from gTLD registries and maintained through frequent periodic updates.
- The ARDS can also provide access to live registration data that is obtained in real-time from gTLD registries, upon request and subject to controls to deter overuse or abuse of this option.
- ARDS (or other third party interacting with ARDS) would be responsible for performing validation services
- ARDS is responsible for auditing access to minimize abuse and impose penalties and other remedies for inappropriate access
- ARDS handles data accuracy complaints
- ARDS manages licensing arrangements for access to data

ICANN contracts with an international third-party provider to develop and operate the ARDS and monitors compliance with requirements

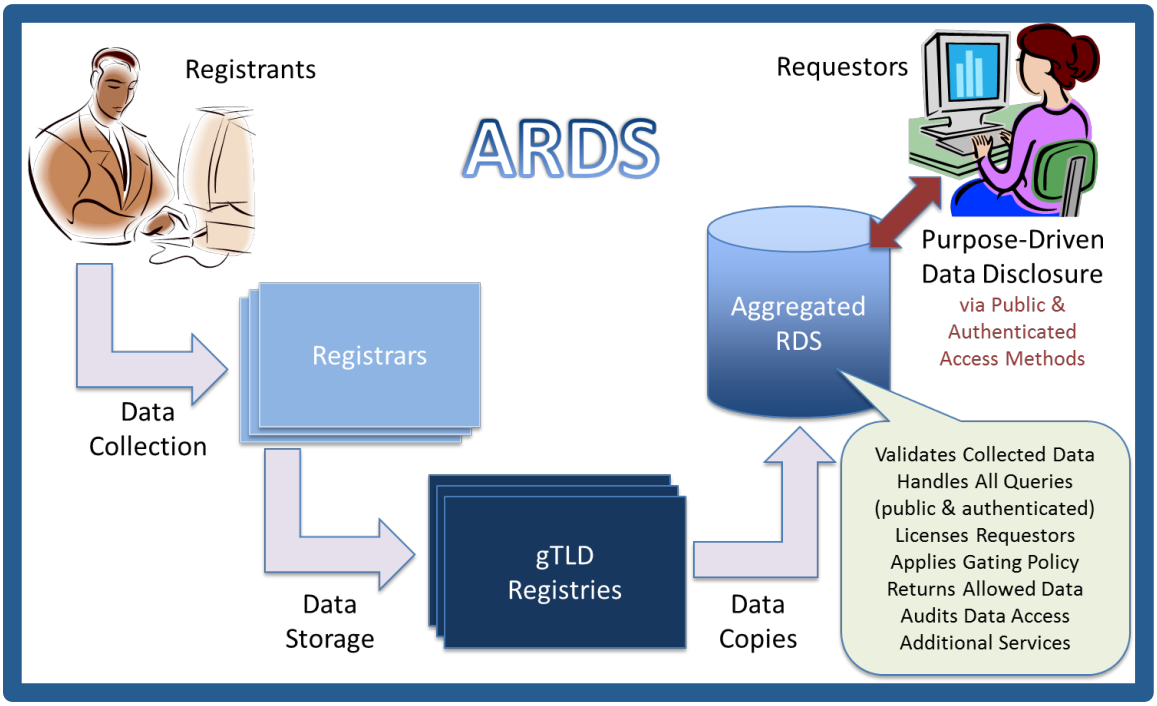

Figure 4. Aggregated RDS Model

This model received EWG members' consensus agreement because of its numerous advantages:

- Scale handled by a single point of contact
- Potential improvements in transport and delivery
- "One stop shop" for requestors of Registration Data
- Greater accountability for Registration Data validation and access (anti-abuse)
- Ability to track/audit/penalize requestors in the same way over multiple TLDs (anti-abuse)
- May reduce some costs currently borne by Registrars and Registries to provide data access
- Normalization or filtering of the data could be provided
- Reduces bandwidth requirements for Registries and Registrars
- Facilitates standardization of approaches to satisfy local data privacy concerns

- Enhanced search capability across multiple TLDs (such as reverse look-ups)
- Minimizes transition and implementation costs
- Enables validation/accreditation of requestors qualifying for special purposes (i.e., law enforcement)
- Facilitates more efficient management of inaccuracy reports
- Enables more efficient random accuracy checks
- Enables user friendly search portal displays in multiple languages, scripts and characters

Of course, nothing is perfect. The EWG also considered the following potential disadvantages to this model:

- Data Latency
- Creation of a “Big Data” source of highly valuable data with potential for misuse if not properly audited and maintained
- Increased risk of insider abuse and external attack, requiring greater attention to security policy implementation, enforcement and auditing
- Registries/Registrars no longer control delivery of registration data

In proposing this new model, the EWG recognizes the need for accuracy, along with the need to protect the privacy of those registrants who may require heightened protections of their personal information. The EWG has discussed ways in which the RDS might accommodate at-risk user needs for maximum protected registration services using “secure protected credentials.” One option might be to have ICANN accredit an independent organization to act as a Trusted Agent that, using a set of agreed criteria, would determine whether a registrant qualified for maximum protection. The EWG expects to further consider potential models for secure protected credentials which might strike an innovative, effective balance between accountability and the personal data privacy needs of at-risk Internet users.

Next Steps

Notwithstanding the progress reflected in these recommendations, the EWG has not completed its deliberations. The group seeks public input on these draft recommendations through 12 August 2013, and will continue refining its recommendations as it carefully considers comments received online, at the ICANN Durban Meeting, and through other public consultation.

In addition, several key issues remain to be fully explored, such as:

- Mapping mandatory/optional data elements to each purpose
- Identifying areas requiring risk and impact analysis
- Considering costs and impacts and ways in which they might be borne
- Examining multi-modal access methods and how they could be enabled by existing or future registration data access protocols.

Following public consultation on this Initial Report, the EWG will publish and deliver a Final Report to ICANN's CEO and Board to serve as a foundation for new gTLD policy and contractual negotiations, as appropriate. As specified by the Board, an issues report based on the Final Report will form the basis of a Board-initiated, tightly focused GNSO policy development process (PDP).

II. EWG MANDATE AND PURPOSE

2.1 Mandate

The EWG was convened as a first step in fulfilling the ICANN Board's directive[1] to help redefine the purpose and provision of gTLD registration data (such as WHOIS), with the stated goal of providing a foundation for the creation of a new global policy for gTLD directory services and contract negotiations. The EWG's objectives are to 1) define the purpose of collecting and maintaining gTLD registration data, and consider how to safeguard the data, and 2) provide a proposed model for managing gTLD directory services that addresses related data accuracy and access issues, while taking into account safeguards for protecting data. The EWG was informed by the WHOIS Review Team's Final Report, the GAC's WHOIS Principles, as well as previous community input and GNSO work over the last decade. In addition, the EWG was asked to address key questions set forth by the Security and Stability Advisory Committee (SSAC) in their report, SAC055, and to take into consideration current and future Internet operations and services. The EWG also evaluated concerns of the parties who provide, collect, maintain, publish or use this data as it relates to ICANN's remit.

[1] The Board Resolution is posted at: http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm. **Annex A** highlights the EWG's response to specific Board questions.

2.2 Statement of purpose to guide the EWG's Work

To help guide the EWG in its deliberations, the group developed a high-level statement of purpose from which to test its conclusions and recommendations, as follows:

> In support of ICANN's mission to coordinate the global Internet's system of unique identifiers, and to ensure the stable and secure operation of the Internet's unique identifier system, information about gTLD domain names is necessary to promote trust and confidence in the Internet for all stakeholders.
>
> Accordingly, it is desirable to design a system to support domain name registration and maintenance which:
>
> - Provides appropriate access to accurate, reliable, and uniform registration data
> - Protects the privacy of personal information
> - Enables a reliable mechanism for identifying, establishing and maintaining the ability to contact registrants
> - Supports a framework to address issues involving registrants, including but not limited to: consumer protection, investigation of cybercrime, and intellectual property protection
> - Provides an infrastructure to address appropriate law enforcement needs.

III. METHODOLOGY - IDENTIFYING USERS AND PURPOSES

3.1 Use Case Methodology

The EWG was encouraged to take a clean slate approach in its efforts to define the next generation of registration directory services, rather than improvements to the current WHOIS system, which is widely regarded as inadequate. Consistent with the Board's directive, the EWG commenced its analysis by examining existing and potential purposes for collecting, storing, and providing gTLD registration data to a wide variety of users.

To accomplish this, EWG members drafted an extensive set of actual use cases involving the current WHOIS system, analysing each of them to identify (i) the users who want access to data, (ii) their rationale for needing such access, (iii) the data elements they need and (iv) the purposes served by such data. Cases were also used to identify all stakeholders involved in collecting, storing and providing registration data, helping the EWG understand existing and potential workflows and ways in which these users and their needs might be better satisfied by a next generation RDS.

These use cases were not intended to be exhaustive, but rather representative of the many uses of the current WHOIS system, illustrating a wide variety of users, needs and workflows. An inventory of uses cases considered by the EWG is provided in **Annex B**.

The EWG considered the totality of these use cases and lessons learned from them in order to derive a consolidated set of stakeholders and desirable purposes that should be accommodated by the RDS, as well a set of potential misuses that the system should attempt to deter (further detailed in the next section of this report.)

Moreover, the EWG consulted reference materials from previous WHOIS-related activities, community inputs, and use cases to examine specific needs in each of the areas set forth in Figure 1 below.

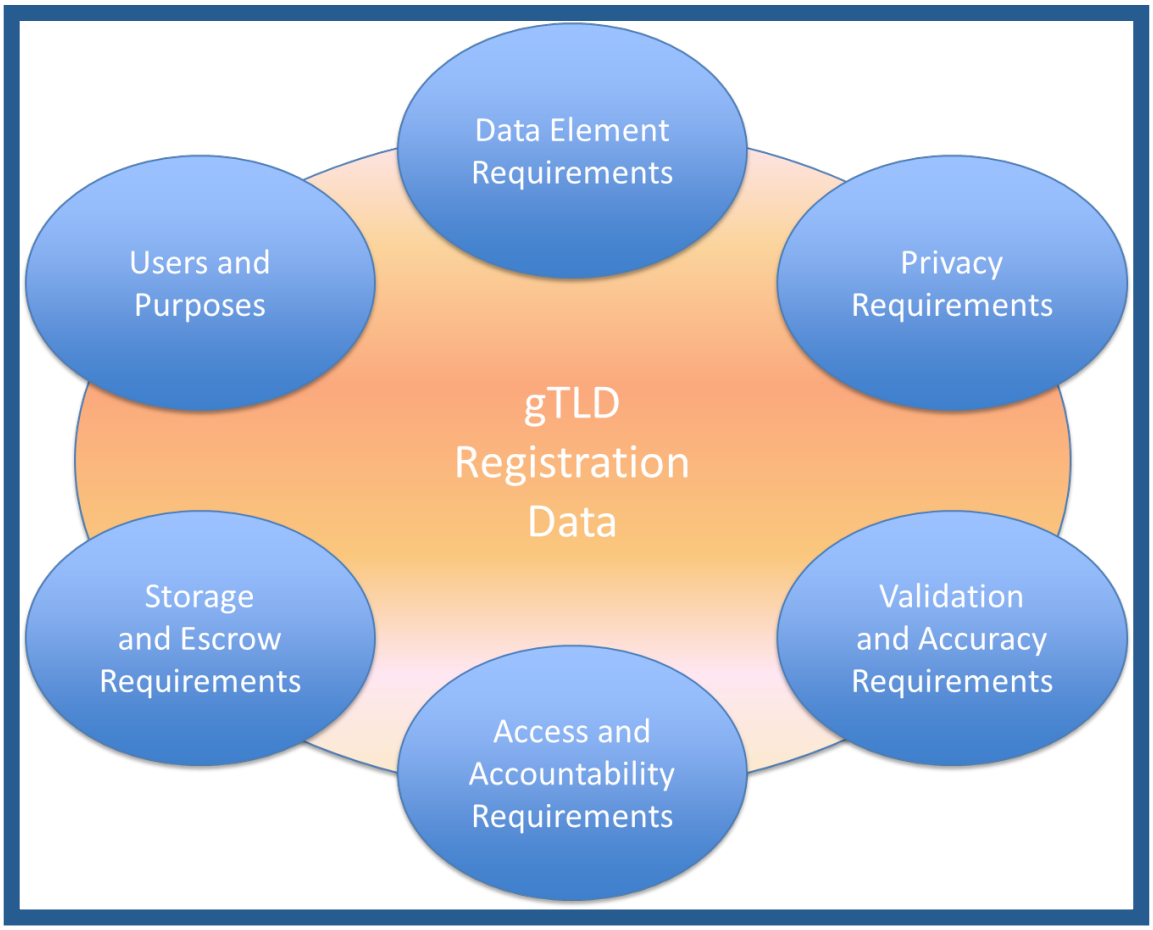

Figure 1: Needs Analysis

The EWG expects to continue its work by analyzing these purposes and needs to derive minimum data elements, related risks, privacy law and policy implications, and additional questions to be more fully explored in the final draft of this report.

3.2 Identifying the Users of the RDS

The EWG analyzed each of the representative use cases to develop the following table, which summarizes the kinds of users who want access to gTLD registration data, the rationale for needing access, and the overall purposes

served by that data. Further detail about each use case and user interactions with the RDS is provided in **Annex B**.

User	Purpose	Example Use Cases	Rationale for registration data access
All Registrants (e.g., natural persons, legal persons, privacy/proxy providers)	Domain Name Control	Domain Name Registration Account Creation	Enable registration of domain names by any kind of registrant by creating a new account with a registrar
		Domain Name Data Modification Monitoring	Detect accidental, uninformed or unauthorized modification of a domain name's registration data
		Domain Name Portfolio Management	Facilitate update of all domain name registration data (e.g., designated contacts, addresses) to maintain a domain name portfolio
		Domain Name Transfers	Enable registrant-initiated transfer of a domain name to another registrar
		Domain Name Deletions	Enable deletion of an expired domain name
		Domain Name DNS Updates	Enable registrant-initiated change of DNS for a domain name
		Domain Name Renewals	Enable renewal of a registered domain name by the domain name's billing contact (an individual, role or entity)
		Domain Name Contact Validation	Facilitate initial and on-going validation of domain name registration data (e.g., designated contacts, addresses)
Protected Registrants (e.g., customers of privacy/proxy services)	Personal Data Protection	Enhanced Protected Registration	Enable use of accredited privacy or proxy registration services by any registrant seeking to minimize public access to personal names and addresses
		Maximum Protected Registration	Enable use of accredited proxy registration services by individuals or groups under threat, using blind credentials issued by a trusted third party
Internet Technical Staff (e.g., DNS admins, mail admins, web admins)	Technical Issue Resolution	Contact with Domain Name Technical Staff	Facilitate contact with technical staff (individual, role or entity) who can help resolve technical or operational issues with Domain Names (e.g., DNS resolution failures, email delivery issues, website functional issues)
On-Line Service Providers (e.g., ISPs, hosting providers, CAs, reputation services)	Internet Services Provision	Contact with Domain Name Registrant	Enable re-establishment of contact with a customer (individual, role or entity) to deal with business issues for a Domain Name when a provider's usual contact methods fail
		Domain Name Reputation Services	Enable domain name white/black list analysis by reputation service providers
		Domain Name Certification Services	Help a certification authority (CA) identify the registrant of a domain name to be bound to an SSL/TLS certificate

User	Purpose	Example Use Cases	Rationale for registration data access
Individual Internet Users (e.g., consumers)	Individual Internet Use	Real World Contact	Help consumers obtain non-Internet contact information for domain name registrant (e.g., business address)
		Consumer Protection	Afford a low-key mechanism for consumers to contact domain name registrants (e.g., on-line retailers) to resolve issues quickly, without LE/OpSec intervention
		Legal/Civil Action	Help individual victims identify the domain name registrant involved in potentially illegal activity to enable further investigation by LE/OpSec
Business Internet Users (e.g., brand holders, brokers, agents)	Business Domain Name Purchase or Sale	Domain Name Brokered Sale	Enable due diligence in connection with purchasing a domain name
		Domain Name Trademark Clearance	Enable identification of domain name registrants to support trademark clearance (risk analysis) when establishing new brands
		Domain Name Acquisition	Facilitate acquisition of a domain name that was previously registered by enabling contact with registrant
		Domain Name Purchase Inquiry	Enable determination of domain name availability and current registrant (if any)
		Domain Name Registration History	Provide domain name registration history to identify past registrants and dates
		Domain Names for Specified Registrant	Enable determination of all domain names registered by a specified entity (e.g., merger/spinoff asset verification)
Internet Researchers	Domain Name Research	Domain Name Registration History	Enables research and statistical analysis about domain name registrations (also needed by Business Internet Users)
		Domain Names for Specified Registrant	Enables research and statistical analysis about domain name registrants (also needed by Business Internet Users)
		Domain Name Registrant Contact	Enables surveys of domain name registrants (also needed by On-Line Service Providers)
Intellectual Property Owners (e.g., brand holders, trademark owners, IP owners)	Legal Actions	Proxy Service Provider Customer Identification	Enables identification of customer of proxy service associated with a domain name being investigated for possible infringement or IP theft (i.e., reveal)
		Domain Name User Contact	Enables contact with party using a domain name that is being investigated for TM/brand infringement or IP theft
		Combat Fraudulent Use of Registrant Data	Facilitate identification of and response to fraudulent use of legitimate data (e.g., address) belonging to another registrant
Non-LEA Investigators	Regulatory and Contractual Enforcement	Online Tax Investigation	Facilitate by national, state, province or local tax authority identification of domain name engaged in on-line sales

User	Purpose	Example Use Cases	Rationale for registration data access
(e.g., Tax Authorities, UDRP Providers, ICANN Compliance)		UDRP Proceedings	Let UDRP Providers confirm the correct respondent for a domain name, perform compliance checks, determine legal process requirements and protect against cyberflight
		RAA Contractual Compliance	Let ICANN Contractual Compliance audit and respond to complaints about registrar conduct (e.g., data inaccuracy or unavailability, UDRP decision implementation, transfer complaints, data escrow and retention)
LEA/OpSec Investigators (e.g., law enforcement agencies, incident response teams)	Abuse Mitigation	Investigate Abusive Domain Name	Enable effective investigation and evidence gathering by LEA/OpSec personnel responding to an alleged maliciously-registered domain name
		Abuse Contact for Compromised Domain Name	Assist in remediation of compromised domain names by helping LEA/OpSec personnel contact the registrant or designated abuse handler/ISP
Miscreants (e.g., those engaged in spam, DDoS, phishing, identity theft, domain hijack)	Malicious Internet Activities	Domain Name Hijack	Harvest domain name registration data to gain unlawful access to registrant's account and hijacking that registrant's domain name(s)
		Malicious Domain Name Registration	Use an existing/compromised domain name registration account to register new names to support criminal, fraudulent or abusive activities
		Registration Data Mining for Spam/Scams	Harvest domain name registrant data for malicious use by spammers, scammers and other criminals (miscreants)

Table 1. Users

Figure 2 sets forth a non-exhaustive summary of users of the existing WHOIS system, including both those with constructive and malicious purposes. Consistent with the EWG's mandate, all of these users were examined to identify existing and possible future workflows and the stakeholders and data involved in them.

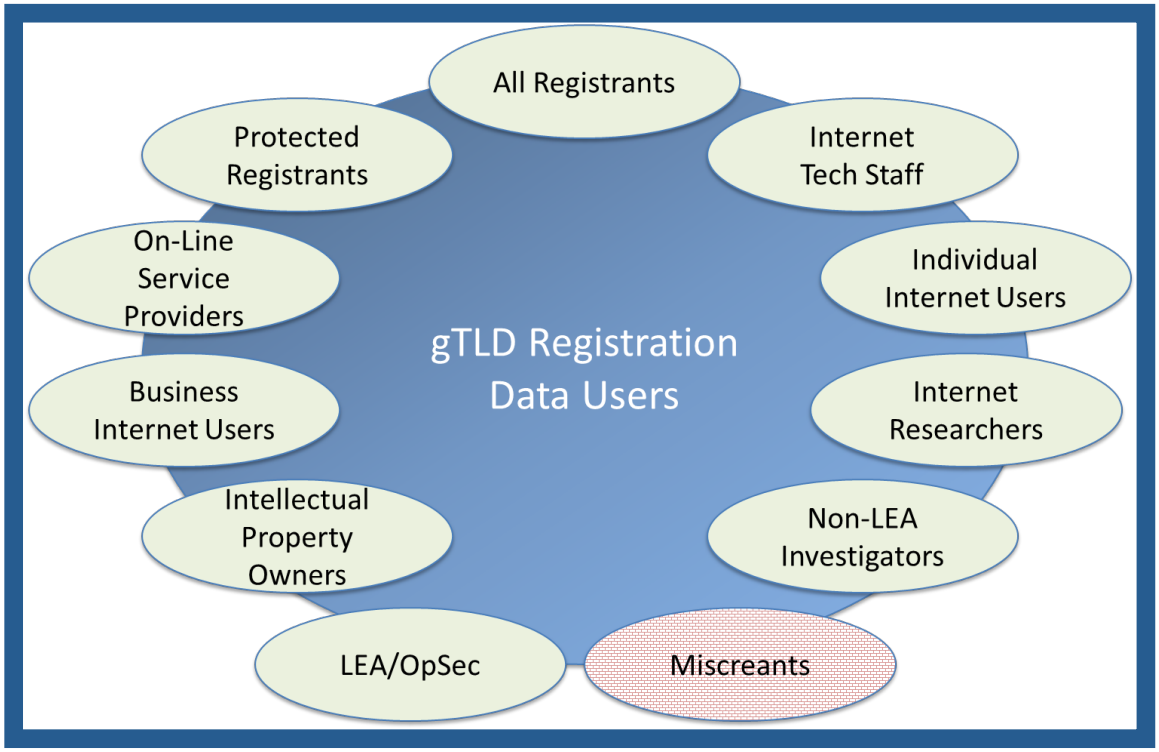

Figure 2: Users

In this report, the term "requestor" is used to refer generically to any of these users that wishes to obtain gTLD registration data from the system. As further detailed in Section IV below, the EWG recommends abandoning today's WHOIS model (and protocol) that gives every user the same anonymous public access to (too often inaccurate) gTLD registration data. Instead, the EWG recommends a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.

3.3 Identifying the Purposes to be Accommodated or Prohibited

The EWG sought to prioritize the purposes enumerated in section 3.2 in order to focus use case development and narrow the spectrum of permissible purposes. However, it was difficult to establish a rationale for accommodating the needs of some users that access the current WHOIS system today but not others, so long as their purposes were not malicious. This finding led the EWG to recommend

that all of the purposes identified in Section 3.2 be accommodated by the RDS in some manner, with the exception of known-malicious Internet activities that should be actively deterred. The EWG's recommended permissible purposes are therefore summarized below.

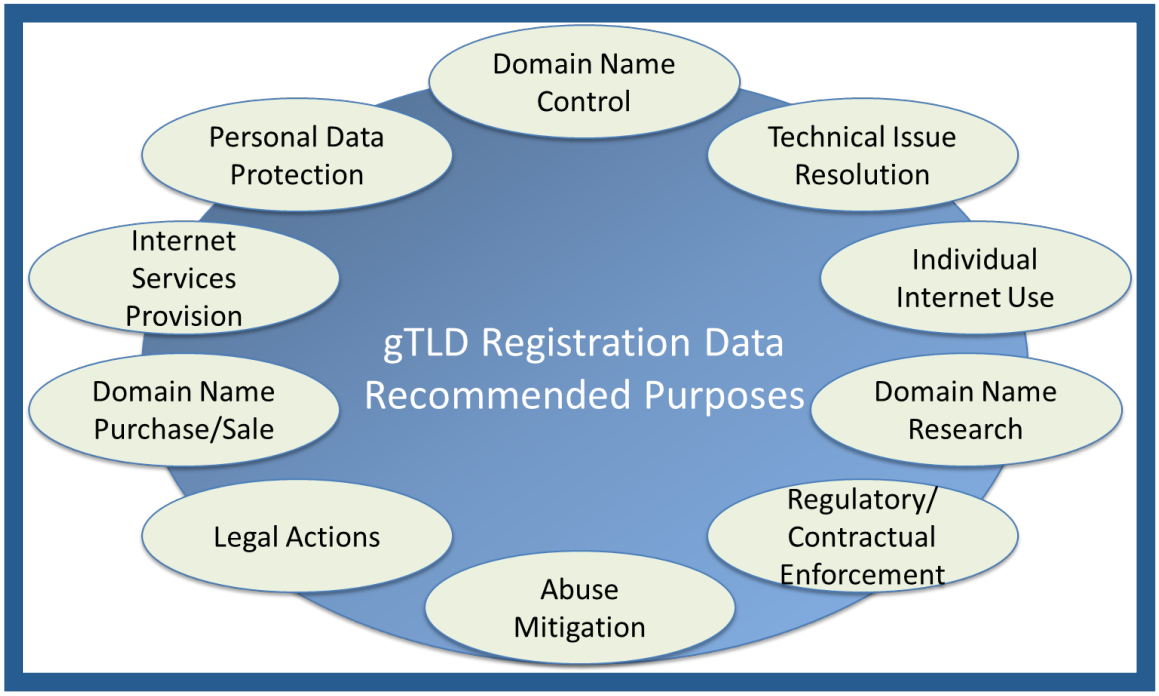

Figure 3: Purposes

It should be noted that, within each purpose, there are an infinite number of existing and possible future use cases. Although the EWG did not attempt to identify all possible use cases, it endeavoured to explore a representative sample in hopes of rigorously identifying kinds of users and their purposes in wanting access to gTLD registration data. However, the RDS should be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time.

3.4 Stakeholders Involved in the RDS

The following table provides a representative summary of the various stakeholders involved in collecting, storing, disclosing and using gTLD registration data, mapped to associated purposes. Some stakeholders supply

data (e.g., registrants), while others collect/store data (e.g., registrars, registries) or disclose data (e.g., RDS operator, Privacy/Proxy Service Providers). However, most stakeholders are parties involved in initiating data requests (e.g., brand owners, their agents) or parties identified, contacted or otherwise impacted by data disclosed (e.g., domain name abuse contacts). This summary is intended to illustrate the breadth of stakeholders most likely to be affected by the RDS. However, in any given transaction involving registration data, there may well be additional stakeholders not enumerated here.

Stakeholders	Purposes
Abuse Contact for Domain Name	Abuse Mitigation
Acquiring Company	Business Domain Name Purchase or Sale
Acquiring Company's Agents/Attorneys	Business Domain Name Purchase or Sale
Address Validation Service	Domain Name Control
Agents of Registrant	Domain Name Control
Brand Holder	Regulatory/Contractual Enforcement
Brand Management Service Provider	Domain Name Control
Brand Owner	Business Domain Name Purchase or Sale
Certification Authority	Internet Services Provision
Complainant	Regulatory/Contractual Enforcement
Consumers using Websites	Individual Internet Use
Domain Broker	Business Domain Name Purchase or Sale
Domain Buyer	Business Domain Name Purchase or Sale
Fraud Victim	Legal Actions
Fraud Victim's Agent	Legal Actions
Government Agency Personnel	Regulatory/Contractual Enforcement
ICANN Compliance	Regulatory/Contractual Enforcement
Internet Service Providers	Abuse Mitigation
Investigator	Individual Internet Use
Law Enforcement Personnel	Abuse Mitigation Legal Actions
Listed Contacts	Internet Services Provision
Online Service Provider	Internet Services Provision
Op/Sec Service Providers	Abuse Mitigation
Organization Sponsoring Study	Domain Name Research
Person/Entity under investigation	Regulatory/Contractual Enforcement
Privacy/Proxy Service Customer	Business Domain Name Purchase or Sale Domain Name Control Internet Services Provision Regulatory/Contractual Enforcement Personal Data Protection
Privacy/Proxy Service Provider	Abuse Mitigation Business Domain Name Purchase or Sale Domain Name Control Domain Name Research

	Internet Services Provision Legal Actions Personal Data Protection Regulatory/Contractual Enforcement Technical Issue Resolution
RDS Operator	All Purposes
Registrant	All Purposes
Registrant's Agent	Business Domain Name Purchase or Sale Internet Services Provision Regulatory/Contractual Enforcement
Registrar	Business Domain Name Purchase or Sale Domain Name Control Domain Name Research Individual Internet Use Internet Services Provision Legal Actions Personal Data Protection Regulatory/Contractual Enforcement Technical Issue Resolution Abuse Mitigation
Registry	All Purposes
Reporter of Problem	Technical Issue Resolution
Researcher	Domain Name Research
Reseller	Abuse Mitigation
Resolver of Problem	Technical Issue Resolution
Target of Legal/Civil Action	Individual Internet Use
Technical Contact	Technical Issue Resolution
Third Parties seeking Contact	Legal Actions Personal Data Protection
Trusted Agent	Personal Data Protection
UDRP Panellists	Regulatory/Contractual Enforcement
UDRP Provider	Regulatory/Contractual Enforcement
Validator of Heightened Need for Protection	Personal Data Protection
Victim of Abuse	Abuse Mitigation
Web Hosting Provider	Technical Issue Resolution

Table 2. Representative Summary of Stakeholders

3.5 Areas of Commonality

As the EWG analyzed use cases, it became clear that many users have needs for similar data elements, but to satisfy different purposes. Some of these needs are well understood, for example:

- The ability to determine whether a domain name is registered
- The ability to determine the current status of a domain

However, some needs are common and yet not readily fulfilled by the current WHOIS system in a consistent manner. Examples include:

- The ability to determine all domains registered by a given entity
- The ability to determine when a domain was first registered

The EWG took these common needs into consideration when developing recommended principles to guide the design of the RDS. However, since it is likely that further common needs will be identified over time, the system should be designed with extensibility in mind.

3.6 Matching Data Elements to Acceptable Purposes

Annex C describes data elements that are relevant to each acceptable purpose. Ultimately, some of these data elements should be collected for every domain name, while others may be optionally collected for a subset of domain names. Furthermore, collected data elements may or may not be made accessible to requestors through the RDS. The EWG expects to further consider these issues to derive initial recommendations in this area, but recommends that a more thorough risk and impact analysis be performed on each data element to complete this categorization. Public comment would be helpful in identifying how this risk and impact analysis should be conducted, who should conduct it, and the criteria by each data element should be identified as mandatory or optional, for collection and disclosed via public or gated access methods.

IV. DESIRED FEATURES & DESIGN PRINCIPLES

Subject to future appropriate risk and impact analysis in many areas, the EWG believes that the next generation Registration Directory Service (RDS) should incorporate the following features and design principles:

	Feature	EWG Design Principles
4.1	**Applicability**	
	4.1.1	• The RDS needs to apply to all gTLD registries, whether existing, or new. No grandfathering, or special exemption should be allowed.
4.2	**International Considerations**	
	4.2.1	• One or more policies should be established by each of the stakeholders participating in the RDS relating to data access, data use, data retention, and due process. ○ These may vary depending upon the jurisdiction. ○ These policies must enable compliance with local laws. ○ The EWG expects to explore these issues further.
	4.2.2	• To be truly global, the RDS should accommodate the display of registration data in multiple languages, scripts & character sets ○ Additional analysis is needed by IDN experts to define these requirements.
4.3	**Accountability**	
	4.3.1 4.3.2 4.3.3 4.3.4	• All parties in the domain name ecosystem have accountabilities to one another. • Registrants are accountable for providing and maintaining current, accurate & timely registration data in the RDS. • Registrants are responsible for ensuring that someone is reachable to facilitate timely resolution of any problems that arise in connection with their domain names. • Registrants should assume sole responsibility for the registration and use of their domain.

	4.3.5 4.3.6	• Registrars are accountable to provide service to registrants as specified in their contracts, including ensuring provision of current, accurate registration data. • There should be repercussions for the failure to provide and maintain accurate information. ○ The EWG expects to explore this issue further.
4.4	**Privacy Considerations**	

	4.4.1
	
	4.4.2
	
	4.4.3
	
	4.4.4
		• The RDS should accommodate needs for Privacy, including:
		  ○ An Enhanced Protected Registration Service for general personal data privacy needs; and
		  ○ A Maximum Protected Registration Service that offers Secured Protected Credentials Service for At-Risk, Free-Speech uses.
		• There should be accreditation for privacy/proxy service providers and rules regarding provision and use of accredited privacy/privacy services.
		• Outside of domain names registered via accredited privacy/proxy services, all registrants should assume responsibility for the domain names they register.
		• The EWG expects to explore this issue further, including:
		  ○ Standardized processes to be implemented by all accredited Privacy and Proxy service providers.
		  ○ Specific processes related to handling of requests made by accredited Law Enforcement Agencies.
		  ○ Specific processes related to handling of requests made by other licensed Requestors (e.g., Intellectual Property Owners).

4.5	**Permissible Purposes**	
	4.5.1 4.5.2	• There should be clearly defined permissible/impermissible uses of the system. • **Section 3** broadly describes the acceptable uses identified by the EWG.

4.6	Data Disclosure	
	4.6.1	• The RDS should accommodate purpose-driven disclosure of data elements.
	4.6.2	• Not all data collected is to be public; disclosure options should depend upon Requestor and Purpose.
	4.6.3	• Public access to an identified minimum data set should be made available, with restrictions to limit bulk harvesting.
	4.6.4	• Data Elements determined to be more sensitive after conducting the risk & impact assessment should be protected by gated access, based upon: ▪ Identification of a permissible purpose ▪ Truthful disclosure of requestor/purpose ▪ Auditing/Compliance to ensure that gated access is not abused
	4.6.5	• Some data elements determined (after conducting the risk & impact analysis) to be extremely sensitive could be accessed through defined legal process (e.g., subpoena).
	4.6.6	• Only the data elements permissible for the declared purpose should be disclosed.
	4.6.7	• **Annex C** describes the data elements identified as relevant to the specific acceptable uses identified in **Annex B**.
4.7	**Data Elements**	
	4.7.1	• The only data elements that should be collected are those with at least one permissible purpose.
	4.7.2	• Each data element should be associated with permissible purposes, based upon the acceptable uses identified.
	4.7.3	• The list of minimum data elements to be collected, stored and publically disclosed should be based on a risk assessment.
	4.7.4	• To enable extensibility, the system should accommodate any additional data elements collected by registries by making

	4.7.5	them accessible through the common access methods and interfaces. • The full set of data elements should be stored by registries.
4.8	**Access Methods**	
	4.8.1 4.8.2 4.8.3 4.8.4 4.8.5 4.8.6	• Access should be non-discriminatory (i.e., the process should create a level playing field for all requestors, within the same purpose). • To deter misuse and promote accountability, ○ All access should be authenticated to the appropriate level; and ○ Requestors needing access to data elements should be able to apply for and receive credentials for use in future authenticated data access queries. • Some type of accreditation should be applied to requestors of gated access ○ When accredited Requestors query data, their purpose should be [alternative a] implied, or [alternative b] stated every time a request is made?[2] ○ Different terms and conditions may be applied to different purposes. ○ If accredited requestors violate terms and conditions, penalties should apply. • All queries/responses should protect the confidentiality and integrity of data in transit. • Premium data access services (e.g., Reverse WHOIS, WhoWas) may be offered, subject to some type of accreditation regime. • All disclosures should occur through defined access methods. The entire data set should not be exported in bulk form for

[2] The EWG expects to explore these two alternatives further.

	4.8.7	uncontrolled access. • Disclosure may include display and other output methods. ○ To make data easier to find and access in a consistent manner, a central point of access (e.g., web portal) should be offered. ○ Access to public data should be available to all requestors through an anonymous query method (at minimum, via website). ○ Gated access to sensitive data should be supported through web and other access methods and formats (e.g., xml responses, SMS, email), based on requestor and purpose. ○ Requestors should be able to obtain authoritative data in real-time when needed.
4.9	**Validation and Accuracy**	
	4.9.1 4.9.2 4.9.3	• To improve data quality, Registrant data should be validated syntactically (i.e., checked for correct format [per SAC58]) at the time of collection. • To improve usability, Registrant name/contact data should be validated operationally. (i.e., checked for reachability). • To reduce fraud ○ Registrants should be able to pre-validate by supplying a globally unique Registrant name/organization and associated contact prior to initial domain name registration. ○ Once pre-validated data has been checked for accuracy and uniqueness, an auth code (e.g., PIN) should be issued to that Registrant. No domain names

		should be registered with an identical[3] name/organization without supplying this auth code. ○ ICANN should enter into an appropriate contract with a third party provider to perform this pre-validation service and issue auth codes.
	4.9.4	• To promote consistency and uniformity and simplify maintenance, ○ Pre-validated data elements should be reusable – that is, applied to future registrations, with an option to over-ride these defaults on a per-domain name basis. ○ Any updates to pre-validated data elements could be automatically applied to all linked domain names.
	4.9.5	• To improve quality, Registrant name/contact data that is not pre-validated should still be validated in some way (e.g., implicitly via successful credit card payment with name/contact).
	4.9.6	• To preserve rapid activation while still promoting quality, delayed validation of Registrant name/contact should not prevent successful registration and DNS listing. However, such domain names could be flagged and suspended/deleted, if not validated within a defined period.
	4.9.7	• To enable successful Registrant name/contact validation globally, operational validation methods should not rely exclusively upon a single contact method (e.g., postal address).
	4.9.8	• To maintain the quality of data over time, validated data elements should be periodically re-validated – for example, whenever name/contact updates are made or domain names linked to a previously validated name/contact are transferred.
	4.9.9	• The system should record whether each data element was validated and when,

[3] The EWG expects to explore this further.

	4.9.10	even for data elements that are never disclosed. • To promote successful registration of domain names linked to high-quality name/contact data, Registrants must be educated about this process and associated policies.
4.10.	**Standard Validation Service**	
	4.10.1	• Use of a standard validation service is preferable because it: o Reduces costs/burdens on Registrars/Registries. o Enables more efficient licensing of validation databases such as UPS address cross-checking, yellow pages, corporate/company, government registries, electoral rolls, credit bureau records, etc. o Standardizes the validation procedures as appropriate for a specific country/jurisdiction. o Reduces the number of compliance inquiries on registries/registrars.
	4.10.2	• ICANN should enter into an appropriate contract with the third party provider of standard validation services in a manner that enables data accuracy compliance, auditing & availability.

4.11	**Contractual Relationships**	
	4.11.1 4.11.2 4.11.3 4.11.4	• A truly international third party provider should operate the RDS. • ICANN should enter into appropriate contract with the third party provider of the RDS to enable compliance, auditing and availability. • ICANN should enter into appropriate contracts with the standard validation service provider, privacy/proxy service providers, secured credential providers, and others that may interact with the RDS. • ICANN should amend existing agreements (RAA, Registry Agreements) to accommodate the RDS and eliminate legacy requirements.
4.12	**Storage and Escrow Requirements**	
	4.12.1 4.12.2 4.12.3	• To maintain redundant systems and eliminate the single point of failure, the data should reside at multiple locations (e.g., registrar, registry, escrow, and RDS). • Audits should be conducted of escrowed data to test the format, integrity, and completeness. • The RDS should maintain the data elements in a secure fashion, protecting the confidentiality and integrity of the data elements at risk from unauthorized use.
4.13	**Costs of Operating and Accessing the RDS**	
	4.13.1	• The issue of cost is an important aspect of the RDS. The EWG expects to explore this issue further, including costs of development and operation and possible ways in which these expenses might be borne (e.g., absorbed by RDS funding, offset by value-added service fees).

V. SUGGESTED MODEL

The need to collect, store, and disclose accurate data elements for various purposes led the EWG to propose a rough model for a next generation RDS that satisfies the principles identified in Section 4. Each player in the RDS eco-system has different needs for data, different risks, and potentially different responsibilities. Historically, most of these responsibilities were transferred to the Registrars, whose primary goals were to provide working domain names to customers, and to maintain paying customers. The EWG recognizes that as the Internet ecosystem becomes more complex, and hundreds of new gTLDs are introduced, it is likely that new players will be required to take on some of the many responsibilities that come with satisfying such a broad range of registration data purposes.

Based on the feature and design principles set forth in Section IV, Figure 4 below illustrates the EWG's recommended model for a next generation RDS that could potentially incorporate many of these principles.

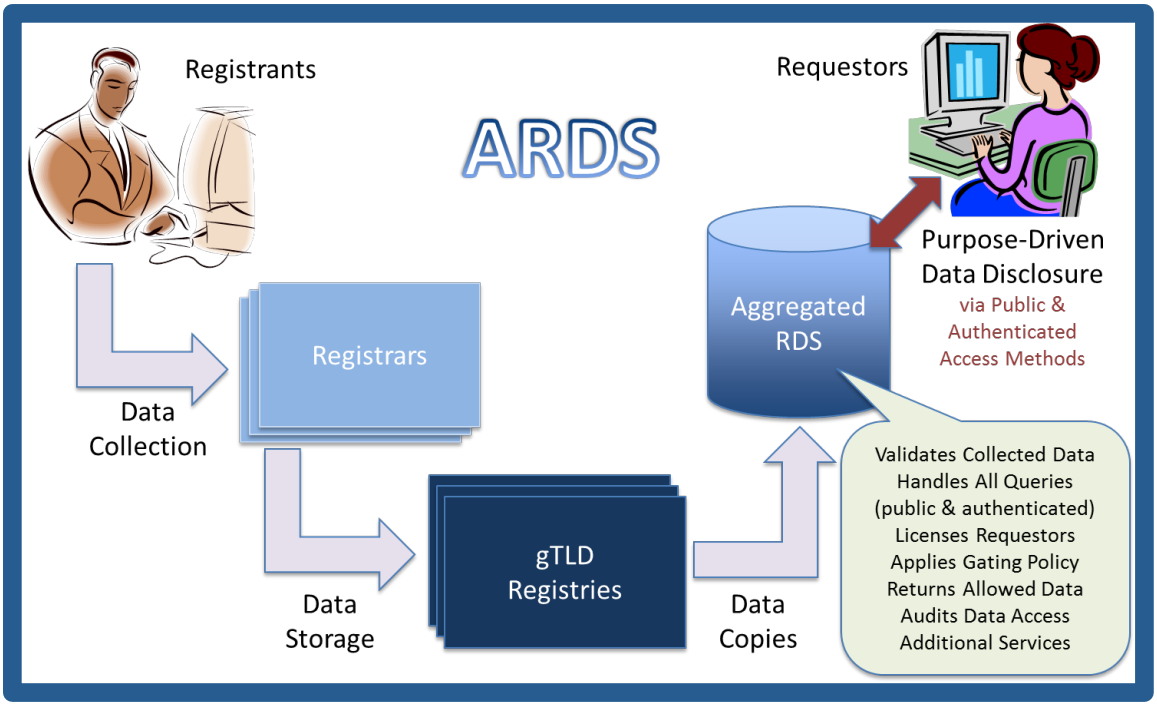

Figure 4. Aggregated RDS Model

5.1 Examination of Multiple System Designs

After identifying the recommended principles and desired features for a new RDS, the EWG considered several alternative models to determine how each model might address the identified registration data needs. The EWG evaluated distributed systems, such as that employed by today's WHOIS system, as well as aggregated systems. The EWG also considered a proxy-type system, where a third-party would serve as an intermediary to enable access to, but not as a repository of, the data queried. The work of the Zone File Access (ZFA) Advisory Group[4] that considered similar issues in the context of the New gTLD Program was valuable in informing the EWG's understanding in this regard.

Distributed systems present shortcomings that could be better served by alternative models. With potentially thousands of registries coming online, the EWG recognized that continuing the current distributed system introduces inefficiencies and additional costs as consumers of this information may have to deal with differing formats, credentials, access points, licensing terms, and other hurdles that may be created by the registry or registrar. As noted by the ZFA Advisory group, when "disparate access systems are used, processes or automation implemented by zone file consumers are more prone to break. When errors result in loss of access, problem resolution is cumbersome for data consumers, since the consumer must engage with unique reporting systems to resolve the problem."[5] These issues would equally apply to the RDS.

In addition, the costs associated with requiring each registry and/or registrar to modify their systems to create a new distributed system to implement a next generation RDS will likely constrain innovation and adoption, given that there is

[4] See archives of the Zone File Access Advisory group for more information at: http://archive.icann.org/en/topics/new-gtlds/zone-file-access-en.htm

[5] See Zone File Concept Paper, posted at: http://archive.icann.org/en/topics/new-gtlds/zfa-concept-paper-18feb10-en.pdf

no apparent financial or operational incentive to support significant changes to the method by which this data is accessed. As noted by the ZFA Advisory Group:

> "In general, providing reliable access to zone file data imposes operational costs and liabilities on the gTLD registries without direct compensation. While this has been accepted by registry operators as a cost associated with operating one of the Internet's primary namespaces, it would be logical for registries to lower these costs if there were more efficient ways to provide this access. For example, registries are required to provide continuous access to all takers, without any specific Service Level Agreements (SLA's) specified. This clearly costs money to operate… The registry is also responsible for providing a secure connection and clean data file to data consumers, which creates significant security requirements for registries."[6]

Moreover, both distributed or proxy systems make it difficult or impossible to offer commonly needed features such as a cross TLD registrant look-up, reverse registrant-domain look-up or even a historical ownership-type registry. All of these features could be made possible through an aggregated database that collects and maintains the applicable data.

5.2 Aggregated RDS Suggested

An aggregated RDS (ARDS) model (as illustrated above) was supported by a consensus of the EWG, as one way of addressing the desired features and design principles identified in Section 4 above.

In the proposed model:

- ARDS serves as an aggregated repository that contains a non-authoritative copy of all of the collected data elements

[6] See the Zone File Access Concept Paper for additional considerations.

- Each gTLD registry remains the authoritative source of the data
- Requestors apply for access credentials to the ARDS
- Registrars/Registries are relieved of obligations to provide Port 43 access or other public access requirements
- In most cases, the ARDS provides access to cached registration data that is copied from gTLD registries with frequent periodic updates.
- The ARDS can also provide access to live registration data that is obtained in real-time from gTLD registries, upon request. ARDS (or other third party interacting with ARDS) would be responsible for performing validation services
- ARDS is responsible for auditing access to minimize abuse and impose penalties and other remedies for inappropriate access
- ARDS handles data accuracy complaints
- ARDS manages licensing arrangements for access to data
- ICANN contracts with an international third-party to develop and operate the ARDS and monitors compliance with requirements

	Aggregated RDS Model
Advantages	• Scale handled by a single point of contact • Potential improvements in transport and delivery • "One stop shop" for requestors of Registration Data • Greater accountability for Registration Data validation and access (anti abuse) • Ability to track/audit/penalize requestors in the same way over multiple TLDs (anti abuse) • May reduce some costs currently borne by Registrars and Registries to provide data access • Normalization or filtering of the data could be provided • Reduces bandwidth requirements for Registries and Registrars • Facilitates standardization of approaches to satisfy local data privacy concerns

	Aggregated RDS Model
	• Enhanced search capability across multiple TLDs (such as reverse look-ups) • Minimizes transition and implementation costs • Enables validation/accreditation of requestors qualifying for special purposes (i.e., law enforcement) • Facilitates more efficient management of inaccuracy reports • Enables more efficient random accuracy checks • Enables user friendly search portal displays in multiple languages, scripts and characters
Disadvantages	• Data Latency • Creation of "Big Data" source of highly valuable data with potential for misuse if not properly audited & maintained • Increased risk of insider abuse and external attack, requiring greater attention to security policy implementation, enforcement and auditing • Registries/Registrars no longer control delivery of registration data

VI. ADDRESSING PRIVACY CONCERNS

Central to the remit of the EWG is the question of accuracy of the registration data. If the next generation RDS calls for much greater accuracy of registration data, then a number of issues immediately arise, perhaps the most contentious of which is privacy.

The EWG recognizes the need for accuracy, along with the need to protect the privacy of those registrants who may require heightened protections of their personal information. Examples of registrants that could qualify for these heightened protections include individuals or groups under threat, those who wish to exercise rights of free speech on the Internet which are widely regarded as protected, or where identification of speakers would cause a threat to their lives or those of their families.

In accordance with recommended principles enumerated in section 4.4, the EWG has discussed ways in which the RDS might accommodate at-risk user needs for maximum protected registration services using “secure protected credentials.” One option might be to have ICANN accredit an independent organization to act as a Trusted Agent that, using a set of agreed criteria, would determine whether a registrant qualified for maximum protection. The EWG expects to further consider potential models for secure protected credentials which might strike an innovative, effective balance between accountability and the personal data privacy needs of at-risk Internet users.

VII. ILLUSTRATION OF GATED ACCESS FEATURES

The proposed model for Gated Access (illustrated in Figure 5) can be summarized as follows:

- A carefully selected subset of data elements would be made publically accessible to anonymous requestors through a web interface[7] to the RDS.
- All other data elements would be made accessible to authenticated requestors only through multi-modal gated access methods supported by the RDS.
- Gated access would only be available to requestors who applied for and were issued credentials to be used for RDS query authentication. The process by which credentials would be issued is not defined herein, but the EWG recommends that this process take into consideration each requestor's purpose for wanting access to registration data.
- Each gated access query would identify the authenticated requestor's purpose (either explicitly or implicitly) and a desired list of data elements. Only data elements that were available for the domain name and accessible to the requestor for the declared purpose would be returned.

The EWG expects to further discuss multi-modal access methods and how they could be enabled by existing or future registration data access protocols.

[7] The EWG expects to further explore the possibility of making some registration data elements associated with a visited website's domain name accessible via browser integration.

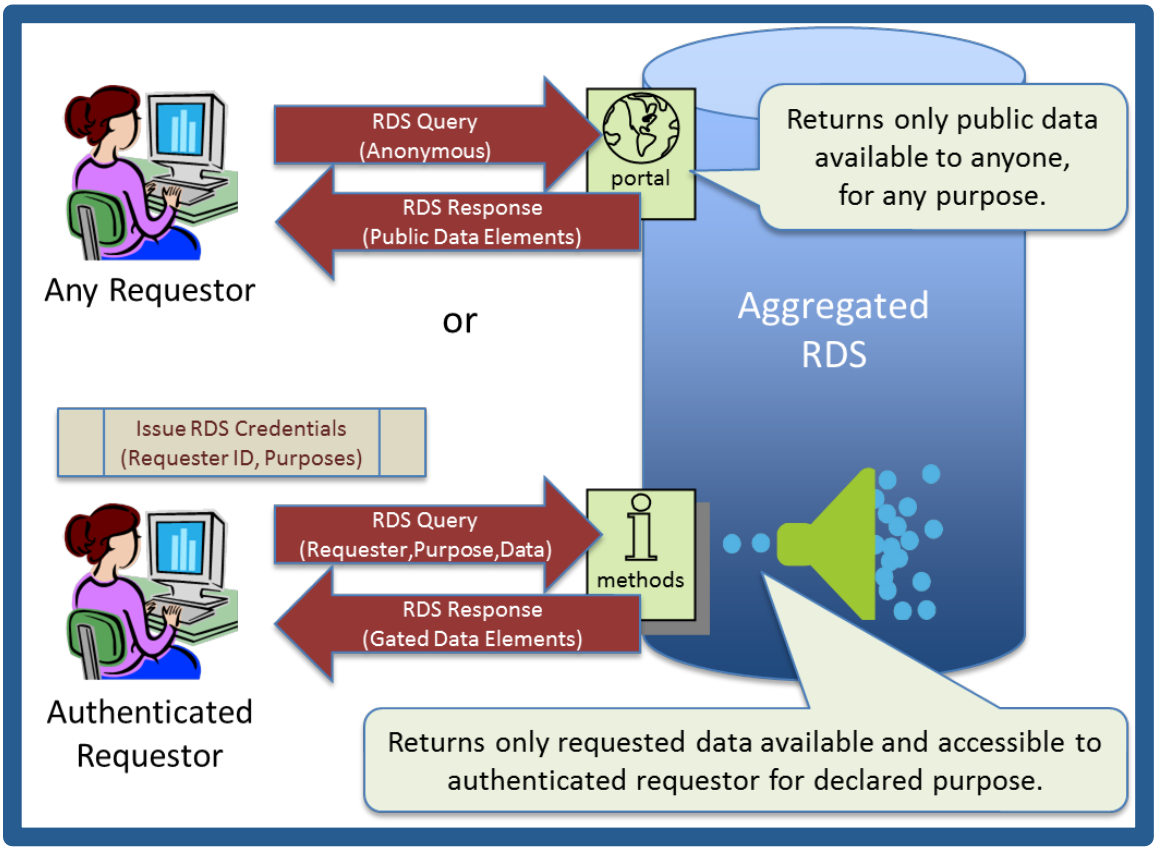

Figure 5. Gated Access Model

VIII. CONCLUSION & NEXT STEPS

The EWG suggests the adoption of an aggregated RDS to replace the current WHOIS System to satisfy the design principles and features identified by the EWG and described more thoroughly in this Report. This includes support for a "secured protected credentials" feature that provides heightened privacy protections for those registrants that are considered at-risk, such as those exercising their free-speech rights. It also sets forth recommendations for validating collected registration data to increase accuracy, along with greater accountability through "gated access" controls that enable requesters with a need for additional information to apply for credentials for limited access, based upon the stated purpose. The proposed model incorporates accountability and auditing capabilities intended to penalize misuse by those requesters who may seek access beyond their authorized level.

It is important to recognize that the proposed model reflects hard-fought compromises from among the diverse membership of the EWG, and will surely not satisfy all stakeholders affected by the RDS. However, the EWG hopes that these recommendations will, as a whole, be recognized as a significant improvement over the current WHOIS system.

The EWG welcomes public comment online and debate with the ICANN community at the ICANN Durban Meeting on specific questions identified in the forum, as well as any other comments on this Report, to inform its future deliberations. Following the public consultation on this Report, the EWG will reconvene to reflect upon the comments received, and to make appropriate revisions to its recommendations. Upon conclusion of the EWG's deliberations, a Final Report will be published and delivered to ICANN's CEO and Board to serve as a foundation for new gTLD policy and contractual negotiations, as appropriate. As specified by the Board, an issues report based on the Final Report will form the basis of a Board-initiated, tightly focused GNSO policy development process (PDP).

ANNEX A

RESPONSE TO THE BOARD'S QUESTIONS

The Board's resolution that directed the EWG's work included a series of specific questions to be answered as it conducted its analysis. This Annex references the sections of this Initial Report that address the Board's concerns, and identifies areas where further work is to be undertaken by the EWG:

Board Questions & Guidance Requested	Report Sections
EWG redefine the purpose of: • collecting, • maintaining • providing access to gTLD registration data • Consider safeguards for protecting data	2.2, 3.2, 3.3, 4.5, 4.7, 4.8, 4.12
Why are data collected?	2.2, 3.2, 3.3, 4.5
What purpose will the data serve?	2.2, 3.2, 3.3, 4.5
Who collects the data?	V, Figure 4
Where is data stored and how long is it stored?	V, Figure 4, length of time TBD
Where is data escrowed and how long is it escrowed?	TBD
Who needs the data and why?	3.2, Table 1, Annex B & C
Who needs access to logs of access to data and why?	TBD
Public access to details about domain name registration	4.6.2-4.6.3
Law enforcement access to details about a domain name registration	3.2, 3.4, Figures 2 & 3, Annex B & C
Intellectual property owner access to details about a domain name registration	3.2, 3.4, Figures 2 & 3, Annex B & C
Security practitioner access to details about a domain name registration	3.2, 3.4, Figures 2 & 3, Annex B & C
What value does the public realize with access to registration data?	2.2
Of all the registration data available, which does the public need access to?	TBD, Annex C
Is the WHOIS protocol the best choice for providing that access?	3.1
Security	
What comprises a legitimate law enforcement need?	TBD
How is a law enforcement agent identified?	TBD
What registration data and to what level of accuracy comprises the real identity of the responsible party?	TBD

What registration data and to what level of accuracy comprises valuable information to a law enforcement agent that is looking for the real identity of the responsible party?	TBD
Is the WHOIS protocol the best choice for providing that	3.1
Intellectual Property	
Is the desired domain name registration data access consistent with access that intellectual property owners have to similar types of data in other industries?	TBD
How is an intellectual property owner identified?	TBD
Of all the registration data available, what does an intellectual property owner need access to?	Annex C
What registration data is appropriate to be made available?	TBD, Annex C
Is the WHOIS protocol the appropriate method for access?	3.1
How is the party to be provided access to be identified?	TBD

ANNEX B
EXAMPLE USE CASES

As described in Section 3, the EWG analyzed actual use cases involving the current WHOIS system to identify users who want access to gTLD registration data, their purposes for doing so, and the stakeholders and data involved. A list of representative uses cases considered by the EWG is provided below.

Purpose	Example Use Cases
Domain Name Control	Domain Name Registration Account Creation
	Domain Name Data Modification Monitoring
	Domain Name Portfolio Management
	Domain Name Transfers
	Domain Name Deletions
	Domain Name DNS Updates
	Domain Name Renewals
	Domain Name Contact Validation
Personal Data Protection	Enhanced Protected Registration
	Maximum Protected Registration
Technical Issue Resolution	Contact with Domain Name Technical Staff
Internet Services Provision	Contact with Domain Name Registrant
	Domain Name Reputation Services
	Domain Name Certification Services
Individual Internet Use	Real World Contact
	Consumer Protection
	Legal/Civil Action
Business Domain Name Purchase or Sale	Domain Name Brokered Sale
	Domain Name Trademark Clearance
	Domain Name Acquisition
	Domain Name Purchase Inquiry
	Domain Name Registration History
	Domain Names for Specified Registrant
Domain Name Research	Domain Name Registration History
	Domain Names for Specified Registrant
	Domain Name Registrant Contact
Legal Actions	Proxy Service Provider Customer Identification
	Domain Name User Contact
	Combat Fraudulent Use of Registrant Data
Regulatory and Contractual Enforcement	Online Tax Investigation
	UDRP Proceedings
	RAA Contractual Compliance
Abuse Mitigation	Investigate Abusive Domain Name
	Abuse Contact for Compromised Domain Name
Malicious Internet Activities	Domain Name Hijack
	Malicious Domain Name Registration
	Registration Data Mining for Spam/Scams

Table 3. Example Use Cases

To illustrate the EWG's methodology, a single use case is given below. The final version of this report will include links to several published use cases to more fully illustrate the breadth of users, purposes and needs considered.

Technical Issue Resolution – Contact with Domain Name Technical Staff

Goal/Scenario #1
A person experiences an operational or technical issue with a registered domain name. They want to know if there's someone they can contact to resolve the problem in real or near-real time, so they use the RDS to identify an appropriate person, role, or entity that possesses the ability to resolve the issue. An incomplete list of examples of technical issues includes email sending and delivery issues, DNS resolution issues, and web site functional issues.

Brief Format Use Case

Use Case: Identify a person, role, or entity that can help resolve a technical issue with a domain name.

Main Use Case: A person accesses the RDS to obtain contact information associated with registered domain names under a TLD or TLDs. The person submits a domain name to the RDS for processing. The RDS returns information associated with the domain name that identifies a person, role, or entity that can be contacted to resolve technical issues.

Casual Format Use Case

Title: Identify a person, role, or entity that can resolve a technical issue with a domain name.

Primary Actor: Person experiencing a technical issue with a registered domain name.

Other stakeholders: Operator of the RDS; person, role, or entity associated with the registered domain name who can resolve technical issues; registrant (who may care to know about operational issues); registrar or hosting provider (who may be providing an operational service); privacy/proxy service provider (who may assist in reaching the person, role, or entity associated with the domain name who can resolve technical issues).

Scope: Interacting with RDS

Level: User Task

Data Elements: Data elements that allow communication in real or near-real time are the most useful in the context of this use case. These include an email address, an instant messaging address, a telephone number, and/or an indicator that identifies the preferred contact method specified by the registrant. Section 4 of RFC 2142 describes recommendations for abuse@, noc@, and security@ email addresses to "provide recourse for customers, providers and others who are experiencing difficulties with the organization's Internet service", but it is important to note that the public nature of these addresses often makes them attractive to unsolicited bulk email senders.

Story: A person (requestor) experiencing a technical issue with a registered domain name accesses the RDS to obtain information about registered domain names under a TLD or TLDs. The RDS could be accessible via a website or some other electronic processing means.

The requestor submits a registered domain name to the system for processing.

The RDS processes the request and either reports error conditions or proceeds to query gTLD registration data to retrieve information associated with a person, role, or entity that has been previously identified as a resource to help resolve technical issues for this domain name.

The RDS returns either the registration data associated with the domain name or an error condition that was encountered while retrieving the data.

Figure 6. Example Use Case

ANNEX C
PURPOSES AND DATA NEEDS

As described in Section 3, the EWG analyzed use cases to identify users who want access to gTLD registration data, their purposes for doing so, and the stakeholders and data involved. The following table summarizes existing and potential RDS data elements, mapped to permissible purposes.

- Bolded data elements are publically accessible through today's WHOIS system, although not always present in every WHOIS record.
- Non-bolded data elements were identified as desired to fully-address the associated purposes, but not generally presented through WHOIS today.

The EWG intends to continue its work in this area by classifying data elements as (i) mandatory to collect at time of registration, (ii) optional to collect at time of registration or (iii) metadata supplied by the registrar/registry.

Furthermore, these data elements have yet to be categorized as (i) publically accessible, (ii) accessible via gated access by authenticated requestors for specified purposes or (iii) inaccessible through the RDS.

Note that, in accordance with principles in Section 4, the EWG recommends that this categorization be based on risk assessment and that only data elements with at least one permissible purpose should be collected by the RDS and that collected data be validated. However, this list of data elements is not exhaustive; the EWG recommends that the RDS provide common access methods and interfaces to additional data elements that may be collected for some gTLDs or by some registries.

Data Element	Purposes
Registrant Name/Organization	Domain Name Control Personal Data Protection Technical Issue Resolution Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Registrant Postal Address	Domain Name Control Personal Data Protection Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Registrant Telephone Number	Domain Name Control Personal Data Protection Technical Issue Resolution Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Registrant Email Address	Domain Name Control Personal Data Protection Technical Issue Resolution Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Registrant Fax Number	Domain Name Control Regulatory/Contractual Enforcement

Data Element	Purposes
Registrant IM/SMS	Domain Name Control Personal Data Protection Technical Issue Resolution Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Registrant Preferred Contact Method	Domain Name Control Personal Data Protection Technical Issue Resolution Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Registrant Contact Role	Domain Name Control Personal Data Protection Technical Issue Resolution Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Original Registration Date	Domain Name Research Business Domain Name Purchase/Sale Regulatory/Contractual Enforcement
Client Status	**Domain Name Control** **Business Domain Name Purchase/Sale** **Domain Name Research** **Regulatory/Contractual Enforcement** **Abuse Mitigation**
Server Status	**Domain Name Control** **Business Domain Name Purchase/Sale** **Domain Name Research** **Regulatory/Contractual Enforcement** **Abuse Mitigation**
Creation Date	**Domain Name Control** **Business Domain Name Purchase/Sale** **Domain Name Research** **Regulatory/Contractual Enforcement** **Abuse Mitigation**

Data Element	Purposes
Updated Date	**Domain Name Control** **Business Domain Name Purchase/Sale** **Domain Name Research** **Regulatory/Contractual Enforcement** **Abuse Mitigation**
Expiration Date	**Domain Name Control** **Business Domain Name Purchase/Sale** **Domain Name Research** **Regulatory/Contractual Enforcement** **Abuse Mitigation**
DNS Servers	**Domain Name Control** **Business Domain Name Purchase/Sale** **Regulatory/Contractual Enforcement** **Abuse Mitigation**
Registrant Company Identifier (e.g., Trading Name)	Domain Name Control Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation
Registrant IP Address (used to register DN)	Abuse Mitigation
Registrant Account Data (used to register DN)	Domain Name Control Regulatory/Contractual Enforcement Abuse Mitigation
Privacy/Proxy Service Customer	Domain Name Control Business Domain Name Purchase/Sale Personal Data Protection Legal Actions Regulatory/Contractual Enforcement Abuse Mitigation
Domain Name Purpose (Commercial/Non-Commercial)	Personal Data Protection Individual Internet Use Business Domain Name Purchase/Sale Domain Name Research Legal Actions Regulatory/Contractual Enforcement
Reseller (used to register DN)	Domain Name Control Regulatory/Contractual Enforcement Abuse Mitigation
Registrant Type (Legal/Natural Person, Proxy/Third Party)	Domain Name Control Business Domain Name Purchase/Sale Personal Data Protection Legal Actions Regulatory/Contractual Enforcement Abuse Mitigation

Data Element	Purposes
Privacy/Proxy Service Provider	Domain Name Control Business Domain Name Purchase/Sale Personal Data Protection Legal Actions Regulatory/Contractual Enforcement Abuse Mitigation
Registration Agreement Language	Domain Name Control Regulatory/Contractual Enforcement
Registrar Jurisdiction	Domain Name Control Regulatory/Contractual Enforcement
EPP Transfer Key	Domain Name Control

ANNEX D
BACKGROUND ON THE EWG

Background

In December 2012, ICANN's President and CEO announced the creation of an Expert Working Group on gTLD Directory Services (EWG). The EWG was convened as a first step in fulfilling the ICANN Board's directive[8] to help redefine the purpose and provision of gTLD registration data (such as WHOIS), with the stated goal of providing a foundation for the creation of a new global policy for gTLD directory services and contract negotiations. A Board-directed Generic Names Supporting Organization (GNSO) policy development process (PDP) is to follow the work of the EWG to evaluate the policy implications of the EWG's recommendations.

Working Group Volunteers

ICANN received expressions of interest from dozens of highly qualified experts from across the Internet ecosystem. In selecting the EWG, geographical diversity and balance criteria were considered, along with each candidates' operational and understanding of the WHOIS, their consensus-building skills, and aptitude to innovate. After an extensive evaluation of each of the candidates against these criteria, a unique group of individuals was selected to participate in this key project, led by Jean-Francois Baril, the EWG's facilitator.[9]

---

[8] The Board Resolution is posted at: http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm

[9] Biographies of each of the EWG members are posted at: http://www.icann.org/en/news/announcements/announcement-14feb13-en.htm

EWG Mode of Operation

The EWG participated in a series of in-person and telephonic conference calls, including multiple, all-day, face-to-face sessions, held in Los Angeles, Beijing and London.[10] In addition, the EWG sought input from the ICANN community at its session in Beijing.[11] These meetings and intense work sessions resulted in the draft proposals that are described in this Initial Report.

[10] Meeting reports for each of the EWG's face to face sessions are posted at: https://community.icann.org/pages/viewpage.action?pageId=40175189

[11] The transcript from the Beijing Public Session and presentation materials are available at: http://beijing46.icann.org/node/37051 .

ANNEX E
POLICY CONSIDERATIONS

To be provided in the EWG Final Report.