**Expert Working Group on gTLD Directory Services (EWG)**
**Frequently Asked Questions (FAQs) – 2014 Final Report Update**

## Origin and Purpose of the EWG

1) What is the Expert Working Group (EWG)?
2) Who are the members of the EWG?
3) What is the EWG's objective? How does it differ from the WHOIS RT?
4) What did the EWG produce and when?
66) How does the RDS make life simpler for individual registrants?

## Origin and Purpose of the RDS

5) What is the next-generation gTLD Registration Directory Service (RDS)?
6) Why is a next-generation RDS really needed?
7) What makes the RDS fundamentally different from today's WHOIS?
8) Why is the RDS so complicated?

## Registration Data Users and Purposes

9) Who are the users of the RDS? How did the EWG determine this?
10) Why do those users need access to registration data?
11) Which purposes should not be permissible?
12) Why didn't the EWG consider user X or purpose Y?
67) How will members of the press and bloggers gain access to RDS data?

## Registration Data Elements

13) What registration data should be collected and stored by the RDS?
14) How would gTLD-specific data be accommodated?
15) Why is the RDS only concerned with gTLD registration data?
16) How would RDS data differ from WHOIS data?
17) Would the RDS collect the same registrant data for domains used for commerce?
18) When and how will a risk assessment be performed?

## Registration Data Collection and Storage

19) What roles do registrars, registries and the RDS play in data collection and storage?
20) How would "Contacts" and "Contact IDs" be created?
21) How would contacts be used in domain name registrations?
69) Why is Legal Contact mandatory? Is it publicly available, outside the gate?
70) Why is Business Contact mandatory? Is it publicly available outside the gate?
22) What data would be mandatory to collect/store?
23) How long would data be stored by the RDS?
24) Where would data be stored by the RDS?

## Purpose-Driven Data Access and Disclosure

25) What is purpose-driven registration data access?
26) Does the RDS eliminate free public access to registration data?
27) Who would have gated access to registration data?
28) What would deter abuse of gated access?

29) Would registrars and registries still be able to provide direct access?

30) Would the RDS provide WhoWas and Reverse query services?
68) How are third party commercial providers that use WHOIS today accommodated?

## Addressing Registration Data Privacy Concerns

31) Would privacy and proxy services still exist in the RDS? How would they differ?
32) How would the RDS accommodate the personal data privacy needs of at-risk registrants?
33) What would prevent insider abuse or external hacking of RDS data?
34) How would the RDS comply with local data protection laws?
35) Will the RDS require Registrants to publish all of their personal data?
36) Do purpose-based contacts require registrants to publish their personal data?
37) Will requestors that "get through the gate" have access to everything?
38) How would law enforcement access the RDS?

## Addressing Registration Data Accuracy Concerns

39) Why would RDS data be any more accurate than today's WHOIS data?
40) How and when would the RDS validate registration data?
41) Wouldn't registrars and registries still have to validate data?
42) How would the RDS deal with inaccurate registration data?
43) What is the unique contract data option and how would it help prevent identity theft?
44) Who will serve as Validators?
45) How will data be validated cost-effectively on a global scale?

## Addressing Registration Data Accountability Concerns

46) Would the RDS offer greater accountability for unauthenticated public data access?
47) How would credentials be issued for gated access?
48) Who would decide which requestors should have access to which data elements?
49) How would the RDS hold requestors accountable for use of data obtained via gated access?
50) Who will accredit RDS users?

## Suggested Model and Benefits/Limitations

51) Why did the EWG suggest a Synchronized RDS model?
52) What are the primary benefits of the SRDS model?
53) Doesn't the SRDS model elevate risk of abuse and attack?
54) What other models did the EWG consider? Why weren't they chosen?
55) Who will operate the RDS?

## Impacts and Costs

56) What would the RDS cost to build?
57) Would registrant's costs increase?
58) Would requestor's costs increase?
59) In what ways would the RDS likely reduce cost?

60) How would registrar obligations be reduced?
61) How would registry obligations be reduced?

## Next Steps

62) What did the EWG do with comments on its draft and update reports?
63) When did the EWG produce its final report?
64) What will be done with the EWG's final report?
65) Will WHOIS go away?

## Origin and Purpose of the EWG

1) What is the Expert Working Group (EWG)?
The EWG was formed by ICANN's President & CEO, at the request of ICANN's Board, to help resolve deadlock within the ICANN community on how to replace the current WHOIS system with a next-generation gTLD directory service that better meets the needs of today's & tomorrow's Internet.

2) Who are the members of the EWG?
The EWG is comprised of 13 volunteers, selected from over 70 applicants to use their diverse experiences, perspectives and expertise to help solve the problem. The group is guided by lead facilitator, Jean-Francois Baril, and includes two liaisons from the ICANN Board. This small diverse group was chosen to participate as individuals while bringing many different perspectives to bear when recommending a better solution for all stakeholders.

3) What is the EWG's objective? How does it differ from the WHOIS RT?
Unlike past efforts to fix WHOIS, the EWG started with a clean slate, questioning fundamental assumptions about the purposes, uses, collection, maintenance and provision of gTLD registration data, as well as accuracy, access, and privacy needs.

4) What did the EWG produce and when?
The EWG published its Final Report in June 2014 for delivery to ICANN's CEO and Board to serve as a foundation for new gTLD consensus policy development, and contractual negotiations, as appropriate.

## Origin and Purpose of the RDS

5) What is the next-generation gTLD Registration Directory Service (RDS)?
The RDS is a proposed successor for today's WHOIS that would collect, validate and disclose gTLD registration data for permissible purposes only, with some data elements accessible only to authenticated requestors that are then held accountable for appropriate use.

6) Why is a next-generation RDS really needed?
The WHOIS system is over 25 years old and has not kept pace with the evolution of the global Internet. After more than 12 years of task forces, working groups, and studies, concerns about WHOIS data access, accuracy and privacy remain unresolved.

7) What makes the RDS fundamentally different from today's WHOIS?
The RDS takes a clean-slate approach, abandoning one-size-fits-all WHOIS in favor of purpose-driven access to validated data in hopes of improving privacy, accuracy and accountability.

8) Why is the RDS so complicated?
The next-generation directory service proposed by the EWG is a complex solution to a very complex problem, as needed to balance privacy, accuracy, and accountability concerns across a

large diverse group of stakeholders and legal regimes, in a manner that scales to meet existing and future needs of the global Internet.

**Registration Data Users and Purposes**

9) Who are the users of the RDS? How did the EWG determine this?
   The EWG analyzed previous reports and use cases to identify users who want access to gTLD registration data, including registrants, protected registrants, on-line service providers, business Internet users, intellectual property owners, law enforcement agencies and OpSec staff, Internet technical staff, individual Internet users, Internet researchers, non-LEA investigators of malicious activity, the general public, and bad actors.

10) Why do those users need access to registration data?
    Use cases also shed light on rationale and purposes served by gTLD registration data, including domain name control, regulatory/contract enforcement, academic/public interest domain name research, domain name purchase/sale, personal data protection, individual Internet use, technical issue resolution, domain name certification, legal action, regulatory and contractual enforcement, criminal investigation and DNS abuse mitigation, DNS transparency, and malicious Internet activities.

11) Which purposes should not be permissible?
    Given no rationale for accommodating the needs of some users but not others that access WHOIS today, the EWG recommended the RDS accommodate **all** non-malicious uses.

12) Why didn't the EWG consider user X or purpose Y?
    Use cases examined by the EWG were not exhaustive, but representative enough of existing and potential uses to establish RDS needs. The EWG also recommended a process for adding new purposes as may be required to address future global Internet needs.

**Registration Data Elements**

13) What registration data should be collected and stored by the RDS?
    The EWG also analyzed use cases to identify data needs. The EWG's final report summarizes existing and potential RDS data elements and queries needed to satisfy permissible purposes.

14) How would TLD-specific data be accommodated?
    To make TLD-specific data accessible through the RDS, each TLD registry may establish their own data collection and disclosure policy for TLD-specific data elements (consistent with over-arching RDS collection/disclosure principles), including validation and mapping to permissible purposes. Registries may also establish TLD-specific principles that build upon RDS options – for example, a brand-specific TLD might mandate collection of certain RDS-optional data elements or require use of the identity validation option.

15) Why is the RDS only concerned with gTLD registration data?
The EWG was tasked with making recommendations to inform gTLD policy-making, but has also examined ccTLD WHOIS to inform RDS principles, many of which are meaningful for any TLD.

16) How would RDS data differ from WHOIS data?
Unlike WHOIS data, RDS data would be validated at the time of collection and periodically by applying standard checks. The RDS may also collect some data elements identified as desired to fully-address identified purposes, but not generally presented through WHOIS today.

17) Would the RDS collect the same registrant data for domains used for commerce?
Some potential new data elements (e.g., Registrant Type, Registrant Company Identifier, Business Contract) have been recommended to more clearly identify domains used by legal person registrants. The EWG considered but did not recommend adding a Domain Name Purpose, given difficulty in defining, collecting, and enforcing meaningful accurate values for such a data element.

18) When and how will risk assessment be performed?
The EWG recommends that risk analysis be performed on the entire RDS prior to implementation. An initial RDS risk survey was conducted in 2Q14 to identify potential risks and benefits as input to risk assessment and to inform the EWG's recommendations.

**Registration Data Collection and Storage**

19) What roles do registrars, registries and the RDS play in data collection and storage?
In the suggested model, registrars continue to collect and maintain data from their customers (registrants), while registries continue to store gTLD data collected from their customers (registrars) as done for "thick WHOIS." In addition, the EWG recommends that a new contracted party be introduced to focus on contact data collection and validation. The core RDS is not involved in data collection, but uses data synchronized from validators and registries to provide uniform access for all gTLD registration data.

20) How would "Contacts" and "Contact IDs" be created?
In the RDS ecosystem, each registrant or designated point of contact submits his or her own contact data (e.g., name, postal and email address, phone number) to a validator of his or her choice. A reusable "Contact" is created to store that validated data, bound to a unique identifier ("Contact ID"). Any future contact data updates are also made through validators, using Contact IDs to retrieve associated contact data.

21) How would contacts be used in domain name registrations?
Registrants still register domain names using registrars as they do today. But in the RDS, each registrant supplies the registrar with his or her own Contact ID, along with Contact IDs for Administrative, Technical, Abuse, Legal, and other relevant contacts. All designated contacts must agree to fulfill the designated role(s) before a domain name can be activated. Whenever the RDS processes a query about a domain name, Contact IDs are used to retrieve any contact data that should be returned, in accordance with gated access.

22) What data would be mandatory to collect/store?
The EWG recommends that only data elements with at least one permissible purpose be collected by the RDS. The EWG's final report categorizes every data element needed for a permissible purpose as mandatory or optional to collect, and public or gated to disclose. In addition, the EWG recommended development of an RDS privacy policy and mechanisms to enable routine compliance with local data protection laws.

23) How long would data be stored by the RDS?
Registration data storage, escrow and access log requirements are addressed in the EWG's final report through a series of principles. However, specific duration requirements must be determined during policy development.

24) Where will data be stored?
In the Synchronized RDS model recommended by the EWG, data synchronized from validators and registries will reside in multiple places in a consistent, coordinated way, using engineering best practices to achieve fault tolerance, high availability, and load balancing, including geographically diverse data centers.

**Purpose-Driven Data Access and Disclosure**

25) What is purpose-driven registration data access?
The RDS introduces *purpose-driven data access*, which provides gated access to data based on a requestor's identity and stated purpose. Only authenticated requestors authorized for a given purpose (and held accountable to terms and conditions) can access data elements needed and authorized for a declared permissible purpose.

26) Does the RDS eliminate free public access to registration data?
No. The EWG recommends that unauthenticated public access to an identified (non-null) minimum data set be made available to promote Internet stability and meet basic DNS needs. This minimum public data would still be accessible by anyone, for any permissible purpose, without requiring authentication. For example, statuses and dates provided by Registrars/Registries to the RDS would remain public, as would the Registrant's email address. However, most personal data supplied by registrants and designated contacts would be gated by default..

27) Who would have gated access to registration data?
The EWG recommends that gated access processes should create a level playing field for all requestors with the same purpose. The EWG issued an RFI to gather information from potential RDS User Accreditors, and used results to inform recommendations included in its final report – for example, identifying alternative implementation models that different RDS user communities may wish to consider when choosing Accrediting Bodies and Accreditation Operators.

28) What would deter abuse of gated access?
The RDS would log and audit public and gated data access to minimize abuse, applying escalated remedies for unauthorized access to data, improper use of data, abuse of access credentials, and terms of use violations. Different terms and conditions would be applied to different purposes, commensurate with risk. If requestors violate terms and conditions, penalties would apply.

29) Would registrars and registries still be able to provide direct access?
To enable authentication, access control, and accountability, all authoritative access to gTLD registration data would occur through the RDS. However, this would not impede other registrar and registry data interactions with their own customers, or prevent these entities or other third parties from providing user interfaces that relay requests to the RDS.

30) Would the RDS provide WhoWas and Reverse query services?
To meet the needs of authenticated RDS user with permissible purposes, the RDS will provide a Reverse Query service that searches public and gated data, and a WhoWas service that returns historical snapshots of public and gated data elements. Third parties may also provide Reverse Query, WhoWas, and other innovative services, subject to terms and conditions of RDS data use.

**Addressing Registration Data Privacy Concerns**

31) Would privacy and proxy services still exist in the RDS? How would they differ?
The EWG recommends there be accreditation for privacy/proxy service providers and rules regarding provision and use of accredited privacy/privacy services. The RDS has been designed to leverage accredited privacy/proxy services to address routine privacy needs, incorporating new data elements to facilitate provider identification, customer contact, and abuse reporting. Principles are included in the EWG's final report, as input to the GNSO PPSAI working group now developing this policy.

32) How would the RDS accommodate the personal data privacy needs of at-risk registrants?
The RDS accommodates needs for anonymity by offering an accredited "secure protected credentials" service for persons at risk, and in instances where free-speech rights may be denied or speakers persecuted. The EWG recommended that ICANN facilitate the establishment of an independent trusted review board to validate claims of at-risk organizations or individuals to approve (and when necessary, revoke) credentials that can be used to register domains names on behalf of these at-risk entities.

33) What would prevent insider abuse or external hacking of RDS data?
The EWG evaluated these concerns when recommending an implementation model and compliance principles for RDS ecosystem players. As with other systems that collect personal data, proper system design, security measures, audits and oversight would be needed to minimize data breach risk. Insider abuse should be deterred through security policy, implementation, enforcement and third-party auditing.

34) How would the RDS comply with local data protection laws?
The EWG recommends that mechanisms be adopted to facilitate routine legally compliant data collection and transfer between actors within the RDS ecosystem. To accomplish this, RDS actors will be held to standard contract clauses that are harmonized with data protection and privacy laws, codified in RDS policy, and implemented through a "rules engine" that applies policy as appropriate for each jurisdiction.

35) Will the RDS require Registrants to publish all of their personal data?
Within the RDS, Registrants would have more control than ever over personal data. To improve both accountability and reachability, validated Registrant, Administrative, Technical, Abuse, and Legal Contacts would be required for all new domain names. However, Registrants would have many ways to be accountable without publishing personal data, including inexpensive/free accredited Privacy Services and new third-party contact options. To deter identity theft, a Contact ID could not be used within a domain name registration without authorization.

36) Do purpose-based contacts (PBCs) require registrants to publish their personal data?
While the RDS would require every registered domain name to be associated with Contact IDs as needed to satisfy permissible purposes, Purpose-Based Contact (PBC) data elements would NOT be publicly available to everyone. The Contact ID for each PBC would be publicly accessible to all, but PBC names and addresses would only be accessible to authenticated requestors, authorized to access RDS data for the specific purpose associated with each Contact.

37) Will requestors that "get through the gate" have access to everything?
No requestor would ever have unfettered access to the entire data set. The RDS does not use a one-size-fits-all "gate." Requestors and their registration data needs vary; so would gated access policies. Like most on-line services that hold private data, the RDS would apply policy-defined permissions, driven by requestor identity and stated purpose, with uniformly-enforced terms of service, backed by more consistent measures to deter and mitigate abuse.

38) How would law enforcement access the RDS?
The EWG recommends that the RDS store data in jurisdiction(s) where law enforcement is globally trusted. In addition, the EWG recommends that a recognized, trusted Law Enforcement organization such as Interpol take responsibility for accrediting its own members for RDS access, leveraging existing systems to authenticate those users, proxying gated access requests for permissible purposes to the RDS, and detecting and dealing with potential access abuses.

**Addressing Registration Data Accuracy Concerns**

39) Why would RDS data be any more accurate than today's WHOIS data?
The EWG proposes more robust validation of registrant data than the 2013 RAA. In addition, with gated access to more sensitive data elements, registrants would have less incentive to supply inaccurate data. Registrants and their designated contacts would have more direct and scalable control over their own data, along with accountability for ensuring data accuracy.

40) How and when would the RDS validate registration data?
The RDS would apply standard validation to all gTLD registration contact data, requiring syntactical and operational validation of all registrant and contact addresses at time of entry, and offering optional identity validation. Periodic revalidation checks would also be used to detect data that later becomes invalid, triggering a defined remediation process. Furthermore, when contact data is updated, changes automatically apply to all domain name registrations that refer to that contact.

41) Wouldn't registrars and registries still have to validate data?
Registrars would still be accountable to provide services to registrants as specified in their contracts, including ensuring provision of current, accurate registration data. However, introducing a conceptually separate contact management system, where registrants and contacts enter their own data using a Validator, makes this more efficient..

42) How would the RDS deal with inaccurate registration data?
The RDS would hold registrants and contacts accountable for providing and maintaining current, accurate and timely data updates. In addition to establishing escalated remedies for inaccurate data, the final report recommends using incentives to encourage accuracy, such as new validation status and timestamp data elements that enable user/browser-visible flagging.

43) What is the unique contract data option and how would it help prevent identity theft?
To improve accuracy and reduce fraud, Contacts could optionally supply a globally-unique name/organization and associated details to be "identity validated". Once identity validated for accuracy and uniqueness, that Contact (and only that Contact) could maintain and associate that data with many domain names, acting as registrant or for any PBC.

44) Who will serve as Validators?
The RDS improves data accuracy in many ways, starting with a new Validator ecosystem for Contacts to maintain their own data. Any entity that meets contractual requirements may offer Validation services for use with the RDS, including Registrars, Registries, and third parties that specialize in address validation.

45) How will data be validated cost-effectively on a global scale?
By separating Contact Validation from Domain Name Registration, difficult validation tasks can be carried out by specialists – many of whom already validate addresses on a global scale today. Registrars and Registries won't be forced to create global validation systems and Registrants can choose local Validators, reducing overall cost. While the RDS requires every Contact used by a registration to be syntactically-validated, operational validation is required only for email, phone, or other data easily-validated at this level. Identity validation would be available as an option for Contacts seeking more protection against fraudulent use of their data.

**Addressing Registration Data Accountability Concerns**

46) Would the RDS offer greater accountability for unauthenticated public data access?
Yes, to some degree. The RDS would log all access to gTLD registration data, including unauthenticated public data access, with restrictions to deter bulk harvesting. The RDS would also limit this publicly accessible data to a minimum set, encouraging RDS users to authenticate themselves to meet broader data needs.

47) How would credentials be issued for gated access?
Gated access would only be available to requestors who applied for and were issued credentials for RDS query authentication. The final report outlines tasks performed by Accrediting Bodies and Accreditation Operators, illustrating possible implementations that might be adopted by different RDS user communities to issue credentials and apply them for RDS access.

48) Who would decide which requestors should have access to which data elements?
The EWG has recommended data and query needs for each identified user/purpose, but purposes needing approved gated data must be further analyzed in consultation with those RDS user communities. Additionally, the EWG recommends that risk analysis be performed on each data element to inform access policy.

49) How would the RDS hold requestors accountable for use of data obtained via gated access?
The RDS would log and audit public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use. Different terms and conditions may be applied to different purposes. If requestors violate terms and conditions, penalties would apply.

50) Who will accredit RDS users?
As specific user communities may have access to gated data for an approved purpose, policies for identifying possible Accreditation Bodies and models appropriate for each community should be examined during the implementation phase.

**Suggested Model and Benefits/Limitations**

51) Why did the EWG suggest a Synchronized RDS model?
The Synchronized RDS (SRDS) model was suggested as one beneficial way of addressing the desired features and principles recommended to satisfy identified users and their data needs. This conclusion was reached only after consideration of several alternative models and detailed comparison and cost analysis of the two most promising models.

52) What are the primary benefits of the SRDS model?
Benefits of this model include “one stop shopping” and reduced confusion for requestors, greater accountability and ability to track/audit data and access across TLDs, ability to apply appropriate data protection measures, ability to support Reverse Query and WhoWas search capabilities more cost-effectively, opportunity to minimize some costs, and opportunity for internationalized web portal.

53) Doesn't the SRDS model elevate risk of abuse and attack?
As a "Big Data" source of highly valuable data, there is clearly potential for attack or abuse if not properly secured, audited and maintained. However, this risk may be no greater than risk posed by a highly distributed model with inconsistent and less easily-audited security measures. In fact, both the SRDS and FRDS models evaluated by the EWG produced similar results when evaluated against their impact on security.

54) What other models did the EWG consider?
In reaching consensus on the SRDS model, the EWG carefully considered a Federated RDS (FRDS) model, as well as Regional, Opt-Out, and Bypass models, all compared against today's WHOIS model and a specified set of criteria.

55) Who will operate the RDS and where will it be located?
The EWG's final report recommends that data be stored in multiple places in a consistent, coordinated way. The EWG also reached conclusions based in part on a cost comparison performed by IBM. However, choosing an operator or location is beyond the EWG's remit. Such decisions would occur after policy development, before implementation.

**Impacts and Costs**

56) What would the RDS cost to build and who would pay for it?
Recognizing that GNSO policy decisions and Staff implementation actions ultimately will determine the cost, the EWG explored this important issue further at a high level to inform these future efforts. As summarized in the EWG's final report, a study performed by IBM was conducted to analyze potential costs of development and operation for the core RDS.

57) Would registrant's costs increase?
The EWG recommends that the RDS operate on a cost-recovery basis, with the goal of minimizing total cost to the entire ecosystem through greater efficiency. The RDS should reduce many of the "hidden costs" that registrants bear today, and there is no intention to increase registrant cost.

58) Would requestor's costs increase?
The EWG acknowledges that some aspects of the proposed model will incur new costs, but believes that many other hidden costs incurred with today's inefficient and too-often-inaccurate WHOIS system will be reduced. As the proposed RDS delivers new and improved services, both benefits and costs must be evaluated. The proposed approach will provide policy-makers the option, for the first time, to craft ways for those requesting registration data from the system to efficiently contribute to the operation of that system.

59) In what ways would the RDS likely reduce cost?
The proposed RDS will reduce cost in many ways, including more scalable and efficient validation and contact management, reduced fraud, improved accuracy, reduction in inaccuracy complaints, reduced personal privacy risk to registrants, improved ability to comply with data protection and privacy laws, efficiencies gained through automation, and faster time-to-

resolution for all requestors using RDS.

60) How would registrar WHOIS obligations be reduced?
Registrars would no longer be obligated to collect or validate WHOIS contact data from registrants. Instead, registrars would collect pre-validated Contact IDs from registrants, forwarding these IDs along with domain name data to the registry. Associated contact data validation, compliance, and data protection burdens would be shifted to validators. Registrar's RDS obligations would be more narrowly focused on DNS-related registration data.

61) How would registry WHOIS obligations be reduced?
Registries would no longer be obligated to receive or disclose WHOIS contact data relayed by registrars. RDS contact data storage and processing obligations would be shifted to validators. In the recommended Synchronized RDS model, obligations associated with port 43 WHOIS access would also be shifted to the RDS. Instead, registries would use a familiar protocol – EPP – to supply timely domain name registration data updates to the RDS.

**Next Steps**

62) What did the EWG do with comments on its draft report and update report?
All input received on the report was used to inform the EWG as it refined its recommendations and finalized its report. Responses to public comments on the draft report are also available on-line.

63) When did the EWG produce its final report?
The EWG published its final report in June 2014, before the London ICANN meeting.

64) What will be done with the EWG's final report?
The EWG's final report was delivered to ICANN's CEO and Board to serve as a foundation for the Board-requested GNSO Policy Development Process (PDP) for the provision of gTLD registration data and contractual negotiations, as appropriate.

65) Will WHOIS go away?
At this juncture, the RDS is a recommended solution, to be considered by the ICANN board, the GNSO, and the community. If the RDS is adopted, a transition plan will be created to address migration from WHOIS to the RDS.

**24 June Additions**

66) How does the RDS make life simpler for individual registrants?
If the RDS replaces WHOIS, Registrants will have more visibility into what their data is used for. They can enter and update their data more easily, have more flexibility and control over what data is public, and have options to deter fraudulent use of their data. Registrants will have one place where they can access their own data to see what RDS users can learn about them. They will have greater assurance that privacy, data protection, security, and auditing policies will be applied, that access to their data will be limited to those with a need to know, and that requestors who access data will be held accountable for proper use.

67) How will members of the press and bloggers gain access to RDS data?
The DNS Transparency purpose was intended to cover media needs for registration data. However, if the data available for that permissible purpose does not prove sufficient, the EWG also recommended an on-going process for users to suggest new permissible purposes.

68) How are third party commercial providers that use WHOIS today accommodated?
Unlike WHOIS today, the entire RDS data set must not be exported in bulk form for uncontrolled access. However, third parties can still offer innovative services by using the RDS's purpose-driven access framework to query, process, and then deliver data to accredited users with permissible purposes, while being held to terms and conditions of RDS use.

69) Why is Legal Contact mandatory? Is it publicly available, outside the gate?
A Legal contact is collected for every domain name to handle communication involving legal actions and regulatory/contractual issues raised about that domain name. The Legal Contact's ID (i.e., numeric handle) is publicly available. However, the Legal Contact's name and address are only available to authenticated users authorized for these permissible purposes.

70) Why is Business Contact mandatory? Is it publicly available outside the gate?
A Business Contact is collected only from Registrants that self-declare as Legal Persons. A Business Contact is intended to help efficiently direct consumer requests for information about a business or consumer contact with businesses. It is a recommended way that businesses may choose to make additional data about themselves readily-available to Individual Internet Users. The Business Contact's ID (i.e., numeric handle) is publicly available, but contact data is only available to authenticated users authorized for these permissible purposes.