WHOIS Access and the EU General Data Protection Regulation

Part 2

ICANN | IPC
Intellectual Property Constituency

ICANN | BC
Business Constituency

Panelists

Brian Winterfeldt – Winterfeldt IP Group – IPC President (Co-Moderator)

Steve DelBianco – NetChoice – BC Vice Chair for Policy (Co-Moderator)

Cathrin Bauer-Bulst – European Commission

Christian D'Cunha – European Data Protection Supervisor

Paolo Grassia – European Telecommunications Network Operators' Association

Claudia Selli – AT&T – BC Chair

Lori Schulman – INTA – IPC Member

Tim Chen – DomainTools – BC Member

Susan Kawaguchi – CNA Consulting – GNSO Councilor for the BC

Alex Deacon – MPAA – IPC Member

Akram Atallah – ICANN – President of Global Domains Division

John Jeffrey – ICANN – General Counsel

Agenda

9:00 – 9:15 am	Introduction
9:15 – 9:30 am	Overview of ICANN Convergence Model
9:30 – 9:45 am	Latest Updates on EU Level Discussions
9:45 – 10:15 am	WHOIS User Perspective on ICANN Convergence Model
10:15– 10:45 am	Designing a Certification/Accreditation System
11 am – 11:45 am	Discussion of the ICANN Convergence Model
11:45 am – 12 pm	Next Steps

Introduction

- What is the GDPR?
- What is WHOIS?
- How does GDPR relate to WHOIS?
- What is ICANN doing to comply with GDPR?

Overview of ICANN Convergence Model

Category	**ICANN Convergence Model Element**
Data Collection	Continue to mandate that registrars collect all “thick” registration data. “Thick” data includes registrant, administrative and technical contact information.
Data Sharing	Continue to mandate that registrars provide all collected thick data to registry operators and data escrow providers.
Data Retention	Life of the registration plus two years.

Overview of ICANN Convergence Model

Category	ICANN Convergence Model Element
Territoriality Scope	Model must be applied to all contracted parties and registrants within the European Economic Area (EEA). It may also be applied globally by individual registrars and registries, but only subject to a “controller agreement” that specifies additional implementation parameters.
Natural vs. Legal Person Scope	No distinction between data of natural persons and legal persons.

Overview of ICANN Convergence Model

Category	**ICANN Convergence Model Element**
Public WHOIS	1. Registrant Organization 2. Registrant State/Province 3. Registrant Country
Non-Public WHOIS	1. Registrant Name 2. Registrant Street Address 3. Registrant City 4. Registrant Postal Code 5. Registrant Email 6. Registrant Phone Number 7. Administrative / Technical Contacts Option for registrant to publish additional data through opt-in mechanism

Overview of ICANN Convergence Model

Category	ICANN Convergence Model Element
Credentialed or Accredited Access to Non-Public Data	No need for self-certification to access non-public data if the public data fields are sufficient for most legitimate purposes. Otherwise, an accreditation program is necessary to facilitate access to non-public data for legitimate purposes. ICANN would like the Governmental Advisory Committee (GAC) to coordinate its members to prepare country-by-country lists of authorized law enforcement agencies, to use as the basis for accredited law enforcement access to non-public WHOIS data. ICANN would also like the GAC to prepare a Code of Conduct for law enforcement access to WHOIS data. ICANN is also exploring other accreditation mechanisms for non-law enforcement access to non-public WHOIS data, including for intellectual property enforcement and cybersecurity, but details remain scant.

Overview of ICANN Convergence Model

- Key model elements not addressed:
  - Data Accuracy
  - Bulk or Aggregated Data Access

Latest Updates on EU Level Discussions

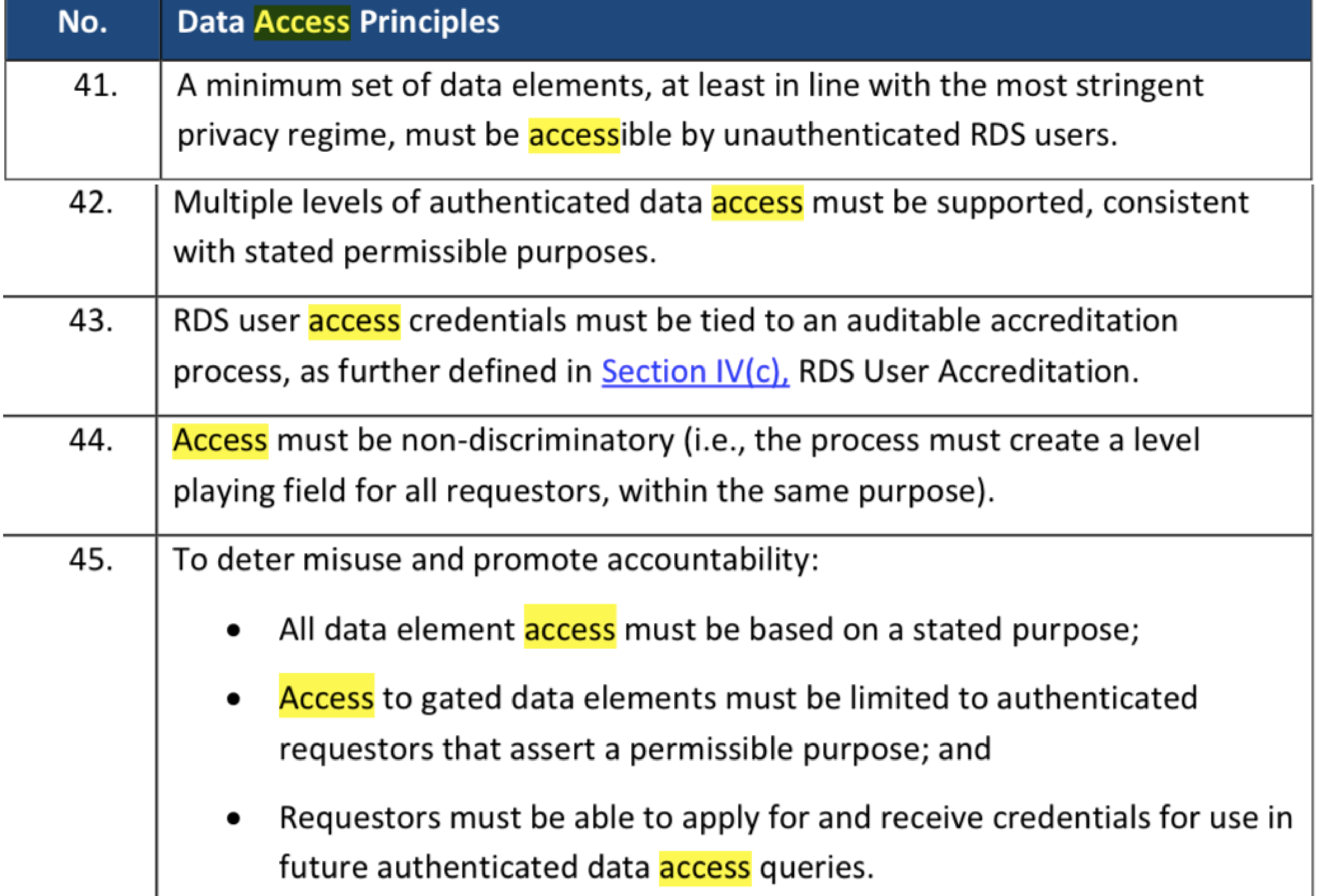
- European Commission
- European Data Protection Supervisor
- European Telecommunication Network Operators’ Association
- Other discussions with European data protection authorities and other EU parties

WHOIS User Perspective on ICANN Convergence Model

- Business Use Cases
- Consumer Protection and Intellectual Property Use Cases
- Cybersecurity and Platform Operator Use Cases
- Other key WHOIS users and needs

Designing an Accreditation System for Non-Public Data Access

- Existing concepts for accreditation
  - Self-Certification
  - Self-Certification Plus
  - Purpose/User-Based Credentialing
  - EWG Accreditation Model
- Other certification or accreditation system ideas and challenges



No.	Data Access Principles
41.	A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated RDS users.
42.	Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.
43.	RDS user access credentials must be tied to an auditable accreditation process, as further defined in Section IV(c), RDS User Accreditation.
44.	Access must be non-discriminatory (i.e., the process must create a level playing field for all requestors, within the same purpose).
45.	To deter misuse and promote accountability: • All data element access must be based on a stated purpose; • Access to gated data elements must be limited to authenticated requestors that assert a permissible purpose; and • Requestors must be able to apply for and receive credentials for use in future authenticated data access queries.

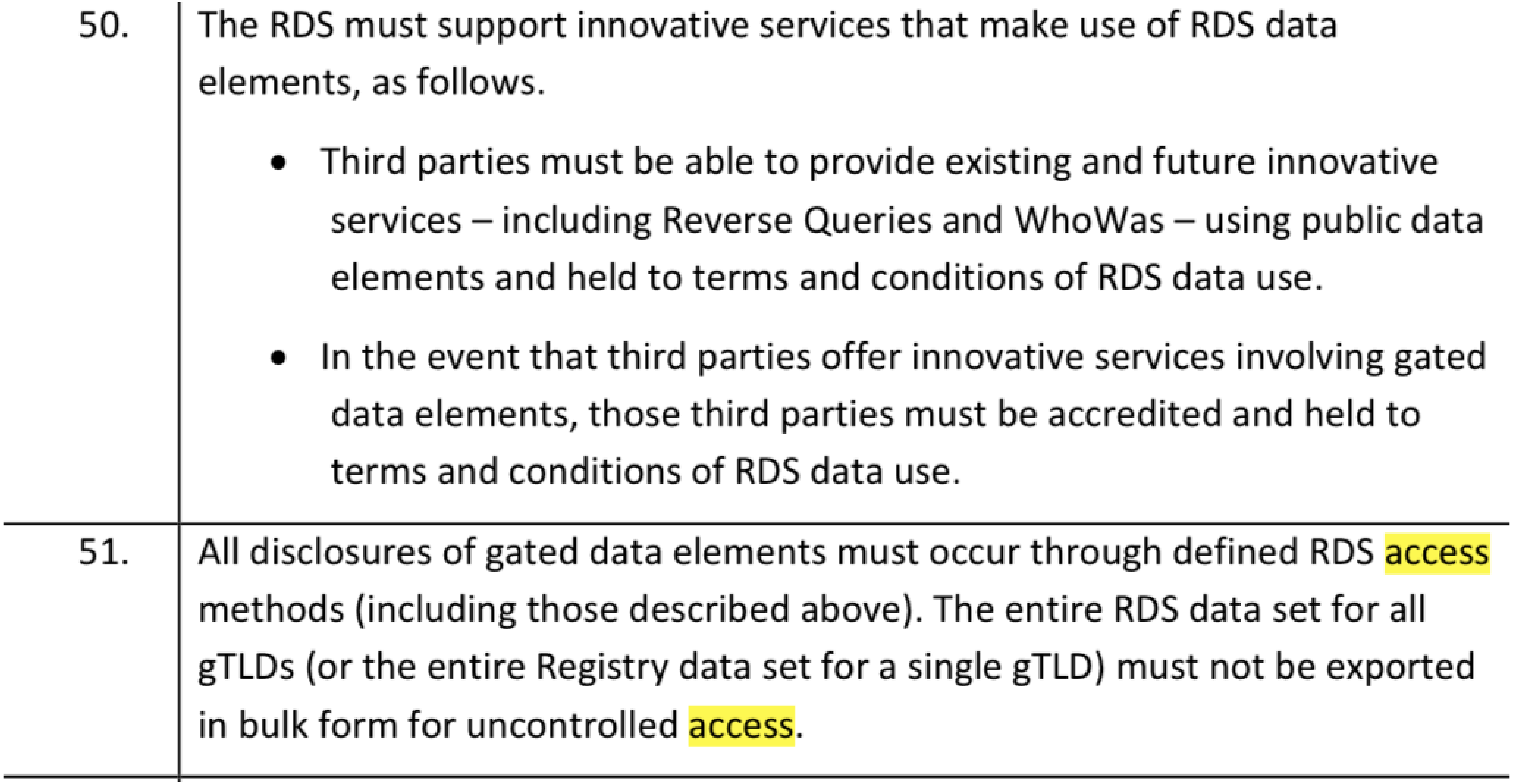
46. Some type of accreditation must be applied to requestors of gated access:

- When accredited Requestors query data, their purpose must be stated every time a request is made.
- Different terms and conditions may be applied to different purposes.
- If accredited requestors violate terms and conditions, penalties must apply.

47. To raise the standard of gTLD registration data protection, all RDS queries/responses must make use of commonly-available message encryption and authentication measures to protect the confidentiality and integrity of data in transit.

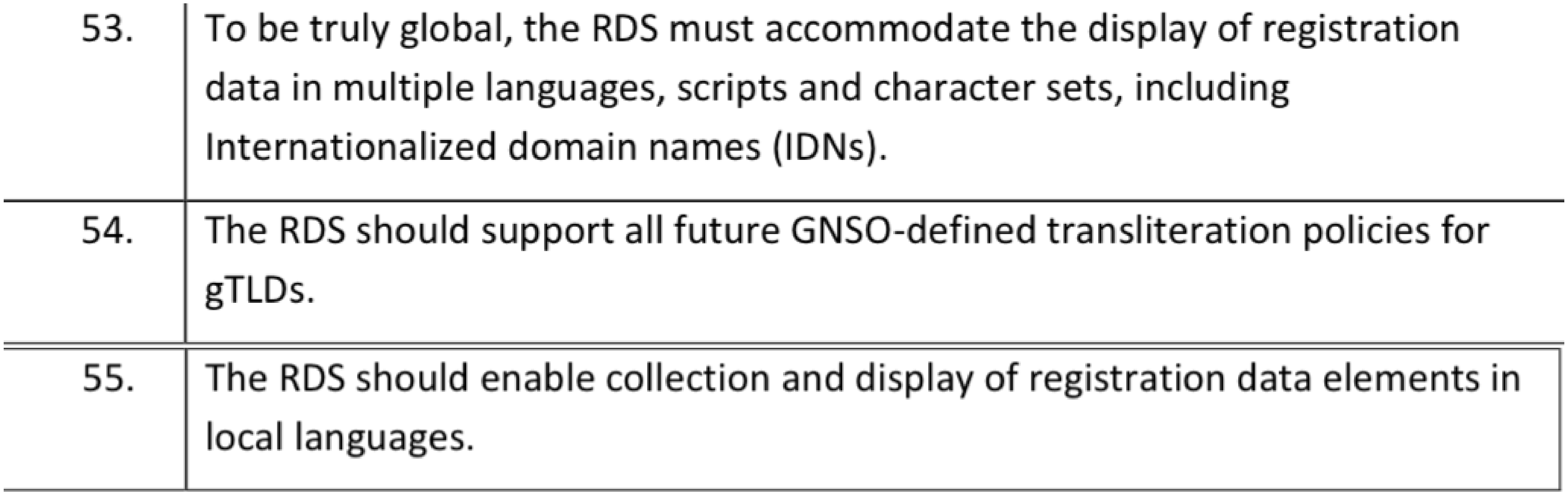
48. To meet the needs of authenticated RDS users with permissible purposes, the RDS must provide a Reverse Query service that searches public and gated data elements for a specified value and returns a list of all domain names that reference that value.

47.	To raise the standard of gTLD registration data protection, all RDS queries/responses must make use of commonly-available message encryption and authentication measures to protect the confidentiality and integrity of data in transit.
48.	To meet the needs of authenticated RDS users with permissible purposes, the RDS must provide a Reverse Query service that searches public and gated data elements for a specified value and returns a list of all domain names that reference that value.
49.	To meet the needs of authenticated RDS users with permissible purposes, the RDS must provide a WhoWas service that returns historical snapshots of public and gated data elements for specified domain names, limited to the historical data available to the RDS.



50.	The RDS must support innovative services that make use of RDS data elements, as follows. • Third parties must be able to provide existing and future innovative services – including Reverse Queries and WhoWas – using public data elements and held to terms and conditions of RDS data use. • In the event that third parties offer innovative services involving gated data elements, those third parties must be accredited and held to terms and conditions of RDS data use.
51.	All disclosures of gated data elements must occur through defined RDS access methods (including those described above). The entire RDS data set for all gTLDs (or the entire Registry data set for a single gTLD) must not be exported in bulk form for uncontrolled access.

52.	Disclosures may occur through interactive display and other RDS access methods. • To make data easier to find and access in a consistent manner, a central point of access (e.g., web portal) must be offered. • Secure access to public data must be available to all requestors through an unauthenticated query method (at minimum, via secure website). • Secure access to gated data must be supported through secure web and other access methods and formats (e.g., RDAP xml responses, SMS, email), based on authenticated requestor and purpose. • Requestors must be able to obtain authoritative data from the RDS in real-time when needed. • The RDS must accommodate automation for large-scale lookups for various use cases and permissible purposes.



53.	To be truly global, the RDS must accommodate the display of registration data in multiple languages, scripts and character sets, including Internationalized domain names (IDNs).
54.	The RDS should support all future GNSO-defined transliteration policies for gTLDs.
55.	The RDS should enable collection and display of registration data elements in local languages.

Requirements for self-certification:

1. Name of Requestor
2. If Requestor is not an individual, name of individual completing self-certification on behalf of Requestor
3. Physical Address of Requestor
4. E-mail Address of Requestor
5. Phone number of Requestor
6. Purpose of Request (note: could be tick-box to select one of the 5 purposes set forth for ICANN proposed interim models)
7. Agreement, under penalty of perjury, to all of the following conditions (tick-box: yes/no):
   - a) Is the requested data necessary to further the purpose set forth in item 6?
   - b) Will the data requested be used for the potential establishment, exercise or defense of legal claims?
   - c) Requestor will process data received in accordance with the purpose for which access is sought as indicated in (6.), above.
   - d) Requestor will take all reasonable steps to protect against unauthorized access to, use of, or disclosure of received data.
   - e) Requestor will comply with the GDPR and other applicable laws with respect to the received data.
   - f) Requestor will not use received data to:
     - i. allow, enable or otherwise support any marketing activities to entities other than the user's existing customers, regardless of the medium used (such media include but are not limited to transmission by e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts of mass unsolicited, commercial advertising or solicitations to entities),
     - ii. enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar, or
     - iii. interrupt, disrupt or interfere in the normal business operations of any registrant, with the understanding that investigations into potential illegal or abusive activity of a registrant and efforts to stop such alleged illegal or abusive behavior through criminal or civil legal action or communication directly with registrant, registrar, Registry Operator or any other intermediary concerning such alleged illegal or abusive activity shall not be considered an interruption, disruption or interference in normal business operations of any registrant.

Discussion of the ICANN Convergence Model

- Akram Atallah – ICANN President of Global Domains Division
- John Jeffrey – ICANN General Counsel

Next Steps

- Review and providing input on remaining concerns with the ICANN Convergence Model
- Develop ideas for interim certification/credentialing/accreditation system for access to non-public data
- Prepare questions for ICANN to present to DPAs for specific feedback
- Continue cross-community dialogue to bridge divides on model elements and contracted party and WHOIS user needs

Thank You!

ICANN | IPC

Intellectual Property Constituency

ICANN | BC

Business Constituency