RDS Data Elements – Inputs & Summaries – drafted by gnso-rds-pdp-data@icann.org

Question, as stated in the Charter:

Data Elements: What data should be collected, stored, and disclosed?

Executive Summary of inputs relevant to this Question:

[A single paragraph highlighting the most helpful inputs that this small team found and summarized in its effort to educate the full WG to finalize its work plan and prepare to analyze this specific Question. Further description of each Question is available in this mind map and the WG charter.]

Input Documents that the WG should at minimum consider when addressing this Question:

Input Documents (hyperlinked to source)	Identified by	Summarized by / Link to
WHOIS Task Force Final Report (2003)	Issue Report	Dinculescu
WHOIS Task Force Final Report (2007)	Issue Report	Dinculescu
2013 RAA's Data Retention Specification Discussion Document (2014)	Phifer	Mounier
SAC058, Report on Domain Name Registration Data Validation (2013)	Galvin	Mounier
SAC055, WHOIS: Blind Men and an Elephant (September 2012)	Issue Report	Mounier
SAC054, Report on Domain Name Registration Data Model (June 2012)	Issue Report	Raiche
Registrar Accreditation Agreement (2013), especially RAA WHOIS requirements for Registrants (2013)	Charter	Mounier
New gTLD Registry Agreement (2014), especially Specificiation 4 Registration Data Publication Services	Pruis	Pruis
WHOIS Registrant Identification Study (2013)	Charter	Mounier
Article 29 WP statement on the data protection impact of the ICANN RAA (2013-2014) - https://www.icann.org/en/system/files/correspondence/namazi-to-kohnstamm-25mar14-en.pdf - https://www.icann.org/en/system/files/correspondence/kohnstamm-to-jeffrey-08jan14-en.pdf - https://www.icann.org/en/system/files/correspondence/jeffrey-to-kohnstamm-20sep13-- en.pdf https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf	Issue Report	Bockey
Article 29 WP comments on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS (2012) - https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-atallah-26sep12-en.pdf - https://www.icann.org/en/news/correspondence/chehade-to-kohnstamm-09oct12-en	Issue Report	Bockey Also Ali (p5)
Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2007) - http://gnso.icann.org/en/correspondence/cerf-to-schaar-24oct07.pdf - https://www.icann.org/en/system/files/files/cerf-to-schaar-15mar07-en.pdf - https://www.icann.org/en/correspondence/schaar-to-cerf-12mar07.pdf	Issue Report	Bockey
Article 29 WP on ICANN's WHOIS Database Policy (2006) - https://www.icann.org/en/system/files/files/schaar-to-cerf-22jun06-en.pdf	Issue Report	Bockey

Input Documents (hyperlinked to source)	Identified by	Summarized by / Link to
- https://www.icann.org/en/correspondence/lawson-to-cerf-22jun06.pdf - https://www.icann.org/en/correspondence/parisse-to-icann-22jun06.pdf - https://www.icann.org/en/system/files/files/fingleton-to-cerf-20jun06-en.pdf		
Article 29 WP Opinion on the application of the data protection principles to WHOIS directories Article 29 WP 76 Opinion 2/2003	Issue Report	Bockey
Additional Article 29 WP documents that may be of interest to this PDP WG		
- Article 29 WP 5 Recommendation 2/97	Perrin	Padilla
- Article 29 WP 33 Opinion 5/2000	Perrin	Padilla
- Article 29 WP 41 Opinion 4/2001	Perrin	Padilla
- Article 29 WP 56 Working Document 5/2002	Perrin	Padilla
- Article 29 WP 217 Opinion 4/2014	Kimpian	Padilla
- Article 29 WP 20 Opinion 3/1999	Ali	Ali
Council of Europe Declaration Declaration of the Committee of Ministers on ICANN, human rights and the rule of law (3 June 2015)	Kimpian	Deacon (p1)
European Parliament - News: Data protection reform – Parliament approves new rules fit for the digital era (April 2016) - Draft Directive of the European Parliament (April 2016)	Samuelson Samuelson	Padilla
EDPS Correspondence regarding Registration Data		
- Opinion of the European Data Protection Supervisor: Europe's role in shaping the future of Internet Governance (23 June 2014)	Perrin	Padilla
- ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and - Legitimate Purposes for Collection and Retention (17 April 2014)	Kimpian	Padilla
International Working Group on Data Protection in Telecommunications and Media Documents		
- Common Position relating to Reverse Directories (Hong Kong, 15.04.1998)	Perrin	Ali (p4)
- Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet (Crete, 4./5.05.2000)	Perrin	Ali (p3)
- Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet (Crete, 4./5.05.2000)	Perrin	Ali
- Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000)	Perrin	Ali (p2)
- Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe (Berlin,	Perrin	Ali (p1)

Input Documents (hyperlinked to source)	Identified by	Summarized by / Link to
13/14.09.2000)		
RFC 7485 Inventory and Analysis of WHOIS Data (including past WG email)	Hollenbeck	Coupet
EWG Recommendations for a Next-Generation RDS, especially - Section 4a, Data Element Principles - Annex D, Purposes and Data Needs	Charter	Dinculescu
EWG Tutorial Pages 10-14, 45-60 and EWG FAQs 13-24	Issue Report	Dinculescu
Video FAQ "What is the RDS minimum public data set?"	Issue Report	Dinculescu
Statements/Blogs by Perrin	Issue Report	Deacon (p2)
Process Framework for a PDP on Next-Generation RDS, especially Page 9, Row 4	Charter	Deacon (p3)
ICANN Internationalized Registration Data (IRD) Working Group Final Report	Elsadr	Elsadr
Expert Working Group on Internationalized Registration Data (IRD) Final Report	Elsadr	Elsadr
GNSO Translation and Transliteration of Contact Information PDP Working Group Final Report	Elsadr	Elsadr

Summaries of Key Input Documents:

TABLE OF CONTENTS FOR SUMMARIES SECTION

1. Title: WHOIS Task Force Final Report (2003)

Summarized by: Dinculescu

Section I Paragraph A and B make reference to the WHOIS Data Reminder Policy and the need for Registrars to remind the Registrant to update their WHOIS information if it is incorrect. This ties into the new 2013 RAA Section 3.3.1, requiring at minimum the following data elements:

- Domain name
- Primary and secondary nameservers
- Registrar's Identify
- Original domain name creation date
- Expiration data of the domain name
- Name and postal address of the Registrant
- Name, postal address, email address, voice telephone number and fax number (if applicable) for the Technical Contact
- Name, postal address, email address, voice telephone number and fax number (if applicable) for the Technical Contact

Sections II, III and IV make reference to the WHOIS Data Reminder Policy, WHOIS Accuracy and Bulk Access, specifically recommending the processes for review of WHOIS data, addressing inaccuracies with the Registrants, and how to access bulk WHOIS information. There is no reference to any specific data element but rather makes mention of the holistic "WHOIS Data".

In the comments to the report, the following data elements were addressed:

- "Telephone number" should be kept secret
- "Telephone number" and "postal address" may not be the optimal way to contact a registrant, therefore is there a need to store the data and keep it accurate
- "Telephone number", "email" and "postal address" are a maintained as the primary way to reach registrants
- A Registrant must have the option to "choose for his/her own name and email address not to be disclosed to anyone but law enforcement".

2. Title: WHOIS Task Force Final Report (2007)

Summarized by: Dinculescu

The document has 2 overarching themes:

- Propose an "Operational Point of Contact" (OPoC) which would replace the use of the Administrative and Technical Contact listing on the WHOIS
- Address privacy and WHOIS data disclosure

From the table in Section 7.1.1, the OPoC would remove the need for the Registrant to list their mailing information, and rather that all inquiries be forwarded to the OPoC or the Administrative or Technical Contacts if the registrant still chooses to provide these contacts. Furthermore, Section 4 Subsection 4

proposes what data the registrars must publish in their WHOIS taking into account that the Administrative and Technical Contacts will be replaced by the OPoC, as follows:

- The name of the Registered Name Holder
- The country and state/province of the Registered Name Holder
- The contact information of the primary OPoC, including:
  - contact name of the OPoC
  - contact address of the OPoc
  - contact telephone number of the OPoC
  - contact email address of the OPoC
- The initial registration date of the domain name
- The expiration date of the domain name
- The following registry level data:
  - the domain name
  - identify of the sponsoring registrar
  - URI of the authoritative nameservers
  - all authoritative nameservers
  - status of the domain name

The proposal requires that registrants must provide at least 1 OPoC, with registrars allowing registrants to provide additional OPoCs. If more than 1 OPoC is provided, the data for those OPoCs must be listed on the WHOIS.

gTLD Registries will publish a limited set of data for each domain name, and will not provide any additional data beyond this set. This data is:

- The domain name
- Identity of the Sponsoring Registrar, namely:
  - Registrar Name
  - Corresponding IANA Registrar Identification number
- URI of the authoritative nameservers
- All authoritative nameserver hostnames and corresponding IP Addresses associated with the domain name record
- Status of the domain name
- Initial registration date of the domain name
- Expiration date of the domain name

Section 5 Subsection “Background Information” looks at “special circumstances” where privacy is important in order to protect the Registrant information being disclosed on the WHOIS. In the case of “special circumstances”, the .NL WHOIS model is proposed, where only the following information will be made public if a “special circumstance” request is approved:

- The domain name
- The name of the Registered Name Holder
- The address of the Registered Name Holder
- The name, telephone number and email address of the Administrative Contact

- The name, telephone number and email address of the Technical Contact
- Technical details

"Technical details" is not defined, but it can be safely assumed that they reference the "Registry Level Data" as mentioned above.

In Table 7.1.4 there is a recommendation to include a "Legal Contact" when the contact details of the Registered Name Holder are not available. The response to the recommendation looks at potentially including a third-party listing to accept service of legal process on behalf of the registrant. No further data elements are provided regarding this contact.

Section 7.2.4 provides a methodology to distinguish between commercial and non-commercial registrants. Through this process, a registrant would declare if they are commercial or con-commercial at registration of the domain name. Based on this it is proposed that non-commercial registrants do not have their "postal address" disclosed, as well not disclose their Administrative Contact's:

- Postal address
- Email address
- Voice telephone number
- Fax number (if applicable)

The response to the aforementioned methodology identifies that it is highly susceptible to abuse.

Section 7.2.5 is a comment from the Dutch Post and Telecommunications Authority, outlining that they would only need the following WHOIS data (and that it must be accurate):

- Name, address, phone number, etc… of the Registered Name Holder ("etc…" is not defined)
- Name, address, phone number of the hosting company or website involved ("etc…" is not defined)
- IP addresses
- Registrar information

Section 10.2, Public access to Data looks to determine what data should be available for public access in the context of the purpose of WHOIS, and how to access data that is not available for public WHOIS. The section takes the data elements from sections 4 and separates request for data into 2 categories. The first category would disclose limited WHOIS information, while the second category will disclose all WHOIS information. There is no actual specification of data elements regarding either category.

3. Title: 2013 RAA's Data Retention Specification Discussion Document (2014)

Summarized by: Mounier

Summary

This document lists and describes all data elements that can be collected by the registrars in accordance with the 2013 RAA and it provides reasons / legitimate purposes for that collection and retention.
I grouped the data elements per types of reasons

1) Standard data elements:

- First and last name of the registrant; Title of registrant's administrative contact, Technical contact and billing contact, Postal address, Email address, Telephone number.
- Types of domain name services purchased.
- Data required to process recurring payments or any information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction.
- Reasons for collection:
- Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing; Billing disputes; Chargebacks.

2) WHOIS information :

- Data Enabling Registrar to populate and make available to the public community the WHOIS register both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP)
- Reasons for collection:
- Abuse mitigation, Facilitating domain name purchases and sales

3) Records of communications with the registrant regarding the registration:

- Information regarding website visits and stored in log files
- Log files including communication sources, IP, ISP, behaviour on the website, method of transmission, source IP address, HTTP header, email, Skype handle associated with communication ;
- log files including dates, times and time zones of communications and sessions, including the initial registration. Registrars and registry operators utilise Extensible Provisioning Protocol (EPP) to track, manage and reconcile the status of domain name registrations. Log files of EPP records indicates when a registration is first made, when it is transferred or deleted, modified etc. Assign unique authorisation codes to event s as a security measures to prevent unauthorised transfer, deletion or author abuse.

Reasons for collection:

- Fraud prevention
- Billing disputes
- Resolution of disputes between Registrar and Registry Operator or between two Registrars or between Registrar and Registrant regarding the status of a Registration, e.g., Registrant says it never authorized the transfer of a domain name from one Registrar to another Registrar; log files maintained by Registrar could show when and from what source a request for transfer was made.
- But also for commercial purposes (examination of consumer behaviour).

4. Title: SAC058, Report on Domain Name Registration Data Validation (2013)

Summarized by: Mounier

This is a report on the issue of domain name registration data quality. The report examines whether it is feasible and suitable to improve registration data accuracy through validation. The report explores the suitability and efficacy of various techniques of validating registration data elements in light of the taxonomy.

The report first summarises: 1) the reasons why accurate registration data is important (technical and legal rationale); 2) the reasons for registration data inaccuracy (anti-abuse considerations, privacy considerations, intentional deception, no corroboration of submitted data i.e. minimalist approach to validation, user error, user expectation mismatch).

The report then proposes a validation taxonomy with 3 types of validation for elements of the registration data (syntactic validation, operational validation, Identify validation).

The report considers the feasibility of validation of four types of contact information elements: name, postal address, email address, and telephone and fax number.

Amongst the recommendations made by SSAC there is one relevant to the sub-group on data: The SSAC recommends a discussion on what data elements need to be added or validated to comply with requirements or expectations of different stakeholders.

Conclusion:
Again, as noted by Holly in a previous email, SAC 058 report is about just validation of domain name registration data and does not go into details about data elements.

5. Title: SAC055, WHOIS: Blind Men and an Elephant (September 2012)

Summarized by: Mounier

- This is a Comment to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning the final report of the WHOIS Policy Review Team submitted to the ICANN Board on 11 May 2012.
- The SSAC believes that the foundational problem facing all "WHOIS" discussions is understanding the purpose of domain name registration data. The SSAC believes that there is a critical need for a policy should address the operational concerns of the parties who collect, maintain or use this data as it relates to ICANN's remit.
- The SSAC reviews the needs of 4 distinct communities to access details about a domain name registration: 1) the public Internet, 2) law enforcement, 3) intellectual property owners, 4) security practitioners. In all 4 cases the SSAC argues that there is a legitimate purpose to access registration data.
- The SSAC recommends establishing a Domain Name Policy Committee which would 1) support the development of a uniform policy for registration data, access protocol, and directory

services, 2) develop clear targets for compliance with respect to registration data accuracy, 3) define "accurate registration data" and provide guidance as to how to achieve it.

Conclusion:
As noted by Holly, this is an interesting background document which summarises well the 2012 final report of the WHOIS Policy Review and makes relevant recommendations but there is no specific emphasis on data elements.

6. Title: SAC054, Report on Domain Name Registration Data Model (June 2012)

Summarized by: Raiche

The important report for this WG's purposes is SAC054 - Report on The Domain Name Registration Data. The report breaks the data held into three areas:

Contact Data Set, including contact information necessary for the registration, administration and technical management - saying that includes the registrant's name, postal address, email address, voice telephone number (and fax!) The discussion points to contact information for the registrant, a billing contact, as well as technical and administrative contact information for ICANN. (I assume that refers to the information required under the 2013 RAA)

Operational Data set, including the domain name registrar ID, the creation, and expiry dats and status, name server information and, if the domain is signed, the DNSSEC information

Update Data Information is the information needed for a transfer including the code for transferring the name.

What is REALLY use for the data set is Part 4 of SAC 054 - all the data required is in tables - with what data is provided in each.

Table 1 is the data model for contact information
Table 2 is the Registrar Data Model
Table 3 is the Host Name Data Model
Table 4 is the Domain Name Data Model
Table 5 is the Registered Mark Information Data Model
Table 6 is the DNSSEC information data mode.

I won't reproduce the information in each table, but that should be a very comprehensive list of all the data. Maybe the next job is to look again at the requirements for information under the RAA - clause 3.1.1 - and see what is listed in SAC054 that is additional to that (I suspect Clause 3.1.1 is only about contact information.)

Additional point from Jim Galvin: [SAC054 also] recognizes that there will be registries with special requirements. Thus, like EPP, we tried to make the data model extensible. In line with that is the idea that new data elements should look for a category to be part of so they can inherit properties if possible.

[Below appears] the text of an email Andrew Sullivan sent to the WG - a good summary of the information. Taken from email to the WG from Andrew Sullivan on 21 March

Every domain on the Internet must have name servers in order to function. The RDS ought to contain those name servers so that, in the event of technical problems, other operators can detect whether there is a gap between what the registry contains and what the authoritative servers contain.

- Many domans are signed, and in a signed domain that delegates the delegation will have a DS record. The RDS ought to contain the DS record for the same reason the RDS ought to contain the name servers. In signed domains today, this may be even more important than the NS records, given the frequency of DNSSEC misconfiguration (but I expect this issue to decline over time).

- Every name server has someone responsible for its operation. The RDS ought to contain contact information for a given domain or the name server or (preferably) both, so that in the event of serious malfunction such that interoperation is impossible there is some mechanism for out-of-band contact in order to rectify the problem.

- In shared registration systems, it is usually (always?) the case that registrations are not single-occasion, but instead are registration at a point in time for some term. It is therefore necessary, for troubleshooting interoperation, to know when a name's registration is expiring and also when it was last updated (to troubleshoot recent problems that might be related to changes).

- In any registry using EPP, every domain has an authInfo associated with it in order to help authorize transfer requests. This data must be collected by the registry (it's part of the protocol. Please don't tell me we're going to investigate whether EPP is the correct protocol. It's the one we have).

- In gTLDs, most (all? I know there have been exceptions in the past, because I made the entries in the relevant database) registrations are registered through a registrar. There are two reasons to be able to learn the registrar of a name. It is necessary for other Internet parties to be able to learn the registrar in order to deal with registration problems and other operational problems where the name server contact was inadequate. It is necessary for other registrars to be able to learn the existing registrar in order to facilitate registrant-demanded transfers. (This second reason of course doesn't require the appearance in the RDS, but we are talking about why registration data needs to be collected in the first place.)

- Every registration is a registration by someone. Some registrations are the source of abuse against other networks, and it is sometimes necessary to be able to learn the real information about such a registrant in order to stop such abuse. Note that this is not an argument that such data need automatically be available anonymously through an RDS; just that it be collected.

- In gTLDs, most (all? I know there have been exceptions in the past, because I made the entries in the relevant database) registrations include some cost that accrues to the registrant in exchange for the registration. The identities of the parties responsible for keeping the data up to date and for paying the registration are required in order to ensure continued operation by the same party at the time of expiry of a registration term. This ensures the utility of a domain name, by making it a useful name for a particular network over time (imagine the operational

confusion if, when sending email to someone, you first had to figure out whether they were at the same domain name as yesterday). Note that this is not an argument that such data need automatically be available anonymously through an RDS; just that it be collected at least by the registrar.

7. **Title:** Registrar Accreditation Agreement (2013)

Summarized by: Mounier

Sections relevant to the work of the NGRDS - Sub-group on data:

Under registrar obligations (section 3):

3.2 Submission of Registered Name Holder Data to Registry. During the Term of this Agreement:

3.2.1 As part of its registration of Registered Names in a gTLD, Registrar shall submit to, or shall place in the Registry Database operated by, the Registry Operator for the gTLD **the following data elements**:
3.2.1.1 The **name of the Registered Name** being registered;
3.2.1.2 The **IP addresses** of the primary nameserver and secondary nameserver(s) for the Registered Name;
3.2.1.3 The **corresponding names of those nameservers**;
3.2.1.4 Unless automatically generated by the registry system, the **identity of the Registrar;**
3.2.1.5 Unless automatically generated by the registry system, the **expiration date of the registration;** and
3.2.1.6 **Any other data the Registry Operator requires** be submitted to it.

The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede Subsections 3.2.1.1 through 3.2.1.6 stated above for all purposes under this Agreement but only with respect to that particular gTLD. When seeking approval for alternative required data elements, the data elements set forth in Subsections 3.

Annex - WHOIS Accuracy program specification

Registrars are requested to:

- validate the format of: email addresses, phone number, postal address.
- verify: email address and the phone number of the registered name holder.

Annex - Registration Data Directory Service (WHOIS) Specification

1.4 Domain name Data:
1.4.2. response format: The format of responses shall contain all the elements.
Domain Name: EXAMPLE.TLD
Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example-registrar.tld
Registrar URL: http://www.example-registrar.tld

Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email@registrar.tld
Registrar Abuse Contact Phone: +1.1235551234
Reseller: EXAMPLE RESELLER1
Domain Status: clientDeleteProhibited2
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Registry Registrant ID: 5372808-ERL3
Registrant Name: EXAMPLE REGISTRANT4
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP5
Registrant Postal Code: A1A1A16
Registrant Country: AA
Registrant Phone: +1.5555551212
Registrant Phone Ext: 12347
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE

Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: AA
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext: 1234
Admin Email: EMAIL@EXAMPLE.TLD

Registry Tech ID: 5372811-ERL9
Tech Name: EXAMPLE REGISTRANT TECHNICAL
Tech Organization: EXAMPLE REGISTRANT LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: AA
Tech Phone: +1.1235551234
Tech Phone Ext: 1234

Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMP

Annex - Data retention specification

1.1 Registrar shall collect the following information from registrants at the time of registration of a domain name (a "Registration") and shall maintain that information for the duration of Registrar's sponsorship of the Registration and for a period of two additional years thereafter:

1.1.1. **First and last name or full legal name of registrant**;
1.1.2. **First and last name or, i**n the event registrant is a legal person, t**he title of the registrant's administrative contact**, technical contact, and billing contact;
1.1.3. **Postal address of registrant**, administrative contact, technical contact, and billing contact;
1.1.4. **Email address of registrant**, administrative contact, technical contact, and billing contact;
1.1.5. **Telephone contact for registrant**, administrative contact, technical contact, and billing contact;
1.1.6. **WHOIS information**, as set forth in the WHOIS Specification;
1.1.7. **Types of domain name services** purchased for use in connection with the Registration; and
1.1.8. To the extent collected by Registrar, "**card on file**," current period third party transaction number, or other recurring payment data.

1.2. Registrar shall collect the following information and maintain that information for no less than one hundred and eighty (180) days following the relevant interaction:
1.2.1. **Information regarding the means and source of payment** reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor;
1.2.2. **Log files, billing records** and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other
Approved by the ICANN Board on 27 June 2013 records containing communications source and destination information, including, depending on the method of transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier, associated with communications between Registrar and the registrant about the Registration; and
1.2.3. **Log files** and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry- wide generally accepted standard practices within the industries in which Registrar operates, other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration.

8. Title: New gTLD Registry Agreement (2014)

Summarized by: Pruis

New TLD Registries have a contractual obligation to collect and publish:
SPECIFICATION 4 : REGISTRATION DATA PUBLICATION SERVICES

1.4. The fields specified below set forth the minimum output requirements. Registry Operator may output data fields in addition to those specified below, subject to approval by ICANN, which approval shall not be unreasonably withheld.

1.5. Domain Name Data:

Domain Name: EXAMPLE.TLD
Domain ID: D1234567-TLD
WHOIS Server: whois.example.tld
Referral URL: http://www.example.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Registrant, Admin, Tech, ID: 5372808-ERL
Registrant, Admin, Tech, Name: EXAMPLE REGISTRANT
Registrant, Admin, Tech, Organization: EXAMPLE ORGANIZATION
Registrant, Admin, Tech, Street: 123 EXAMPLE STREET
Registrant, Admin, Tech, City: ANYTOWN
Registrant, Admin, Tech, State/Province: AP
Registrant, Admin, Tech, Postal Code: A1A1A1
Registrant, Admin, Tech, Country: EX
Registrant, Admin, Tech, Phone: +1.5555551212
Registrant, Admin, Tech, Phone Ext: 1234
Registrant, Admin, Tech, Fax: +1.5555551213
Registrant, Admin, Tech, Fax Ext: 4321
Registrant, Admin, Tech, Email: EMAIL@EXAMPLE.TLD
Name Servers: NS01.EXAMPLEREGISTRAR.TLD
DNSSEC: signedDelegation
DNSSEC: unsigned
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.6. Registrar Data:

Registrar Name: Example Registrar, Inc.
Street: 1234 Admiralty Way
City: Marina del Rey
State/Province: CA
Postal Code: 90292
Country: US
Phone Number: +1.3105551212
Fax Number: +1.3105551213
Email: registrar@example.tld
WHOIS Server: whois.example-registrar.tld

Referral URL: http://www.example-registrar.tld
Admin & Tech Contact: Joe Registrar
Phone Number: +1.3105551213
Fax Number: +1.3105551213
Email: joeregistrar@example-registrar.tld
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.7. Nameserver Data:

Server Name: NS1.EXAMPLE.TLD
IP Address: 192.0.2.123
IP Address: 2001:0DB8::1
Registrar: Example Registrar, Inc.
WHOIS Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

New TLD Registries have a contractual obligation to provide to ICANN:
Specification 3. 2. Monthly Registry Functions Activity Report.

- Whois-43-queries : number of WHOIS (port-43) queries responded during the reporting period
- Web-whois-queries : number of Web-based Whois queries responded during the reporting period, not including searchable Whois
- Searchable-whois-queries : number of searchable Whois queries responded during the reporting period, if offered

SPECIFICATION 4 REGISTRATION DATA PUBLICATION SERVICES

3. Bulk Registration Data Access to ICANN

3.1. Periodic Access to Thin Registration Data. In order to verify and ensure the operational stability of Registry Services as well as to facilitate compliance checks on accredited registrars, Registry Operator will provide ICANN on a weekly basis (the day to be designated by ICANN) with up-to-date Registration Data as specified below. Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN.

3.1.1 Contents. Registry Operator will provide, at least, the following data for all registered domain names: domain name, domain name repository object id (roid), registrar id (IANA ID), statuses, last updated date, creation date, expiration date, and name server names.
For sponsoring registrars, at least, it will provide: registrar name, registrar repository object id (roid), hostname of registrar Whois server, and URL of registrar.

9. Title: WHOIS Registrant Identification Study (2013)

Summarized by: Mounier

NORC at the university of Chicago was contracted by ICANN to conduct a WHOIS Registrant Identification Study (2013)

This project is an exploratory examination of WHOIS data for a representative sample of gTLD domain names, using WHOIS Registrant Name and Registrant Organization values to classify the types of entities that register domains, including natural persons, legal persons, and privacy and proxy service providers. In other words, the study tries to classify the types of entities that appear to be using domains and the various types of activities associated with them.

The study is based on a sample of 1,600 domains, selected from the top five gTLDs.

The purpose of the study is to provide a foundation for answering the following questions posed by the Government Advisory Committee (GAC):

- What is the percentage of registrants that are natural versus legal persons?
- What is percentage of domain name uses that are commercial versus non-commercial?
- What is the relative percentage of Privacy/Proxy use among legal persons?
- What is the relative percentage of Privacy/Proxy use among domains with commercial use?

Conclusion:

- This is an interesting study which gives quantitative information for instance on the percentage of WHOIS registrant address country or region of the world (or the record: more than 50% are US-based), or the percentage of domains found by accredited registrars, or the percent of domains found on spam blacklists.
- However, there is no specific information on data elements relevant for the work of the NGRDS sub-group on data.

10. Correspondence: Article 29 WP on the data protection impact of the ICANN RAA (2013-2014)

https://www.icann.org/en/system/files/correspondence/namazi-to-kohnstamm-25mar14-en.pdf
https://www.icann.org/en/system/files/correspondence/kohnstamm-to-jeffrey-08jan14-en.pdf
https://www.icann.org/en/system/files/correspondence/jeffrey-to-kohnstamm-20sep13--en.pdf
https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf

Summarized by: Bockey

- The documents mainly concern collection, data retention and privacy in EU as related to RAA and waivers
- No direct discussion of registration data elements, although this document <https://www.icann.org/en/system/files/correspondence/jeffrey-to-kohnstamm-20sep13-en.pdf> notes the long standing RAA obligation to maintain billing information, which "serves a legitimate purpose…such as helping registrants resolve problems related to their domain name accounts w/Registrars."

11. Correspondence: Article 29 WP on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS (2012)

https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-atallah-26sep12-en.pdf
https://www.icann.org/en/news/correspondence/chehade-to-kohnstamm-09oct12-en
Summarized by: Bockey

- The documents mainly concern data accuracy, data privacy and data retention under the RAA
- No direct discussion of registration data elements. However, this document <https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-atallah-26sep12-en.pdf> discusses annual re-verification of contact details, namely telephone number and email address, (page 2, 3rd paragraph). While the re-verification originates from LE, phone & email are considered registration data elements.

See also Ali summary of this correspondence:

- The Working Party recalls its previous contributions to the process of collecting and disclosing WHOIS data, as included in the Opinion 2/2003 on the application of the data protection principles to WHOIS directories as well as its letters of 22 June 2006 to the Board of Directors of ICANN5 and of 12 March 2007 to the Chairman of the Board of Directors of ICANN6 in which the relevant data protection principles have been outlined
- In assessing these proposals, ICANN should be aware that the purpose of collecting and publishing contact details in the WHOIS database is to facilitate contact about technical issues. The original purpose definition reads: “The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS name server."
- The Working Party strongly objects to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it is up to national governments to introduce legislation that meets the demands of article 8 of The European data retention directive 2006/24/EC imposes data retention obligations on providers of public electronic communication networks and services. Registrars are not such providers and are therefore not subjected to this European data retention obligation.

12. Correspondence: Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2007)

http://gnso.icann.org/en/correspondence/cerf-to-schaar-24oct07.pdf
https://www.icann.org/en/system/files/files/cerf-to-schaar-15mar07-en.pdf
https://www.icann.org/en/correspondence/schaar-to-cerf-12mar07.pdf
Summarized by: Bockey

- The documents mainly concern data protection and privacy
- Does not discuss registration data elements

13. Correspondence: Article 29 WP on ICANN's WHOIS Database Policy (2006)

https://www.icann.org/en/system/files/files/schaar-to-cerf-22jun06-en.pdf
https://www.icann.org/en/correspondence/lawson-to-cerf-22jun06.pdf
https://www.icann.org/en/correspondence/parisse-to-icann-22jun06.pdf
https://www.icann.org/en/system/files/files/fingleton-to-cerf-20jun06-en.pdf
Summarized by: Bockey

- The documents mainly concern purpose and privacy
- Does not discuss registration data elements

14. Title: Article 29 WP 76 Opinion 2/2003 on the application of data protection principles to WHOIS directories

Summarized by: Bockey

- The document mainly concerns data protection and privacy
- Mentions <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_en.pdf> WHOIS data when a domain is registered and which contains information "of the contact-point for the domains, namely, phone number, email address and other personal data." (paragraph 1 under Intro)

15. Additional Article 29 WP Documents

Article 29 WP 5 Recommendation 2/97
Article 29 WP 33 Opinion 5/2000
Article 29 WP 41 Opinion 4/2001
Article 29 WP 56 Working Document 5/2002
Article 29 WP 217 Opinion 4/2014 (missing?)
Summarized by: Padilla

There has been enough discussion on the if I can call it the maintenance of how data should be kept in according to the laws of various countries as all have different laws that more or less try to do the same thing in different words and explanation. For e.g.

Opinion 5/2000 - The use of Public Directories for Reverse or Multi-criteria Searching Services

1. Directive 95/46/EC - the protection of individuals with regard to the processing of the personal data, in Article 6.1 b), which establishes that personal data must be "collected for specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes".

2. Note the purpose of conventional telephone directories is the disclosure of subscriber's telephone number starting from the knowledge of subscriber's name and that its use is limited to that specific purposes.

3. Must establish the balance of interests, the interests and risks to privacy at stake have to be identified and evaluated. Directive 97/66/EC gives helpful indications: as long as the minimum information necessary to identify a subscriber is at stake, thus this information can be included in conventional public directories unless the subscriber objects. It must be considered that the interest of the individual in being protected override the interests of controller or third parties. Therefore such processing is only legitimate if the individual has given his/her informed consent prior to any inclusion of his /her personal data in public directories for reverse or multi-criteria searches.

4. Specific and informed consent of the subscriber must be obtained prior to the inclusion of his personal data into all kinds of public directories which include all type of communication devices used for reverse or multi-criteria searches. There must be some given consent on how personal data can be used.

5. As most conclusions regard the directives of the EC previous WP on the Protection of Individuals with regards to protection of data takes the position that processing of said personal data in reverse directories or multi-criteria searching services without unambiguous and informed consent by subscriber is unfair and unlawful. Thus fully implementing and accepting the EC proposal for draft directive on processing personal data.

Opinion 4/2001 - On the Council of Europe's Draft Convention on Cyber-Crime

1. Article 15 of draft Convention could create the impression that the protection of human rights shall only be considered when it is "due" and shall on be "adequate". It can be seen as limiting the safeguards and procedures it would considerably low if not fully undermine the protection of fundamental rights.

2. Finally with several EU countries implementing Directive 95/46/EC shows that national laws requires personal data can be in principle only be sent to non-EU countries if this country does provide an adequate level of protection of individuals with regard to the processing of their personal data. The level of protection in these countries must be checked. Otherwise if no adequate protection on offer in third country then transfer pf personal data may nevertheless be necessary to fight against crime.

[Working Document] Adopted 5/2002 - Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based website

In all these cases, the application of EU data protection law means amongother things the following:

1. With a view to making the collection of personal data fair and lawful, the controller has to clearly define the purpose of the processing.

2. The controller has also to ensure that the data are adequate, relevant and not excessive in relation to the purpose for which they are collected.

3. The collection must be based on a legitimate ground (unambiguous consent, performance of a contract, compliance with a legal obligation, in pursuance of legitimate interests of the controller etc.) and the individual has the right of access to and the rectification or erasure of his personal data.

4. The individual has at least to be informed about the identity of the controller and his representative if any, the purpose of the collection, the recipients and about his rights 32 .

5. Another important aspect is the security of the processing which may require the controller, right from the collection on, to apply specific technical and organisational measures in order to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the data are transmitted over a network. Such measures shall ensure a level of security appropriate to the risks presented and the nature of the data.

6. As regards sensitive data, specific provisions, dealing in particular with security requirements, regulate their collection.

7. The Article 29 Data Protection Working Party considers that the development of a programme for the promotion of European data protection rules in a pragmatic way would also help controllers in third countries to better understand, implement and demonstrate privacy compliance. A European system of labels/web seals, open also to non-EU web sites, could be the cornerstone of such action.

Finally the other documents [e.g., Article 29 WP 5 Recommendation 2/97] seem to repeat or rewrite similar points that will not make this summary any easier to further what can be used as a defined process of how data can be collated for use and kept in the way that provides the privacy required. This shows that the EU or EC directive on the protection of personal data has been the benchmark and implemented to used to protect personal data and privacy. No specific mention of length of time to hold such data although I think 6 weeks has been mentioned in one document I think. Also the last couple of summarised documents are definitely more on the privacy relation of personal data but think there may show some relevance towards the items we collect that can reference how data can be seen.

16. Title: Article 29 WP 20 Opinion 3/1999

Summarized by: Ali

Relevant Sections Contained Within Referenced “Opinion No 3/99 on Public sector information and the protection of personal data” by the Working Party on the protection of individuals with regard to the processing of personal data.

One of the key aspects of this opinion is the availability of public sector information. At issue is a specific category of information held by public sector bodies known as "public" information, which would be made public subject to certain rules or for a particular purpose and based, implicitly or explicitly, on the State's desire for transparency with regard to its citizens.

The objective of this Opinion is to provide input for the discussion on the protection of personal data, a dimension which must be taken into consideration when undertaking to grant greater access to public sector data, where such data relates to individuals.

THE RULES ON DATA PROTECTION APPLY TO PERSONAL DATA WHICH HAVE BEEN MADE PUBLIC
Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data covers the principle of the right of public access to administrative documents and other factors which are relevant to the discussion The principle of purpose requires that personal data are collected for specific, explicit and legitimate purposes and are not subsequently processed in a manner which is incompatible with these purposes.

Personal data to be made public do not constitute a homogeneous category which can be dealt with uniformly from a data protection point of view. Instead, a step-by-step analysis is needed of the rights of the data subject and the right of the public to access the data respectively. While there may be public access to data, such access may be subject to certain conditions (such as proof of legitimate interest). Alternatively, the purposes for which the data may be used, for example for commercial purposes or by the media, may be restricted.

At this point it is worth mentioning that regardless of whether or not personal data are published, data subjects always has the right to access their data and, where necessary, to require that they be rectified or erased if they have not been processed in accordance with the Directive, and in particular if they are incomplete or inaccurate.

THE NEW TECHNOLOGIES CAN HELP STRIKE A BALANCE BETWEEN THE PROTECTION OF PERSONAL DATA AND THE PUBLICATION OF SUCH DATA
In addition to promoting access to public data, in particular by providing on-line access, the new technologies and some of the accompanying administrative measures can also help to ensure compliance with the main principles of data protection, such as end purpose, the principle of information, the right to object and the principle of security. However, these technologies do not provide an absolute guarantee against abuses of the principles of personal data protection described above.

Directive 95/46/EC recognises the right of data subjects to be informed about the processing of data concerning them and stipulates that at the very least they have the right to object to legitimate processing. Data subjects must therefore be informed about the commercial usage of data concerning them and must be able to object to such usage by simple and effective means.

Another possibility mentioned in the opinion was to obtain the data subject's consent for commercial usage. Data subjects must have given their consent unambiguously and in full knowledge of the facts, taking into account the fact that anyone applying for planning permission is required to submit a file which meets certain stipulations.

CONCLUSION:
Public access to data does not mean unfettered access: all Member States base their legislation on this philosophy. When personal data are made public, either by virtue of a regulation or because the data

subject himself authorises it, the data subject is not deprived of protection, ipso facto and forever. He is guaranteed such protection by law in accordance with the fundamental principles of the right to privacy.

In order to strike a balance between the right to privacy and the protection of personal data on the one hand, and the right of the general public to access public sector data on the other, conclusions must take account of the following factors and issues:

- a case-by-case assessment of whether personal data can be published/should be accessible or not, and if so, under what conditions and on which media (computerised or not, Internet dissemination or not, etc.);
- the principles of purpose and legitimacy;
- the obligation to inform the data subject;
- the data subject's right to object;
- the use of the new technologies to help protect the right to privacy.

These factors should be taken into account not just in situations where publication or access is already regulated, but also in situations where regulation does not appear necessary, with a view to satisfying the general public's demand for access to public sector information, including personal data.

17. Title: Council of Europe Declaration of the Committee of Ministers on ICANN, human rights and the rule of law (3 June 2015)

Summarized by: Deacon

This document does not make any specific statements regarding the collection, storage and disclosure of user data elements. It does however make one very general statement in paragraph 3 that is germane to “disclosure” of information , e.g.

"In certain criminal investigations, criminal justice authorities need to secure evidence on computer systems and to identify offenders, subject to the conditions and safeguards providing for the adequate protection of human rights pursuant to Article 15 of the Convention on Cybercrime (ETS No. 185)."

In addition, this document references two additional documents that I did not review but may be relevant:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
- Article 15 of the Convention on Cybercrime (ETS No. 185)

18. Title: Draft Directive of the European Parliament (April 2016)

News: Data protection reform – Parliament approves new rules fit for the digital era
Draft Directive of the European Parliament (April 2016)

Summarized by: Padilla

Agreed 14 April 2016:

1. *New EU data protection rules which aim to give citizens back control of their personal data and create a high, uniform level of data protection across the EU fit for the digital era.*

2. "The regulation will also create clarity for businesses by establishing a single law across the EU. The new law creates confidence, legal certainty and fairer competition".

3. The new rules include provisions on:

- a right to be forgotten,
- "clear and affirmative consent" to the processing of private data by the person concerned,
- a right to transfer your data to another service provider,
- the right to know when your data has been hacked,
- ensuring that privacy policies are explained in clear and understandable language, and
- stronger enforcement and fines up to 4% of firms' total worldwide annual turnover, as a deterrent to breaking the rules.

19. Title: Opinion of the European Data Protection Supervisor: Europe's role in shaping the future of Internet Governance (23 June 2014)

Summarized by: Padilla

1. Base the future development of Internet Governance on the respect of fundamental rights. We welcome this principle, but we stress the need to translate it into practical policy initiatives, which is not always sufficiently the case.

2. We emphasise that, in order to "sustain and develop the Internet as an essential part of life" and to create a "single, open, free, unfragmented network of networks" with a "safe, secure, sound and resilient architecture", Internet Governance should be built starting from commonly shared international rights and values. Consequently, privacy and data protection principles need to gain more weight within Internet Governance fora and mechanisms.

3. We note some positive developments at international level in recognising privacy and data protection as essential values for the internet. At the Net Mundial, a general consensus was reached on the need to protect privacy on the Internet, by pointing out that "The right to privacy must be protected. This includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data. The right to the protection of the law against such interference should be ensured".

4. The Communication emphasizes that the Internet has become a key infrastructure with global dimensions and that, as a consequence, greater international balance within the existing structures would increase the probability of issuing legitimate outcomes.

20. Title: EDPS on ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and - Legitimate Purposes for Collection and Retention (17 April 2014)
Summarized by: Padilla

1. The Draft Specification should only require collection of personal data, which is genuinely necessary for the performance of the contract between the Registrar and the Registrant (e.g. billing) or for other compatible purposes such as fighting fraud related to domain name registration. This data should be retained for no longer than is necessary for these purposes. It would not be acceptable for the data to be retained for longer periods or for other, incompatible purposes, such as law enforcement purposes or to enforce copyright.

2. Retention of personal data originally collected for commercial purposes, and subsequently retained for law enforcement purposes, has been the subject of a recent landmark ruling by the European Court of Justice, which held Directive 2006/24/EC to be invalid, as an unjustified interference with those rights. The Court recognised that the retention of personal data might be considered appropriate for the purposes of the detection, investigation and prosecution of serious crime, but judged that the Directive 'exceeded the limits imposed by compliance with the principle of proportionality'. It is reasonable to expect requirements for retaining personal data to be subject to increasing scrutiny and legal challenges in the EU. And limit processing of this data to compatible purposes, such as proportionate measures to fight fraud related to domain name registration.

21. Title: IWG Common Position relating to Reverse Directories (Hong Kong, 15.04.1998)
Summarized by: Ali

It is in any case necessary to endow the persons with the right to be informed by their provider of telephone or e-mail service, at the time of the collection of data concerning them, or if they have already subscribed, by a specific means of information, of the existence of services of reverse search and - if express consent is not required - of their right to object, free of charge, to such a search.

22. Title: IWG Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet (Crete, 4./5.05.2000)
Summarized by: Ali

The Working Group notes that the "Working Party on the protection of individuals with regard to the processing of personal data" of Data Protection Commissioners in the European Union ("Article 29 Group") has addressed these issues extensively in their “Opinion 3/99 on Public Sector information and the Protection of Personal Data” and fully supports their findings.

23. Title: IWG Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet (Crete, 4./5.05.2000)

Summarized by: Ali

- The amount of data collected and made publicly available in the course of the registration of a domain name should be restricted to what is essential to fulfil the purpose specified. In this respect the Working Group has reservations against a mandatory publication of any data exceeding name (which might also be the name of a company and not of a natural person), address and e-mailaddress in cases where the domain name holder is not himself responsible for the technical maintenance of the domain but has this done through a service provider (as is the case with many private persons who have registered domain names).

- Any technical mechanism to be introduced to access the data collected from the registrants must furthermore have safeguards to meet the principle of purpose limitation and avoidance of the possibility to unauthorised secondary use of the registrant's data.

24. Title: IWG Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000)

Summarized by: Ali

Data Austerity: Telecommunications infrastructure has to be designed in a way that as few personal data are used to run the networks and services as technically possible.

Virtual Right to be Alone: Nobody must be forced to let his or her personal data be published in directories or other indices. Every user has to be given the right to object to his or her data being collected by a search engine or other agents. Every user has to be given the right and the technical means to prevent the intrusion of external software into his own devices.

25. Title: IWG Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe (Berlin, 13/14.09.2000)

Summarized by: Ali

In this respect the Working Group fully supports the findings of the European Data Protection Commissioners Conference that such retention of traffic data by Internet service providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights. This goes also for storing data revealing the use of the Internet by individuals. Existing powers for tracing crimes should not be extended in a way that invades privacy until the need for such measures has been clearly demonstrated. The Working Group has in the past stated that any Interception of Private Communications should be subject to appropriate safeguards.

26. Title: RFC 7485 Inventory and Analysis of WHOIS Data

Summarized by: Coupet

Regional Internet Registries (RIRs) and Domain Name Registries (DNRs) have historically maintained a lookup service to permit public access to some portion of the registry database. Most registries offer the servicevia the WHOIS protocol [RFC3912], with additional services being offered via World Wide Web pages, bulk downloads, and other services, such as Routing Policy Specification Language (RPSL) [RFC2622].

This document records an inventory of registry data objects to facilitate discussions of registration data objects. The Registration Data Access Protocol (RDAP) ([RFC7480], [RFC7482],[RFC7483], and [RFC7484]) was developed using this inventory as input.

- Some data elements were not supported by all RIRs, and some were given different labels by different RIRs. Also, there were identical labels used for different data elements by different RIRs.
- All of the 124 domain registries have the object names in their responses, although they are in various formats.
- Of the118 WHOIS services contacted, 65 registries show their registrant contact. About half of the registries (60 registries)support admin contact information. There are 47 registries, which is about one third of the total number, that have technical and billing contact information. Only seven of the 124 registries give their abuse email in a "remarks" section. No explicit abuse contact information is provided.
- There are mainly two presentation formats. One is key-value; the other is data block format. Most of the domain-related WHOIS information is included in the top10 data elements. Other information like name server and registrar name is also supported by most registries.

27. Title: EWG Recommendations for a Next-Generation RDS, especially

Section 4a, Data Element Principles, and Annex D, Purposes and Data Needs
Summarized by: Dinculescu

Section 4 of the report looks at Improving Accountability, and identifies the following:

- Proposed data elements to be collected
- Whether or not each element should be mandatory for collection
- Whether or not each element should be disclosed on a WHOIS search, or require special access

The table below is a direct extract from section 4. The column “Collection M or O” defines whether the data element is “mandatory” or “optional” for collection. The column “Disclosure Default P or G” defines whether the data element is disclosed “publicly” or requires “gated access” by default. All of the

elements required as part of the 2013 Registry Agreement as well as the 2013 Registrar Accreditation Agreement are included, with newly proposed data elements.

Data Element	Collection M or O	Disclosure Default P or G
REGISTRY/REGISTRAR PROVIDED DATA		
Registration Status	M	P
DNSSEC Delegation	O	P
Client Status (registrar)	M	P
Server Status (registry)	M	P
Registrar	M	P
Reseller	O	P
Registrar Jurisdiction	M	P
Registry Jurisdiction	M	P
Registration Agreement Language	M	P
Creation Date	M	P
Original Registration Date	O	P
Registrar Expiration Date	M	P
Updated Date	M	P
Registrar URL	M	P
Registrar IANA Number	M	P
Registrar Abuse Contact Email Address	M	P
Registrar Abuse Contact Phone Number	M	P
URL of Internic Complaint Site	M	P
REGISTRANT DATA COLLECTED FROM REGISTRANT		
Data Element	**Collection M or O**	**Disclosure Default P or G**
Domain Name	M	P
DNS Servers	M	P
Registrant Name	M	G
Registrant Type	M	P
Registrant Contact ID	M	P
Registrant Contact Validation Status	M	P
Registrant Contact Last Validated Timestamp	M	P
Registrant Organisation	O	P
Registrant Company Identifier	O	P
Registrant Street Address	M	G

Registrant City	M	G
Registrant State/Province	O	G
Registrant Postal Code	O	G
Registrant Country	M	G
Registrant Phone + Extension	M	G
Registrant Alternate Phone + Extension	O	G
Registrant Email Address	M	P
Registrant Alternate Email Address	O	P
Registrant Fax and Extension	O	G
Registrant SMS	O	G
Registrant Instant Messenger	O	G
Registrant Social Media	O	G
Registrant Alternate Social Media	O	G
Registrant Contact URL	O	G
Registrant Abuse URL	O	G

The report identifies various Purpose Based Contacts (PBCs) which will be listed on the WHOIS. Each PBC serves a specific purpose as follows:

- Admin: Handling requests related to domain name acquisition and sale, such as purchase inquiries and domain name transfers.
- Legal: Handling requests about this domain name from tax authorities, UDRP investigators, contractual compliance investigators, and legal representatives.
- Technical: Handling requests about this domain name related to problems with website outages, DNS issues, mail delivery issues, etc.
- Abuse: Handling DNS abuse reports about this domain name, including phishing, spam, and other harmful Internet activities.
- Privacy Proxy: Handling requests for relay/reveal, fielding complaints about domain name abuse on behalf of the Registrant/Licensee, complying with LEA investigations into criminal activities.
- Business: Handling consumer requests for information about a business and information for contacting the company for further information or to resolve customer complaints.

The report proposes the following data elements for EACH PBC, to be disclosed in the WHOIS. The "Collection" column now includes an additional option "R" meaning "Recommended". "Recommended" means that the information may not be provided at the discretion of the Contact Holder.:

PURPOSE BASED CONTACTS (PBC)		
Data Element	**Collection M or O**	**Disclosure Default P or G**
PBC Contact Type Contact ID	M	P
PBC ID	M	P
PBC Validation Status	M	P

PBC Last Validated Timestamp	M	P
PBC Name	M	P
PBC Organisation	M	P
PBC Street Address	M	P
PBC City	M	P
PBC State/Province	O	P
PBC Postal Code	O	P
PBC Country	M	P
PBC Phone + Extension	R	P
PBC Alternate Phone + Extension	R	P
PBC Email Address	M	P
PBC Alternate Email Address	R	P
PBC Fax + Extension	O	P
PBC SMS	R	P
PBC Instant Messenger	R	P
PBC Social Media	O	P
PBC Alternate Social Media	O	P
PBC Contact URL	R	P
PBC Abuse URL	O	p

For some PBCs "mandatory" requirements are listed as "recommended" requirements. For the purpose of saving space in this review, all "R" requirements where an "M" is set for another PBC, have been listed as "M" by default. The readers are encouraged to review the differences in "R" and "M" for each PBC, outlined in the table provided in the EWG report on pages 51 to 56.

The report also proposes new data elements which have the following definitions:

- Registrar and Registry Jurisdiction: The legal jurisdiction in which the Registrar or Registry operates, as indicated in their signed agreement with ICANN.
- Registration Agreement Language: The language in which the Registrar's contract with the Registrant is written.
- Original Registration Date: The date on which this domain name was first registered
- Client Status, Server Status: Expanding upon 2013 RAA client status values, these data elements contain the Registrar (client) and Registry (server) status values currently applied to this domain name: DeleteProhibited, RenewProhibited, TransferProhibited.
- Registrant Company Identifier: The UK trading number, D-U-N-S number, or other unique real-world company identifier assigned to the Registrant by a public business directory. This enables searching for a company outside the RDS.
- Registrant Contact ID: A unique handle assigned to a pre-validated block of contact data identified as this domain name's Registrant. This ID enables reuse and maintenance of contact data within the RDS. Note that when Registrant Type = Privacy/Proxy, the Registrant Contact ID will reflect the unique identifier assigned to that accredited Privacy/Proxy Provider. Registrant/PBC Contact Validation Status,

- Registrant/PBC Contact Last Validated Timestamp: The highest level of validation achieved and the date that is was mostrecently validated.
- Registrant/PBC SMS, IM, Social Media: New contact methods that may optionally be used to reach the Registrant or PBC via SMS, instant messaging, or another alternative social media communication vector.
- Registrant/PBC Alt Email, Alt Phone, Alt Social Media: New alternative addresses that may optionally be used to reach the Registrant or PBC when the primary address fails. These new data elements are intended to address common needs such as resolving tech issues when the domain name itself is down and enabling faster contact via mobile phone or social media.
- Registrant/PBC Contact_URL, Abuse_URL: New data elements that optionally lead to web pages where contact or abuse reporting instructions, policies, or forms may be placed to facilitate more productive communication.
- PBC Contact ID: A unique handle assigned to a pre-validated block of contact data identified as a PBC for this domain name, in the role indicated by the Contact Role. Registrant Contact ID and PBC Contact ID may or may not refer to the same contact.

28. Materials: EWG Tutorials and FAQs

EWG Tutorial Pages 10-14, 45-60

EWG FAQs 13-24

Video FAQ "What is the RDS minimum public data set?"

Summarized by: Dinculescu

EWG Tutorial

The document addresses data on slides 10 to 14. It mentions that the WHOIS currently in use is potentially limited and does not allow for additional or alternate data (which may be useful?).

The document proposes a "minimum public data" approach, whereby only certain data elements will be disclosed, while the majority of data will be disclosed based on access rights.

The document introduces Purpose Based Contacts (PBSs), who are validated externally, can update their own information, and whose data elements may be disclosed.

The document defines that the "minimum registration data" be publicly available without any form of authentication. This includes (from the data elements in the report):

- Domain name data supplied by Registrars and Registry
- Registrant Contact ID
- Registrant Email address
- Minimum public registrant contact data
- PBC's ID

EWG FAQs

The EWG FAQ addresses questions regarding data elements in FAQs 13 to 18. There is no specific mention of actual data elements, but references to the report about how the EWG proposed to handle existing and potentially new data elements.

The EWG FAQ addresses questions regarding data collection and storage in FAQs 19 to 24. It recommends (FAQ 19) that a new third-party be introduced to handle the data collection and validation.

The EWG FAQ also addresses the reasoning behind the proposed new Purpose Based Contacts (PBCs), providing the definition and purpose of each, but not the data elements, as the elements are defined in the report.

FAQs 25 to 31 address the purpose of the data and why new data elements have been proposed. It further clarifies how disclosure will be handled through gated access at the registrar and registry level.

Video FAQ: What is the RDS minimum public data set

From 0:26 to 0:42 the speaker mentions that the proposed RDS will provide just enough data to:

- meet basic, common DNS needs
- communicate with each domain's registry and registrar
- identify the email of the registrant
- identity the designated Purpose Based Contacts (PBCs)

If any additional data elements are required, authentication would depict what data elements would be returned.

At 1:05 the speaker mentions that PBCs will maintain their own data (accuracy of the data).

At 1:18 the speaker confirms the "minimum public data" to be provided as:

- Domain name data supplied by Registrars and Registry
- Registrant Contact ID
- Registrant Email Address
- Minimum public registrant contact data
- PBC's ID

At 1:40 the speaker confirms that mandatory PBS data elements will be required as part of a new domain name registration, but the public viewing would be restricted to PBC ID and not the rest of the PBC data.

29. Title: EWG Member Statement by Perrin

Summarized by: Deacon (p2)

The focus of this document is not on the specifics of individual data elements but on topics more relevant to the other sub groups. There are however two mentions of data elements on page one. Specifically:

- Legal Contact Email and Legal Contact Phone Number
- Registrant Address, Registrant Phone Number

It is important to note however that these mentions occur in a section where the author (Stephanie) states that she does not agree with the consensus of the EWG Final Report.

30. Title: Process Framework for a PDP on Next-Generation RDS

Summarized by: Deacon

This document does not make any specific statements regarding the collection, storage and disclosure of user data elements.

[ED NOTE: REFER TO PAGE 9, ROW 4, WHICH DEFINES A 3-PHASE PROCESS FOR DATA ELEMENTS]

31. Internationalized Registration Data (IRD) Reports

Summarized by: Elsadr (to be provided)

ICANN Internationalized Registration Data (IRD) Working Group Final Report
Expert Working Group on Internationalized Registration Data (IRD) Final Report
GNSO Translation and Transliteration of Contact Information PDP Working Group Final Report

Answers to Questions, drawn from Key Inputs and Summaries above:

(i) Did this input inventory produce any insights to inform the WG's work plan?

[no answer provided]

(ii) Which inputs are likely to be the most relevant during WG deliberations and why?

- Whois Task Force Final Report, because it is a good foundation for what was required in the past, and mostly what is still required
- SAC 054, because gives us what us the now of what is required
- EWG Recommendations, including tutorials and FAQs, because gives us insight into what might be required in the future, where data elements might be moving towards. also provides principles regarding why data elements should or should not be collected/displayed or made mandatory/optional, as well as the concept of purpose-based contact data
- RA Spec 4, because gives us what us the now of what is required
- RFC 7485 because it is very helpful to understand what data elements are collected today

(iii) Which inputs, if any, generated the most discussion within the small team?

- SAC54 triggered several emails on the data list.

(iv) Which inputs may be obsolete or super-ceded by subsequent work?

- Whois Task Force 2003 report was superceded by the Whois Task Force report of 2007. 2012 WHOIS RT report is successor to the 2007 TF report, but all reports are relevant as history of discussion on the this issue.

(v) What input gaps, if any, may need to be addressed later?

- Should IRD and related work have been considered by this sub-team or for future review? Consider adding IRD report to list of most relevant inputs.
- Current focus seems to be more on data that is currently displayed in WHOIS. This is a subset of data collected by registrars during registration. Do we need to account for data collected but not made available in the (current) WHOIS?
- Whowas - is covered in EWG but not in any of the other documents that has been reviewed. WHOWAS was briefly touched on in the WHOIS Survey WG, which was a survey built more on the technical requirements of a WHOIS system (see http://gnso.icann.org/en/group-activities/inactive/2013/whois-requirements).
- RDAP Operational profile (see https://whois.icann.org/sites/default/files/files/gtld-rdap-operational-profile-draft-03dec15-en.pdf)

(vi) Other key takeaways from this input inventory the team wishes to share with the WG

- RA Spec 4 (now) and EWG recommendations (possible future) are considered two key documents to help inform the WG's deliberations