RDS PDP WG DT5 Deliverable 26 Oct 17

Purpose Name: **Regulatory or Contractual Enforcement**

Definition:

A variety of entities from both the public sector (apart from traditional law enforcement agencies) and the private sector have a remit to enforce obligations arising under contracts, industry best practices, or governmental regulation, that relate to activities on the Internet. These entities include governmental tax authorities, UDRP and URS providers, the ICANN organization, intellectual property owners, and merchant account monitoring solution providers, among others. This purpose makes it possible for these public and private enforcement entities to identify and in many cases, contact domain name registrants to resolve issues associated with compliance with these contracts, best practices, or regulations. Such enforcement efforts, and/or the necessary investigative steps preliminary to such enforcement, depend upon access to information relating to the identity and/or location of domain name registrants, or other data contained in the RDS.

Tasks:

- Investigation of operators of websites where a property owner's rights are being exercised

    o Using registration data to seek to ascertain the identity and location of the operator (or domain name registrant responsible for) a website on which A's intellectual property rights are being exercised. For example:
        - This could involve use of A's trademark in logos displayed on the site; offers for sale of merchandise bearing A's trademark; making available for download or streaming movies or sound recordings for which A holds the copyright; etc. This is a necessary first step to determining whether the operator (or registrant) is a licensee with respect to the intellectual property in question, and if so, whether the use of the intellectual property exceeds the scope of the license (e.g., because of territorial restrictions in the license).
        - Alternatively, if A determines that the operator/registrant is not a licensee, this is a necessary first step in seeking contractual enforcement of terms of service by the registrar/registry, and/or potentially ICANN contractual enforcement of registrar/registry obligations to investigate and take appropriate action.
        - Additionally, if the registrant contact data obtained is clearly false, this can lead to a false Whois complaint, triggering remedies under applicable contracts with ICANN.

- Apart from the IP this is also used to identify the identity of the holders of domain names as a first level review. This can come from individuals or small companies equally.
- Controlling authority to ensure that bindings contracts between registrants and registries or between registrars and registries are compliant and that they follow established operating procedures for data protection, users privacy, data processing rules, etc.

Users:

- Trademark and copyright owners, or their exclusive licensees, and/or their investigators, attorneys or other agents engaged in contract compliance as well as registrants with family names or small orgs
- Tax collection agencies may request to access registration data to identify identification of contacts for domain name engaged in on-line sales.
- Regulatory agencies may want to access registration for many purposes: investigations, compliance and auditing, billing, etc.
- UDRP and URS Providers confirm the correct respondent for a domain name, perform compliance checks, determine legal process requirements and protect against cyberflight.
- ICANN Compliance audit and respond to complaints about non-compliance by contracted parties (e.g., data inaccuracy or unavailability, UDRP decision implementation, transfer complaints, data escrow and retention).

Data:

- Data tending to establish the identity and/or location of domain name registrant. For example, Registrant Name and Registrant Address (at least province/country address) could be relevant here.
- Data that tend to categorize the type of users: individual, corporation, organization, academic, etc. The types of users may result in different tax systems or different compliance standards.
- Specific data elements by use case:

  1. Investigation into fraudulent and inaccurate information (by government and/or regulatory/controlling authority):
     - Registry Expiry Date
     - Registrant Name
     - Registrant Email
     - Name Server

- Registrant Name
- Registrant Phone
- Log files and, … other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration
- Name server status

2. A tax authority may require the following data elements for billing and tax collection purpose
   - Domain Status
   - Domain Name
   - Registrant Name
   - Registrant Street
   - Registrant Email

3. A government agency (regulatory, for instance)
   - Domain name
   - Registrar Whois Server
   - Registrar URL
   - Update date
   - Registry Expiry Date
   - IP address
   - Registrar
   - Registrar abuse contact email
   - Reseller
   - Domain status
   - Registrant Name
   - Registrant E-mail
   - Admin name
   - Tech ID
   - Name server
   - Billing Contact name
   - DNSSEC
   - Registrar WHOIS server

4. A regulatory or Controlling authority (such as ICANN organization) may require the following data elements to check ICANN contractual compliance
   - Registrant Name
   - Registrant Street
   - Registrant Email
   - Registrant Email
   - Name Server
   - Domain Status

- Log files and, … other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration
- Updated Date
- Registry Expiry Date