Use Cases That Support Automated Disclosure Decisions – V2.00

Assumptions:

1. All requestors have been accredited by Accreditation Authority and all requestors are individually authenticated by the Gateway.
2. All requests are syntactically correct and complete, including any/all required Authorization Assertions.
3. The Authorization Provider (be it the Central Gateway or the CP) has access to the data required to make the decision, such as access to the Public RDS/WHOIS data collected per Phase 1 Policy, or various flags indicating prior disclosure.
4. A requestor can selectively assert whether data specific disclosed in response to a particular request will be used in a way that has legal or similarly significant effects on the data subjects.
5. If the Gateway does not authorize automated disclosure, it may have enough information to make an informed suggestion to a CP regarding the CP’s processing. CPs with enough confidence in the Gateway may choose to automate based on the Gateway's recommendation.
6. CPs shall provide feedback about the quality of past recommendations to the Gateway in order to improve the recommendation of future recommendations.
7. The Gateway can automate a limited subset of requests. For use cases where we determine that the Gateway cannot make an automated decision based on the request alone, the Gateway may require the unredacted RDS data to make a decision to require automated disclosure by the CP. Such cases would require the Gateway Operator to be a data controller, not just for the data of requestors, but for registrants as well.
8. As more legal certainty is acquired, additional use cases may be added to this list.

Use Cases:

1. **LEA in same jurisdiction as CP**
   1. Examples
      1. Law Enforcement Agency from Jurisdiction A requests Registrant RDS data from a Registrar also in Jurisdiction A
      2. Competent DPA requests data in response to a Data Subject complaint that their data is being misused in violation of the GDPR
   2. For the Gateway to make a good recommendation, access to the City field may be required; see below
2. **Request for City Field (only)**
   1. Examples
      1. Requestor submits a request for the City field in order to ascertain which specific jurisdiction to make a legal claim, or
      2. Requestor submits a request for the City field for the purpose of statistical research or similar non-legal purpose
   2. In each example, our Phase 1 policy suggests that the requestor should not join the City field data with any other data held concerning the same data subject.
      1. In Example 2a(i), it is safest if the City field is requested first for purposes of determining jurisdiction, then discarded before requesting the remainder of the data required for the legal claim.
3. **Registration record contains no personal data and has already been disclosed**
   1. Once registration data has been determined to contain no personal data (e.g. as a result of a previous disclosure), it can be flagged for automatic disclosure in future requests.
      1. The flag remains valid so long as none of the contact data fields have changed.
   2. The Gateway shall determine whether any data fields have changed by inspecting the Public RDS/WHOIS data.
   3. The flag could be stored at either the CP and/or in the Gateway, if the Authorization Provider can review it at the time of the request
   4. A registrar could optionally implement a system to flag such a domain for automation when the data is collected, to enable later automation.
   5. NOTE: Some TLDs are not expected to contain any personal data, and this can streamline processing.
      1. See .BANK, .INSURE, .MUSEUM, and others
      2. There may be other TLDs whose registries enforce policies requiring disclosure, even for personal data, which may streamline processing
      3. There should be a verification element included in the registry policies to detect registrants who circumvent the registry policy requirement
4. **Registration record has already been disclosed under the same authorization assertions to a requestor of the same type**
   1. Once registration data has been disclosed, it can be flagged for automatic disclosure in future requests if
      1. The same authorization assertions are used, and
      2. The requestor is of an equivalent type to the previous one, and
      3. None of the contact data fields have changed
      4. Example:
         1. Requestor is an accredited cybersecurity entity requesting to investigate phishing, and the data was already disclosed to a different accredited cybersecurity entity investigating phishing
   2. Gateway can determine whether any data fields have changed by inspecting the Public RDS/WHOIS data
   3. The flag includes details of the previous assertions and previous disclosed-to entity type
   4. The flag could be stored at either the CP and/or in the Gateway, if the Authorization Provider can review it at the time of the request
   5. A registrar could optionally implement a system to flag such a domain for automation when the data is collected, to enable later automation
   6. NOTE: If a record is known to contain patently false information as a result of a previous review, and has already been disclosed, a CP could elect to flag it as such for future processing
5. **“Clear cut” TM claim**
   1. Trademark Owner of "<Example Trademark>" submits a request for RDS data supporting a trademark infringement and justifies its need/necessity to get access to Registrant RDS data in order to determine whether to file a claim or take lighter action
      1. The trademark exists in the Trademark Clearinghouse (TMCH)
      2. The trademark must be “live” (not just applied for, rejected or expired)
   2. TM owner has proved it has "agency" to request this data
      1. The owner of the TM, or
      2. Entity acting on behalf of the owner
   3. Limits
      1. The trademark string is of sufficient length/complexity that collisions with non-trademark strings is very unlikely (e.g. “microsoft”)
      2. The domain name non-public registration data requested is identical with the trademark, or the trademark is a prefix, infix or suffix of the domain name
      3. Automation would not work for figurative marks or where the domain name is allegedly confusingly similar to the trademark.
      4. The Gateway can apply a published algorithm to ensure that recommendations are generated consistently
6. **Request for data from ICANN Compliance**
   1. In order to investigate *[something that is allowed and specified in ICANN's role as controller]* ICANN requests RDS data for a domain name under investigation, such as auditing, validity of name holder, compliance with other laws, (i.e. accuracy under Art. 5 GDPR)
   2. ICANN must agree to be a controller for the purpose of this processing.
   3. ICANN must warrant that the data will not be used in a way that has legal or similarly significant effects on the data subjects
7. **Identify infrastructure involved in botnets, malware, phishing, and consumer fraud**
   1. Requestor is accredited as a cybersecurity professional and has agreed to comply with specific cybersecurity codes of conduct, if applicable.
      1. Not everyone can simply assert that they are such a professional.
   2. Requestor represents that it has investigated and confirmed that the domain name is being used as part of a criminal infrastructure.
      1. Direct evidence can also be included in the request - based on the Request contents building block.
   3. Requestor asserts that the data will not be used in a way that has legal or similarly significant effects on the data subject.
   4. Data to be used in a way that has legal or similarly significant effects on the data subject will require a separate request.
8. **Data subjects have consented to make their registration data public**
   1. See Phase 1 policy Rec #6.
   2. Given the complexities of compliance tracking, it probably only makes sense for the CP to flag this locally to avoid synchronization issues between Gateway and CP.
9. **Request for data from a UDRP/USR Provider.**
   1. UDRP or URS Provider has received a UDRP or URS filing for the domain name.
   2. The Registrar must provide the UDRP or URS Provider with the information requested in the verification request, per section 4(b) of the Rules for Uniform Domain Name Dispute Resolution Policy. (https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en)