Use Cases That Support Automated Disclosure Decisions

Assumptions:

1. All requests have been accredited by Accreditation Authority
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 CPH) has access to the data required to make the decision.   (At a minimum the Public RDS/WHOIS data they collected per Phase 1 Policy).

Disclosure response to all of the following use cases can be automated and result in an automatic disclosure response.

**Use Case 1 - LEA in same jurisdiction as CPH**

* Law Enforcement Agency from Jurisdiction A requests Registrant RDS data from a Registrar also in Jurisdiction A.
* In some cases, this might benefit from access to the City field

**Use Case 2 - Straightforward/"clear cut" TM claim**

* Trade Mark 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
* It is assumed that the TM owner has proved it has "agency" to request this data as it is either the owner of the TM, or acting on behalf of the owner.

**Use Case 3 - Request for City Field**

* Cybersecurity researcher submits a request for the City field (only) in order to ascertain which specific jurisdiction to make a legal claim.

**Use Case 4 - Request for data from a UDRP/USR Provider.**

**Use Case 5 - Request for data from ICANN Compliance**

* 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)
* ICANN must agree to be a controller for the purpose of this processing.

**Use Case 6 - Request for data from a European DPA**

* Responding to a request from a Data Subject that their data is being misused in violation of the GDPR, a European DPA files a disclosure request to ICANN/CPH for additional information.

**Use Case 7 - TLD used only for Legal Entities**

* Responding to some TLDs should be automated because they limit their customers to legal entities and have their own policies. See .BANK, .INSURE, .MUSEUM, and others.

**Use Case 8 - TLD used only for Self-regulating Entities requiring Contact Disclosure**

* In many places lawyers and realtors are obliged to freely publish contact data.  See .LAWYER, .REALTOR
* I don’t know if these TLDs have a policy in place already mandating disclosure of registration data, but it would be reasonable to contact them to discuss.
* Note that these TLDs will contain both natural and legal registrants, but if the policies of the TLD mandate disclosure the disclosure will be automatable.

**Use Case 9 - TLD is registered to a legal person and has already been disclosed for that reason**

* An automation system can flag that a registrant is a legal person so that data can be automatically disclosed if the ownership has not changed.
* The flagging could be done either at the CP or at the Gateway, if submitting that info is supported by the feedback system
* Presumably a registrar could flag a domain name at the moment that the data is collected to enable later automation, but this is an optional implementation decision.

**Use Case 10:  WHOIS record has patently false information and has already been disclosed**

* An automation system can flag that the data has already been reviewed and that the records have not been changed since that disclosure.

**Use Case 12: Identify owner of abusive domains involved in botnets, malware, other fraud**

* Requestor is accredited as a cybersecurity professional and has agreed to comply with specific cybersecurity codes of conduct, if applicable.  Not everyone can simply assert that they are such a professional.
* Requestor represents that it has investigated and confirmed that the domain name is used to deliver malware. [Direct evidence can also be included in the request - based on the Request contents building block.]

**Use Case 13: Phishing with Trademark Infringement in Domain Name**

*Requestor Safeguards*

1. Accreditation Authority determines that the trademark is valid.
2. Accreditation Authority determines that Requestor is the legal owner, agent, or service provider of the trademark.

*Request Safeguards*

1. Requestor alleges that the domain name infringes Requestor’s trademark.
2. Requestor alleges the domain name’s use in a phishing attack.
3. Requestor states its own legal basis and purpose for processing the data. Requestor makes all representations required by policy: use limited to stated purpose, data retention, etc.
4. Domain string contains exact match of trademark string (potentially including prefix or suffix, e.g. “nike-shoes.TLD” or “login-nike.TLD”).

*Additional Safeguards*

1. Registrant committed not to infringe on the rights of third parties in its registration agreement, as required by the RA and RAA.
2. Registrant was informed at the time that its data was collected that it could be processed for third-party purposes, including intellectual property protection and cybersecurity.