

RDS PDP WG – Drafting Team 6: Legal Actions

Purpose Name: Legal Actions

Definition:

The “legal actions” purpose of RDS includes assisting certain parties(or their legal representatives, agents or service providers) to investigate and enforce civil and criminal laws, protect recognized legal rights, address online abuse or contractual compliance matters, or to assist parties defending against these kinds of activities, in each case with respect to all stages associated with such activities, including investigative stages; communications with registrants, registration authorities or hosting providers, or administrative or technical personnel relevant to the domain at issue; arbitrations; administrative proceedings; civil litigations (private or public); and criminal prosecutions.

Tasks:

1. Identify registrant contact information associated with a domain of interest for potential legal action
2. Use of reverse query to identify and combat use of fraudulent contact data in a domain registration
3. Access and review historical domain name registration associated with a domain of interest for potential legal action
4. Use of reverse query to identify all domains registered with a given name or address associated with a domain of interest for potential legal action
5. Identify registrar, registry and IP address/es associated with the domain of interest

Users:

These include:

- Individuals or entities (or their representatives) who have been victim of harm / wrongdoing associated with the domain of interest
- Individuals or entities (or their representatives or service providers) who are concerned that their name, address or other contact information has or will be used fraudulently by a third party to register a domain or obtain other services
- Intellectual property owners (or their representatives or service providers) in order to investigate and enforce their rights where infringing activity is associated with the domain of interest
- Operational security, anti-abuse, merchant monitoring service or domain reputational professionals (or their representatives or agents) in order to investigate and respond to potential abuse including escalating same to possible civil or criminal enforcement
- Non-LEA governmental agencies to investigate and enforce civil violations of law associated with the domain of interest
- LEA, prosecutors, or other governmental actors to investigate and enforce against possible criminal activity associated with the domain of interest or its registrant. This has been used, for example, to investigate cybercrimes, money laundering, and sexual exploitation of children. There is also anecdotal evidence of LEA in certain countries using registrant data to investigate and/or prosecute possible crimes committed by journalists or protesters who have registered the domain of interest, such as blasphemy.

- A person or entity (or their representatives) in order defend a claim related to one of the aforementioned types of legal action for purposes of due process, to provide exculpatory evidence, etc.
- Legal counsel, their clients, and their respective authorized agents.

Data:

These include the following, both for use of the individual data item and to aid in determining attribution and correlation to other relevant data as necessary to support the purpose

Data Element	Purpose
Domain Name	Confirm domain name is registered.
Registrant Name	Ascertain registrant identity, including to help determine the relationship between the registrant and the potential legal action.
Registrant Organization	Ascertain if registrant is a legal person, or is an individual registrant affiliated with an organization or legal entity.
Registrant Postal Address (street address, city, state/province, postal code, country)	Ascertain registrant location both for jurisdictional analyses as well as identifying relevant government or law enforcement agencies for criminal referral, as applicable. Used for service of legal process and providing correspondence and legal notices in hard copy by mail.
Registrant Phone	A means of contacting registrant beyond email or postal mail, if necessary, particularly for urgent requests.
Registrant Email	A means of contacting registrant in writing with legal action (where permitted in the relevant jurisdiction), or related inquiries or requests (cease and desist letters, informal notices of legal action, etc.).
Registrar Name	Identify the domain name registrar to determine jurisdiction of registration authority for various legal purposes (in rem actions against domain name, secondary liability, third party subpoenas, court orders obligating the registration authority to take action, etc.), or to contact registrar in connection with a takedown, hold, or lock request or other inquiry concerning the domain name.
Registrar Abuse Contact	See above.
Original Registration Date	The date on which this domain name was first registered. Generally helpful to establish rough timelines concerning the alleged harm / wrongdoing / illegal activity at issue, such as in a trademark enforcement context to determine if registration predated establishment of trademark rights. .
Creation Date	The latest time that the domain name was registered; it is possible that the domain name was previously registered and subsequently deleted multiple times. See above regarding Original Registration Date – helps establish timeline for purposes of enforcement or investigation into various forms of harm / wrongdoing / illegal activity.
Updated Date	Helps establish timeline for purposes of IP enforcement or anti-abuse investigation, including most recent renewal date or to signal other recent changes to registration data or domain status.
Registrar Expiration Date	Identify possible expiration or renewal date of the domain name, which may signal when the infringing, abusive or other illegal activity may cease (if

	domain is not renewed) or might become available for defensive registration and avoid need for further legal action.
Name Servers	Identify whether domain name is associated with any content, and if so, identify the specific IP address(es) and hosting provider(s) in order to contact hosting provider with takedown requests or other inquiries relating to the domain/website helpful to enforcement one's rights, mitigate the harm, and/or further investigate the alleged harm / wrongdoing / illegal activity.
Technical Contact Name / Organization / Email / Phone	Identify technical contact for anti-abuse response or to investigate or address the forms of harm / wrongdoing / illegal activity that are technical in nature
Administrative Contact Name / Organization / Email / Phone	Identify administrative contact for anti-abuse response or other inquiries where there is no response from registrant (assuming there is a separate admin contact).

ANNEX A

The legal actions purpose generally includes the following tasks:*

Task	Description
<p>1. Identify registrant contact information associated with a domain of interest for potential legal action</p>	<p>Identify name, address, location, email address, phone, etc. of domain registrant to</p> <ul style="list-style-type: none"> • help identify the potential defendant / alleged wrong doer; • be able to contact registrant and for follow through; • determine the jurisdiction for possible civil litigation or criminal referral; • prepare for, and initiate a civil litigation, arbitration, UDRP/URS action, or similar non-criminal process; • prepare for, and initiate a criminal litigation or similar criminal process. <p>Such wrong doing / illegality may include consumer fraud or deception, unfair competition, passing off, intellectual property infringement, computer fraud and abuse, or similar activity where there is the possibility of a civil or criminal remedy to address the alleged wrongdoing.</p> <p>It may include civil action by private actors (such as consumer fraud claims or IP infringement claims), civil enforcement by governmental authorities (such as consumer deception, unfair competition, tax evasion, etc.), and criminal enforcement by LEA, prosecutors, or other governmental criminal enforcement agencies. In certain cases, such action might include pursuing individuals or organizations to suppress or prosecute acts of free speech, political activity, or acts deemed to be blasphemous under the laws of certain countries.</p> <p>It may also include other related uses such as UDRP/URS providers to confirm registrant details in a filed action, ICANN for contractual compliance purposes, and operational security professionals or domain reputational professionals who may escalate matters for civil or criminal enforcement.</p> <p>Such information is relevant for domain name arbitration or other legal proceedings; for purposes of due process and establishing jurisdiction, and contacting the registrant or their legal representative, prior to taking legal action and then taking legal action if the concern is not satisfactorily addressed.</p>

Task	Description
2. Use of reverse query to identify and combat use of fraudulent contact data in a domain registration	Identify and respond to fraudulent use of legitimate data for domain name registration by using a Reverse Query on identify-validated data. For example, this could include a legitimate registrant using such a query to identify if there are domains that are either registered to him/her/it that the registrant did not register, or that use the legitimate registrants address or other points of contact without authorization. This could also include investigation into the fraudulent use of a person/entity's contact information by another for a domain registration.
3. Access and review historical domain name registration associated with a domain of interest for potential legal action	Enable historical research about a domain name registration (whowas) to help identify persons/entities/locations that have historically been involved with a domain that is the subject of potential legal action
4. Use of reverse query to identify all domains registered with a given name or address associated with a domain of interest for potential legal action	Enable research into the potential defendant / alleged wrong doer to determine if the alleged harm / wrong doing / illegality extends to other domains registered to the name or address.
5. Identify registrar, registry and IP address/es associated with the domain of interest	Determine location/jurisdiction of domain name registration authorities and IP addresses/servers associated with the domain for purposes of <i>in rem</i> proceedings involving the domain alleged to engage in harm / wrongdoing / illegality and/or requests for third party subpoenas in connection with a civil action against the domain of interest or its operator.

** In each case, it is also possible to perform the task to refute a claim against a defendant in a legal action.*

RDS Purpose: Legal Actions

DT6 Answers to Questions – 3rd Draft for DT Review 5 Mar 18

From:

[file:///C:/Users/Owner/Downloads/DT6%20Deliverable%20for%20the%20Legal%20Actions%20Purpose%20\(Use%20Case\)%20-%208%20Nov%20171.pdf](file:///C:/Users/Owner/Downloads/DT6%20Deliverable%20for%20the%20Legal%20Actions%20Purpose%20(Use%20Case)%20-%208%20Nov%20171.pdf)

Definition: The “legal actions” purpose of RDS includes assisting certain parties(or their legal representatives, agents or service providers) to investigate and enforce civil and criminal laws, protect recognized legal rights, address online abuse or contractual compliance matters, or to assist parties defending against these kinds of activities, in each case with respect to all stages associated with such activities, including: investigative stages; communications with registrants, registration authorities or hosting providers, or administrative or technical personnel relevant to the domain at issue; arbitrations; administrative proceedings; civil litigations (private or public); and criminal prosecutions.

1. *Who associated with the domain name registration needs to be identified and/or contacted for each purpose?*

- To determine if a legal action may be warranted, legal entities may need to identify and possibly contact one or more of the following:
 - a. The person or entity that currently owns the rights to the domain name or the rights holder’s designated representative; this could be the registrant or the domain name’s current user as in the case of a privacy or proxy service via a relay service.
 - b. The registrar and/or reseller with whom the rights holder has a registration agreement for the domain name.
 - c. The domain name registry for the associated top-level domain.
 - d. Operator of domain name server(s)

Comment [O1]: Note that the operator of the domain name server(s) is not a currently collected data element for Whois. But name servers are collected and they can possibly be used to identify the operator of the servers.

2. *What is the objective achieved by identifying and/or contacting each of those entities?*

- The objectives of identifying any of the entities listed for question 1 above are:
 - For a: to determine who is the authorized holder of the domain name registration and what is that entity’s legal jurisdiction.
 - For b: to determine what registrar entered the domain name into the applicable top-level domain registry and what is the registrar’s legal jurisdiction.
 - For c: to determine what registry entered the domain name into its top-level domain registry and what is the registry’s legal jurisdiction.

- For d: if possible, to determine the identity of the web hosting provider associated with any content located at the domain name and what is the hosting provider's jurisdiction
- The objectives for contacting any of the entities listed for question 1 above, if needed, are:
 - For a: To provide notification of any possible legal issues affecting the authorized holder of the registration and to confirm legal jurisdiction
 - For b: To ask clarifying questions about any possible legal issues and to confirm the registrar's legal jurisdiction
 - For c: To ask clarifying questions about any possible legal issues and to confirm the registry's legal jurisdiction
 - For d: If possible, to ask clarifying questions about any possible legal issues and to confirm the hosting provider's legal jurisdiction
 - For a, b, c & d as applicable:
 - To communicate possible legal actions under consideration such as but not limited to cancelling the domain registration, transferring the domain name or removing website content associated with the name
 - To provide official notification of final actions taken.

3. *What might be expected of that entity with regard to the domain name?*

- Domain name registrants or designated representatives would be expected to do any or all the following as applicable in response to requests from legal authorities:
 - Confirm they are the authorized holder of the domain name registration
 - Identify their legal jurisdiction
 - Ask clarifying questions about issues identified by the legal authority
 - Respond to questions asked by the legal authority
 - Provide relevant information to assist the legal authority in their deliberation
 - Take other specific actions as requested or directed by the legal authority" for each of the categories
 - Appeal actions taken by the legal authority.
- Domain name registrars would be expected to do any or all the following as applicable in response to requests from legal authorities:
 - Confirm they are the registrar of the domain name registration
 - Identify their legal jurisdiction
 - Ask clarifying questions about issues identified by the legal authority
 - Respond to questions asked by the legal authority
 - Provide relevant information to assist the legal authority in their deliberation
 - Appeal actions taken by the legal authority.
- Domain name registries would be expected to do any or all the following as applicable in response to requests from legal authorities:
 - Confirm they are the registry of the domain name registration
 - Identify their legal jurisdiction

- Ask clarifying questions about issues identified by the legal authority
 - Respond to questions asked by the legal authority
 - Provide relevant information to assist the legal authority in their deliberation
 - Appeal actions taken by the legal authority.
- Domain name registrants (or designated representatives), registrars or registries would be expected to respond at their discretion to communications from entities seeking civil or prior to litigation relief. Respond doesn't mean to comply with the request, but rather acknowledge the request and let the requestor know what action, if any, will be taken.

DT6 Legal Actions – Slide 10

- DT6 answers introduced by Griffin –
- Focus is on contracts between private parties (i.e., not contracts with ICANN)
- Possible to accomplish 2d) using IP addresses associated with domain names or Nameservers
 - DT6 had agreed to replace “hosting provider” by “DNS operator” throughout answers
 - Nameserver does not always lead to responsible party – investigative value
 - Why does DT6 (3) refer to “Legal Authority” is communication is between private entities?
 - Answers cover both cases where private entities initiate communication (e.g., a private corporation pursuing a legal action), and also cases where legal authorities have gotten involved in investigating allegations
 - Contacted entity may be more likely to respond to a legal authority than private party – see last bullet under question 3
 - Contacted entity may be under no obligation to respond
 - Some feel that “Legal Action” is too broadly defined