The Palage Differentiated Registrant Data Access Model (aka Philly Special) - Version 2.0

Executive Summary

This document summarizes a proposed differentiated access model for third parties to access non-public registrant data associated with domain name registrations consistent with the feedback provided by the European Union and the Article 29 Working Party, now the European Data Protection Board. Unfortunately, almost the entirety of the debate within the ICANN community--including ICANN's recently filed lawsuit in Germany against a registrar–has been devoid of any discussion of providing legal recourse to negatively impacted Data Subjects. While there are clearly legitimate interests for qualified third parties to access non-public registrant data, there needs to be a framework that balances these interests with those of the data subjects and the registrations authorities, who are looking for business certainty as to their data privacy rights.

This model also seeks to invert the current hierarchy in which Data Subjects are at the bottom of the hierarchical pyramid, need to pay additional fees to secure basic privacy rights, and have little recourse against third parties that violate those privacy rights. The new framework instead places the Data Subject at the apex, provides basic privacy rights at no additional cost, shifts the economic burden and legal accountability to those seeking access to these records, and most importantly provides Data Subject with legal recourse against those that violate their rights.

Definitions

Registration Data Directory Service (RDDS): The provisioning of registration data associated with a domain name registration, historically referred to as the Whois service.

Data Subject(s): Any natural person.

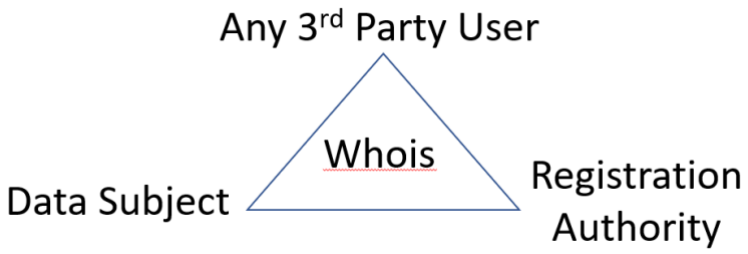
Legitimate Interest User(s): Any third party having a legitimate interest as defined by the ICANN community as part of a proper data privacy impact assessment seeking to access non-public personal data associated with a domain name registration.

Personal Data: Any information relating to an identified or identifiable natural person as set forth in Article 4, Paragraph 1 of the GDPR.

Registration Authority: Either a Registrar or a Registry Operator having a contractual relationship with ICANN.

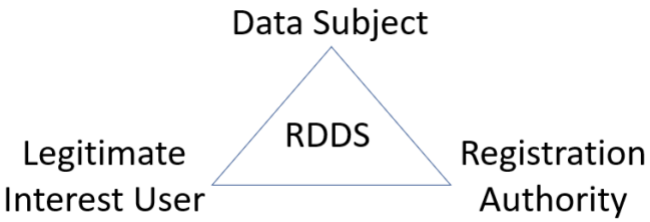
Current Market Inefficiencies/Inequities

The diagram below illustrates the inter-relation of the parties within the current Whois framework:



Unfortunately, there are several inefficiencies and inequities in the existing framework. The historic RDDS/Whois framework largely provided any third party, even those with an illegal intent, with the ability to access Personal Data about a Data Subject with little to no consequences. A Data Subject's primary recourse to avoid their Personal Data from being improperly use by a third party was to pay additional fees for a privacy/proxy service. Legitimate Interest Users—such as law enforcement, the intellectual property community, and the cybersecurity research community—struggled with a de-centralized system of Registrant Data that lacked a standard format, and in which significant portions of data they were trying to access was either shielded behind the privacy/proxy services or contained inaccurate data (often intentionally). Registration Authorities have been required to make this service available at no-cost to any third party, subjecting their customers (Registrants) to unwanted scams that have resulted in real and actual harm.

As discussed above, the proposed model set forth in this paper is about flipping the current hierarchy on its head and placing the Data Subject at the apex of the pyramid, as illustrated below:



RDDS Paradigm Shift

Instead of engaging in a clean-slate approach to RDDS/Whois, most industry participants have instead resorted to patchwork remediation of a fundamentally flawed system. Historically, both Registries and Registrars (Registration Authorities) have been obligated to provide RDDS/Whois access to any third party. This has enabled third-parties to freely extract Personal Data of Data Subjects from the RDDS/Whois. Self-attestation by these third parties is not viable because the only recourse against self-attesters that exceed the scope of their legitimate use and harm a Data Subject is the "threat" to have their future access cut off. This may prevent harm to other Data Subjects, but leaves impacted Data Subjects without an effective remedy.

Consequently, the cornerstone for any RDDS/Whois model lies in the ability to verify and authenticate Legitimate Interest Users. Considering the Hamilton memo that cited the direct privity of contract between Registrar and Registrant, it is proposed that Registrars be the sole gatekeeper via RDAP to provide RDDS differential access. This will enable Registrars to better protect their customers from unauthorized/excess access to their Personal Data using the audit features in RDAP. If there is a failure by a Registrar to provide timely access within mandated RDAP SLA parameters, then those Registries having "thick" registrant data could provide this service as an important failover.

One revolutionary proposed change is a new paradigm in which Registration Authorities (primarily Registrar or potential the Registry) may impose micropayments on Legitimate Interest User for the benefits they receive for access to this data. While RDDS/Whois access has traditionally been free, there are significant costs that Registration Authorities have had to bear in providing this service, and that Registrants have had to bear in keeping their Personal Data private. It is proposed that Registration Authorities be able to charge verified and authenticated Legitimate Interest Users for access to non-public Personal Data, rather than Registrants having to bear the cost of shielding their Personal Data by privacy/proxy services.

The original Philly Special proposal called for ICANN to verify individual Requestors (Legitimate Interest Users) using the CZDS platform. However, this thinking has evolved to permit the decentralization of the verification process to permit third-party organizations the ability to verify Legitimate Interest Users in various specialties (Intellectual Property, Cybersecurity, etc.) After verification, these Legitimate Interest Users would be assigned a digital identity with appropriate attestations of their access privileges. Transactions using these digital identities would be recorded on a permissioned distributed ledger maintained by Registration Authorities. These digital identities could be used to securely access the RDAP platform using multi-factor authentication while also permitting the ability to audit use of the system by Legitimate Interest Users. This system could also process micropayments for access to Whois data, and revocation of access for violation of predefined conditions.

If the verification of Legitimate Interest Users is the cornerstone of this proposal, the incorporation of an Alternative Dispute Resolution (ADR) mechanism is its keystone. This is the

mechanism by which a Data Subject can exercise their rights to challenge a Legitimate Interest User exceeding their access to the Personal Data of a Data Subject under this differential access model. This proposed ADR model (rules and policies to be forthcoming) is intended to be modeled in the spirit of ICANN's original Uniform Dispute Resolution Policy (UDPR). Under this proposal, Legitimate Interest Users would also provide a Financial Instrument (such as a Letter of Credit) to help ensure that Data Subjects could be made whole upon a successful ADR proceeding as described below in more detail.

While the GDPR was the impetus of this new paradigm model, it has the flexibility to handle other international privacy legislative frameworks. Like the ICANN UDRP model in which all domain name registrants are legal bound to a potential UDRP proceeding, all Legitimate Interest Users will be required to execute an access agreement that subjects them to ADR proceedings initiated by a Data Subject, as well as proceedings initiated by a Registration Authority seeking to revoke that user's access due to documented abuse.

Distinction from other Proposed Models

While most access models currently being contemplated within the ICANN community have spent an inordinate amount of time trying to differentiate **accreditation** for an exhaustive list of parties qualified to gain differential access, this proposal attacks the access model from an **accountability** perspective as detailed above. Regardless of how much time is invested in the compiling of lists and vetting requestors, there will undoubtedly be violations of the terms of use, and a Data Subject's Personal Data will be improperly processed. Therefore, the viability of any model is dependent upon placing the rights of the Data Subject at the forefront and ensuring that they are made whole in connection with any illegal processing of their Personal Data. Unfortunately, every model, including ICANN's Temporary Specification, have largely failed to provide any redress to the Data Subject who find their Personal Data improperly processed.

Key Components

Registration Authority – Registrars will be required to replace existing web based and port-43 Whois access with RDAP registrant data services in accordance with ICANN's Temporary Specification. Registrars will act as the primary gateway provider (Registration Authority RDAP) for differential access to non-public Personal Data via RDAP. Registrars will rely on digital identity credentials issued to Legitimate Interest Users. Registrars will also be responsible for hosting a node for the permissioned distributed ledger that will be used for verifying access transactions by Legitimate Interest Users and processing micropayments. Rights and obligations for access would be governed by an Access Agreement between Registrars and Legitimate Interest Users, along with the Registrar's Terms of Use and Privacy Policy. If a Registrar is unable to meet its RDAP SLA requirements, a Registry having access to the "thick" data would be designated to provide this service.

Data Subject – Because Registrars have direct privity of contract with the Data Subject, Registrars are best positioned to include in their standard registrant agreement the disclosed use of the Data Subject's Personal Information as part of this new paradigm. Data Subjects would also be a stated beneficiary of the Access Agreement between the Legitimate Interest User and the Registration Authority allowing them to initiate an ADR proceeding against the Legitimate Interest User.

Legitimate Interest User – This is the third-party seeking to access a Registration Authority (Registrar) RDAP service to obtain differential access to non-public registrant data. This party will need to enter into an Access Agreement with the Registration Authority (Registrar).

Financial Instrument – One of the key components to this model to help ensure that a Data Subject is made whole is the requirement that every Legitimate Interest User have a Financial Instrument in place prior to conducting any queries. The amount of the Financial Instrument will vary based upon several factors: estimated number of queries per month, number of individuals/organization relying on a given Financial Instrument, prior violations, etc. After publication of the initial draft, the author undertook outreach to various insurance underwriters inquiring about the potential of securing a performance bond. Given the non-traditional nature of this service, there currently does not appear to be a sufficiently diverse base of insurers to provide performance bonds for this type of service.

A more viable alternative may be a Letter of Credit based upon those currently held by those Registry Operators that were part of the 2012 round in connection with their Continuing Operations Instrument (COI). After some initial confusing within the banking community about issuing these instruments and their specific wording, ICANN, Registry Operators and the banking community have established a working understanding of the legal and operational parameters of the documents. Similar to the COI's, in which a triggering event is a declaration by ICANN that there had been a disruption of key registry services, the triggering event causing the release of funds to a Data Subject from the access-based Financial Instrument would be an adverse decision by the ADR Panel.

The initial deployment of this model may require Legitimate Interest Users to initially enter into multiple Letters of Credit. Ideally, as more Legitimate Interest Users enter into a common access agreement with Registration Authorities, a single Letter of Credit could be use to cover access across all signatories to that agreement.

Administrative Dispute Provider(s) – These would be qualified ADPs, like those that currently administer UDPR and URS complaints. However, these complaints would be purely GDPR based alleging that the Legitimate Interest User violated the terms the Access Agreement with respect to a Data Subject's Personal Data. During the initial launch, Registrars would be free to engage and enter terms with properly qualified ADRs. However, a preferred solution may be for the EDPB to coordinate this function.

European Data Protection Board (EDPB) – Under the powers granted by the GDPR, the EDPB could provide thought leadership in establishing best practices or certification frameworks for ADRs. Equally important, the EDPB could also provide guidance on decertification of ADRs if the quality of the decisions failed to meet certain standards.

Identity Providers (IDP's) - The digital identity credentials will be managed by third-party organizations that the ICANN community has collectively deemed authoritative. These organizations would be responsible for issuing digital identities having credentials for the respective access class (e.g. Intellectual Property, Cybersecurity, etc.) that would be used to authenticate access and to process micropayments.

Phased Implementation

The proposed model is designed to be implemented in either an incremental or comprehensive approach. Recognizing that certain aspects will have a longer lead time for implementation, other components can be rolled out first. In fact, this model can be implemented by individual Registrars one-off independently of any consensus/temporarily policy.The only elements that are mandatory for a base line implementation are discussed below in additional detail.

Consensus Policy Bootstrapping

The optimal way for Registration Authorities to solve this problem is by implementing this solution through their own initiative. This is exactly what Afilias and Neustar did back in 2008 when both Registry Operators filed simultaneously RSEPs for "Modifications to the Existing Add Grace Period" to address the domain name tasting problem that was plaguing the industry. After both Registries demonstrating the viability of their business solution, the solution was put forward to the GNSO as a consensus policy and was adopted by the ICANN Board shortly thereafter.

Unfortunately, this has been the rare except as opposed to the norm, as ICANN has experienced consensus policy paralysis over the past decade on a range of critical operational issues.

Organizational Overview