Before the

National Telecommunications and Information Administration, Department of Commerce

Washington, DC 20230

In the Matter of	)	
	)	
Introduction of Accountable	)	Docket Number: 230412-0009
Measures Regarding Access to	)	/ NTIA-2023-0006
Personal Information of .us	)	
Registrants	)	

Comments on the Introduction of Accountable Measures Regarding Access to Personal Information of .us Registrations

Introduction and Context

Edgemoor Research Institute is a non-profit 501(c)(3) organization that researches Internet registration systems. Its primary focus is the development of concepts and tools pertaining to DNS registration systems. The president, Stephen D. Crocker, was the founding chair of ICANN's Security and Stability Committee (SSAC). He also served on the ICANN Board from 2003 to 2017, first as a liaison from SSAC and then nine years as a director. For the last six-and-a-half of those years, he chaired the board, overseeing the recruiting of two CEOs and the transition in 2016 to independence from the NTIA agreement.

During this period, ICANN made multiple attempts to develop a coherent and effective WHOIS policy. These efforts stalled, partly due to conflicting goals and partly due to an incomplete understanding of the scope of the problem.

Edgemoor Research Institute has been researching the underlying components of DNS registration data collection and access. The comments offered here reflect the perspective Edgemoor has developed over the past few years.

EDGEMOOR RESEARCH INSTITUTE

Edgemoor Research Institute (ERI) facilitates the development and analyses of proposed and existing policies regarding the collection and access to registration data, including personally identifiable information. ERI serves the public interest by creating and promulgating concepts and urgently needed tools that provide precise specification of data collection, labeling, and access. ERI's goal is to bring together stakeholders from around the world, including non-profit, for-profit, government, end-users, and other stakeholders, to share knowledge and establish voluntary technical solutions to complex data-related public policy challenges.

For further information, see https://www.edgemoorresearch.org or contact Steve Crocker at steve_crocker@edgemoorresearch.org

Comments on the
Introduction of Accountable Measures Regarding Access to
Personal Information of .us Registrations

Basic Concepts

There are two parts to a registration data collection and request service. The first part collects and stores registration data. The second part, historically called the WHOIS service, receives and responds to requests for registration data. Each part embodies a significant portion of the overall policy.

The first part governs what data is collected, the degree of validation of each data element, and the level of sensitivity to assign to each data element. These decisions might be dependent on the type of registration. For example, the validation and sensitivity rules might be different for registrations of businesses ("legal persons") from registrations for individuals ("natural persons"), and there might be other distinctions as well.

We take a broad view regarding the data that are collected (or generated) during the registration process. In particular, the Account Holder has an account with the Registrar and creates the registration. The Account Holder may or may not be the same as the Registrant. Payment information and details about the location of the Account Holder at the time of registration are usually known only to the Registrar and not the Registry. This data is of great importance to law enforcement in certain investigations but would not normally be provided to other Requesters even if they are otherwise authorized to receive non-public information.

The second part governs which requests will be honored and which data will be returned if the request is honored. In keeping with the comment above, different Requesters are likely to be permitted to receive different portions of the overall registration data. This leads to three general principles.

Principles

1. Take a holistic view of the data collected and generated during registration. It is more than just the contact details for the Registrant.

2. Design and build the system with a clean separation between mechanism and policy. Policy decisions should be configurable and not embedded deeply into the design and operation.

3. Take a unified view of the request process. Internally, general requests from the public, authorized requests for non-public data from non-governmental Requesters, and authorized requests from law enforcement agencies and courts should be accommodated through a uniform interface.

   It may be desirable to present a simplified user interface for those uses that require little or no detail about the Requester. Still, such simplifications should be provided as a mild improvement at the user interface level, not a distinct part of the system design.

SPECIFIC ADVICE

1. Insist on the accuracy of the data that are collected. Continue to prohibit privacy/proxy services. Protection of privacy should be handled by controlling who gets to see what data, not by obscuring the data during the registration process.

   In addition to prohibiting privacy or proxy services, set specific standards regarding the accuracy of the data and what methods of validation are to be employed to ensure accuracy.

2. At the time of registration, determine whether the registration belongs to a natural person, a legal person, or is unknown. As a separate, although closely related matter, also determine whether the registration contains personally identifiable information (PII). As noted above, the registration system should make it possible to have different rules for different classes of Registrants.

   For registrations where it is unknown whether the Registrant is a natural or legal person and for registrations where it is not known whether the registration contains PII, choose whether to treat the registration as equivalent to a legal person with no PII.

3. Treat each data element as having a level of sensitivity. The lowest level corresponds to the common notion of "public." Multiple levels above "public" are necessary because not all non-public data will have the same level of sensitivity. The sensitivity level can then be used as one of the controls for determining what data to return for different kinds of requests.

   - Name and address information for natural persons and/or registrations that contain PII might assign a higher level of sensitivity than for a legal person with no PII.

   - The system should also permit Registrants to adjust the sensitivity level. For example, a legal person might request their address data be treated as more sensitive than the default. The system should also permit Registrants to choose <u>less</u> protection than would normally be provided.

4. Repeating the third principle above, use a uniform access method for all requests – public, controlled, and law enforcement.

   - There is no need for a separate API interface for law enforcement, nor is there a need to separate requests for public data from requests for non-public data. Each request should include information about the Requester and their purpose as needed. Requests for public data may leave these parts blank, and the response will be limited to just the data that is deemed to be public.

     For the interactive interface, it may be desirable to provide a separate interface for requests that do not need full details about the Requester or the purpose of the request.

   - Every request, including anonymous public requests, law enforcement requests, and all other requests for non-public data, should be logged. The logging of sensitive requests, usually but not necessarily exclusively from law enforcement, will need to be maintained and protected separately. Notification of domain registrant should be provided for ordinary, non-sensitive requests.

5. The Registry will have contact data for the Registrant, admin, tech, and/or billing. The Registry will <u>not</u> have Account Holder, payment, IP address used during registration, etc. That information

will be available only through the Registrar. The system should therefore include an internal path to reach out to the Registrars.

6. In accordance with the Contractor's proposal, the system should support both requests for any of a set of pre-approved purposes and requests for additional ("ad hoc") purposes.

    - The solicitation suggests the system will have only one class of non-public response. This is too limited. The system should be designed to provide a variety of levels of detail. For example, for some purposes, only a limited portion of the address, such as the city and state but not the street address, might be appropriate. Repeating the second principle, the system should have a clean separation between policy and mechanism, and it should provide controls for tailoring what data is returned for different classes of requests.

    - The requirements for access for pre-approved purposes may vary with the purpose. For example, the quality of the identification of the Requester and the level of authentication of the agreement with the terms of service might be tighter for some types of requests.

    - Requests for purposes not configured in the system or by Requesters not previously authorized to make the request will generally require manual review and decision. The system should include a pathway for such requests.

      Some ad hoc requests will be approved as is. Some ad hoc requests will lead to a decision to add to the list of pre-approved request purposes. Some may lead to both.

7. The system should provide a search capability. For example, the system should make it possible to request data on all registrations that have a specific name or email address.

8. The system should provide an application program interface (API) for submitting requests and receiving responses. This feature is important to facilitate integration into the Requester's system. Web-based and email-based interactions should also be supported, but the basic system design should be API based.

9. To facilitate transition, the sensitivity settings for existing registrations should be publicized in advance of the transition, and existing Registrants should be given an opportunity to adjust their settings.

RESPONSES TO THE SOLICITATION QUESTIONS

NTIA seeks public comments regarding the proposed Accountable WHOIS Gateway System (System). Comments that contain references, studies, research, or other empirical evidence or data that are not widely published should include copies of the referenced materials with the submitted comments. While the public is welcome to submit comments regarding the questions below and other issues relating to the proposal, we ask that comments generally be limited to issues regarding access to WHOIS in the usTLD. Specifically, NTIA seeks input on the following questions:

Q1. In general, what are your views on the public availability of the usTLD domain name registration data to anonymous users? Has public access by anonymous users to usTLD registration data, especially personal information, resulted in exposing Registrants to spam, phishing, doxxing, identity theft and other online/offline harms? If such abuses have occurred, please provide illustrative examples. And, whether or not you are aware of examples of such abuse, do you believe that there is a significant risk of such abuse occurring in the future, if the current system remains unchanged (and if so, why)?

ERI: Newly registered Domain Names can be discovered by analyzing publicly available Zone File data, and once a newly registered Domain Name is discovered, entities can leverage protocols such as WHOIS and RDAP to query for underlying related Registration Data Directory Service (RDDS) data. This RDDS data includes the contact information of the Registry, the contact information of the Registrar, and both Personally Identifiable Information (PII) and non-PII data related to the Registrant, including email address, phone number, and physical address. While ICANN-regulated TLDs and most ccTLDs redact much of the Registrant PII data to support privacy laws and policies (e.g., GDPR, etc.), TLDs such as .US currently requires the full disclosure of this information, leading to rampant, automated, and oftentimes illegal use of the data. Simply by processing the .US Zone File, acquired by submitting a request to support@about.us, a bad actor can identify newly registered Domain Names, the time and date of Registration, the Registrar associated with each Domain Name, and the associated Registrant name, phone number, and email address.

With this information in hand, bad actors can and do target unsuspecting Registrants with a host of scams and unscrupulous offers for unsolicited services. As a single example of one type of the many possible abuses perpetrated by bad actors, these individuals or organizations run campaigns where they will fraudulently identify themselves as a "business partner" of the Registrar. In so doing, they promote their services, falsely claiming the direct endorsement of their services by the Registrar.

By leveraging non-PII and PII RDDS data elements, the bad actor can customize emails and phone calls with information that unsuspecting Registrants believe could only have been provided by the Registrar with whom they did business only minutes ago. This leads to a false sense of confidence in the bad actor, a negative customer experience for the Registrar who is wrongly accused of selling customer data, and is antithetical to the data privacy initiatives that are designed to keep the Internet and DNS healthy.

Q2. Do you believe the current system of anonymous access to usTLD domain name registration data should remain unchanged? If so, why?

ERI: No. A gated access System should be put in place.

Within the gated service, there should also be a category of requests that requires only the Requester's identity and agreement to abide by the terms of service. Such requests should require justification or a declaration of the purpose. This category will provide widespread access but still allow monitoring to detect patterns of abuse.

Q3. What legitimate purposes for access to usTLD domain name registration data should be included in the System's pre-defined list? Please provide a rationale for each category recommended.

ERI: A few purposes and a few classes of Requesters are easy to list. However, we believe the future will bring additional purposes and new types of requests and requestors.

The system should be designed and operated in a way that anticipates and facilitates incremental addition of new purposes and new classes of Requesters as part of its ordinary operation.

Among the obvious candidates for initial inclusion are public safety officials in the U.S. or allied nations, intellectual property attorneys pursuing possible infringement situations, security researchers doing longitudinal studies, and security practitioners combating malware. Other uses, such as due diligence for mergers and acquisitions, etc., will emerge over time.

Q4. Are there policies and practices developed or employed by other ccTLDs regarding WHOIS access that could be incorporated into the usTLD space? Please be specific in your response.

ERI: We don't have data on the full range of ccTLD policies. It has been suggested that .DK, .NO, and the policies of several other ccTLD should be studied.

Q5. Should the System distinguish between personal and non-personal registration data, and if so, how?

ERI: The GDPR, which presumably doesn't control the policies for .us but nonetheless provides an important frame of reference, specifies a distinction between businesses (Legal persons)

and individuals (Natural persons.) It requires privacy protection for Natural persons, but it does not require comparable protection for Legal persons. Some privacy advocates argue that this distinction is not sufficient because the registration data for some businesses include personally identifiable information (PII) and thus should be protected.

We advocate incorporating the possibility of asking the Registrant whether the Registrant is a legal vs. a natural person AND whether the registration does or does not contain PII. These are two distinct questions. They are usually but not always related. Further, with those answers in hand, the protection of the registration data can be different depending on the answers.

Asking those questions raises additional questions as to whether the answers are accurate and what impact inaccurate answers might have. The key motivation for providing inaccurate data would be to gain a higher degree of protection than might be available if accurate data were supplied. How problematic would this be? Further, there are plausible situations where a business, e.g., an NGO operating in a contested area, might have a legitimate need for privacy even if no PII is involved.

A simple approach Is to have four levels of protection, ranging from none up to legal paperwork (warrant, subpoena, or equivalent) required, and ask the Registrant to choose which level they want. No matter which level they choose, the registration data will be available to at least some types of Requesters, with public safety officials being the most obvious.

In the work we've been doing, we use four levels of sensitivity for each data element. These are usually set in accordance with the classification of the Registrant. For example, a registrar can have one policy for natural persons and a separate policy for legal persons. In the natural person policy, the street address is set at a higher sensitivity level than it is in the legal person policy.

Q6. Should usTLD Registrants be notified when their data is accessed through the System? If so, why, when or in what circumstances?

ERI: For proper system performance, all requests and responses should be logged. Requests that are sensitive, e.g., law enforcement investigating a suspect, need to be curtained off from view. Other requests should be accessible to the Registrant. Whether the Registrant should be notified is a separate matter which involves trade-offs between the cost of operation and the impact on the Registrant.

Not all requests from law enforcement agencies are automatically sensitive, i.e., requiring

curtaining off from scrutiny. Conversely, it is possible some requests from other parties may require curtaining off from scrutiny. Requests should include a flag as to whether protection of the request is required, and the use of this flag should be part of the permission structure for the requests. This approach moves the protection of law enforcement requests up to the level of configuration management instead of a separate piece of the design.

The question of notifying the Registrant touches on a related but slightly different use of the registration data. The notion of a "data request" can be expanded to include other forms of requests. A Requester may wish to send a message to the Registrant even if they don't know who the Registrant is. Therefore, a simpler and more powerful way to think of a request transaction is that it causes any or all of three actions:

a. Returning information about the registration
b. Creating an accessible entry in a log
c. Sending a message to the Registrant.

Notifying the Registrant of a request and forwarding a message are both instances of the last.

As a separate matter, aggregate information about requests might be reportable on a regular basis. If such reports are not specific enough to identify individual registrations, there is no need to notify the Registrants.

Q7. Under what circumstances, if any, should the Contractor require certain requestors to furnish a warrant when requesting access to usTLD registration data?

ERI: If the Requester is properly identified and authenticated and has executed an agreement that spells out the circumstances under which it is sufficient for the Requester to declare a warrant exists, there's no need for the Requester to furnish the warrant as part of the request. Such an arrangement would need to be bolstered by audits and consequences for violations of the agreement.

Additional elements of this question are what data should be available with a warrant that is not available without a warrant and the converse, what data should not require a warrant.

Q8. The Contractor has proposed that the System provide special access to recognized and authenticated law enforcement and similar entities. Please provide feedback on this concept. If this proposal is adopted, how should it work? Are there best practices in other similar situations or other TLDs that could be used for such a special access portal? What

steps should be taken, if any, to ensure the confidentiality of law enforcement requests through the System?

ERI: The best way to provide special access is to make it part of the regular process, with the necessary privileges assigned to law enforcement and similar entities. There are myriad law enforcement entities. The privileges approved for, say, the FBI, may be much stronger than the privileges accorded an officer from a small-town police force in the U.S. or a federal official in another country. There will need to be a process for issuing credentials to agencies and even specific individuals.

One attribute of such credentials should be whether the Requester may request confidentiality. Requests requiring confidentiality require special handling. Such requests must be logged, but the log needs to be curtained off from regular access.

Q9. What entities in addition to law enforcement, if any, should have special access to usTLD registration data through an authenticated portal? Why?

ERI: As stated above, we believe there should be a unified portal capable of handling the full range of requests – public, non-public, and law enforcement. Authorization of other organizations to have the same access as law enforcement is a configuration decision and does not affect the design. Such decisions can be determined later. Further, it is likely that different law enforcement agencies will be granted different levels of access, with changes in authorization occurring over time.

Q10. What accountability and/or enforcement mechanisms should be put in place in the case of breach of the System's TOS by those that access the registration data?

ERI: Accountability and enforcement have two parts. The first part is the detection of abuses; the second part is the mitigation of the abuse. To detect abuses, regular audits and clear lines of communication for reporting abuses are needed. Mitigation depends on the severity of the abuse.

Q11. Do you foresee any challenges to implementation of the System, or elements thereof, for example in distinguishing between personal and non-personal registration data, enforcement of System misuse, etc? If so, how might these challenges be addressed?

ERI: The simplest and most direct way of distinguishing between personal and non-personal registration is to ask the Registrant during the registration process. Heuristic techniques,

e.g., the existence of an organization data element, can be used to form a reasonable guess, but the guess should be confirmed by the Registrant.

Q12. Should the Accountable WHOIS Gateway System be offered as an opt-in or opt-out service for current and new usTLD domain name Registrants?

ERI: This should be standard for all access.