Data Protection and Privacy

Issue Description

Whois records contain domain registrants' names, addresses, email addresses, and phone numbers. These details would be considered personal information in colloquial use and are provided legal protection in regimes that provide data protection to personal information. The fundamental question before the Thick Whois PDP WG is whether thin and thick registry models present different risks with respect to data protection and privacy. These risks might arise with respect to data at rest, information held in registry databases, and data in motion, records being transferred from registrars to registries in a thick model.

"Risks" include unauthorized disclosure in a security sense and issues related to information disclosure in violation of local law and regulations. The WG notes now that discussions of information security are oversimplified for purposes of clarity. Detailed risk analyses are beyond our ability given the complexity of issues and variety of possible system setups. As an example, we will focus on the necessity for data to be transferred in a thick Whois model. We do not discuss whether data may in fact move when a registrar in a thin environment has redundant systems.
As an explanation in advance, "data at rest" is information maintained in a system. "Data in motion" is information that is being transferred from one system to another.

Data Protection and Privacy in a 'thin' Whois environment

Data at rest: Information will be protected to the extent that registrars' security safeguards are in place.

Data in motion: Information is not transferred to registries in a thin model.

Data protection laws; Whois records must be made public under ICANN rules. At first glance, any applicable data protection laws will be the rules of the location of a registrar. However, it is conceivable that a registrant's location might be determinative where a registrant and registrar are not in the same jurisdiction.

Data Protection and Privacy in a 'thick' Whois environment

Data at rest: Information will be protected to the extent that security safeguards are in place in registrar or registry systems.

Data in motion: Information transfer introduces the need for additional security safeguards beyond measures required for data that remains with a registrar.

Data protection laws; Whois records must be made public under ICANN rules. Thick Whois models present additional challenges with respect to possible data protection conflicts. Do rules governing registrars apply because registrant contracts are signed in their countries, or does a registry's regime govern because the registry publishes the data? How relevant is the location of the registrant?

Possible advantages for Data Protection and Privacy in a 'thick' Whois environment

Data at rest: Whois databases would be held by the registry and not necessarily multiple registrars. This single point of failure instead of multiple ones would increase data protection. In addition, it may be that a registry, being in most cases larger than registrars, will be able to institute better security safeguards.

Data in motion: Thick registries provide no advantage in this category.

Data protection laws: To the extent that controlling data protection laws and regulations are deemed to be those of the registry, a Thick Whois environment will provide additional assurances where local rules limit information disclosure more

than in the locale of an applicable registrar. We must stress however, that any discussion of laws that might apply is speculation. It is beyond the ability of the work group to do an exhaustive review of applicable rules and contract provisions.

Possible downsides for Data Protection and Privacy in a 'thick' Whois environment

Data at rest: More copies of Whois records will exist. The level of risk will depend on decisions concerning, for example, who must maintain escrow systems, but registrars certainly still will have the Whois information even if it is not contained in defined Whois databases.

Data in motion: Thick Whois models introduce the necessity for data transfer, which requires additional security measures beyond what are needed for information that remains in a single system.

Data protection laws: As a counterpoint to possible increased legal protection when laws in a registry's jurisdiction are less information disclosure than an applicable registrant's, rules governing a registry's may in fact be less restrictive.. In addition, questions concerning whether registry or registrar location controls may add a level of complexity for the overall system and of confusion for a registrant.

Conclusion

Data at rest: We cannot identify an advantage between a thin and thick environment. The same information is contained in Whois databases in the two models. While ostensibly all Whois data as such will be in a single system in a thick environment, the data elements still will be kept by registrars. While more official copies of Whois information may exist in a thick environment, the fact is that bulk record access is available to the public and the likely magnitude of those copies in

the hands of individual analysts or of aggregators makes the discussion meaningless.

Data in motion: Again, we cannot identify an advantage for either model. On the surface, the need for Whois transfers from registrars to registries presents an additional point of data vulnerability and need for additional security measures. However, Whois information regularly moves through downloads and replication, as well as through transfer of data from registrars to registries in the existing thick registries . We find it hard to say that risks will increase at an identifiable level in a thick model over a thin one.

Data Protection Laws, or Welcome to the Rats' Nest: This subject is especially complex when it comes to drawing conclusions. It raises a level of complexities, uncertainties, and emotions that are beyond the ability of the WG to address conclusively given available resources and time constraints, and that also may spill beyond the bounds of the scope of this WG in the case of certain issues.

To begin with, thick registries have existed for many years, and .org transitioned from a thin to a thick environment. We have not been able to identify a formal analysis of data protection laws in the context of Whois information with respect to thin or thick models or the transition from one to another. We would hope that analyses have been done, and the fact that we can find no public objections from the registry or registrar community indicates that no problems have been identified.

In addition, we are not aware of any formal government actions against registries or registrars for maintaining Whois systems in accordance with ICANN requirements. In particular, no registrar has sought to adjust contract requirements pursuant to ICANN Procedure for Handling Whis Conflicts with Privacy Laws (http://www.icann.org/en/resources/registrars/whois-privacy-conflicts-procedure-17jan08-en.htm), which permits exceptions if a government begins an inquiry under data protection laws and regulations. Further, the comment on Thick

vs Thin Whoiis submitted by the Registrar Stakeholder Group did not raise privacy or data protection concerns.[

On the other hand, the fact that we have not seen analyses or objections from the contracted party community does not prove a lack of problems. In addition, data protection and privacy laws and regulations change over time so any analyses from the past might need to be revisited periodically. RSEPs initiated by .cat and .tel suggest that they have identified data protection and privacy legal issues that they considered valid even if no formal government action was initiated. As a final point, whether registrants are aware of the full ramifications of data publication, legal or real, might be questioned, and local rules concerning coercive contract provisions conceivably could come into play.

The Thick Whois PDP WG notes the increasing number of data protection and privacy laws and regulations around the world, as well as specific Whois-related concerns raised by the public. While recognizing that this suggestion may exceed the scope of our remit, we recommend that, as part of the development of the registration data directory system model currently in process, ICANN ensure that the ramifications of data protection and privacy laws and regulations with respect to Whois requirements be thoroughly examined. . We make these points as part of that recommendation:

1) Government inquiries can be expensive for a registrar or registy even if they do not lead to formal action. We suggest specifically that the procedures cited above for handling conflcts with privacy laws be reviewed to ensure that they can be invoked on the basis of documented and objectively well-founded concrete concerns about conflicts with local rules. Accommodations for conflicts between Whois requirements and data protection laws have been made without a requirement of law enforcement inquiry through RSEPs initiated by .cat and .tel;

2) Reviews of the relevant questions already are occurring, for example in RAA negotiations, and (we believe) in the development of the registration data directory service model referenced above. [It is the Work Group's understanding that the rules governing registrars have been broadened in the final draft 2013 RAA, but we have not seen the specific language] [Presumably we will be seeing this language very soon.];

Author
Comment [1]: This draft was completed before publication of the RAA late yesterday. This paragraph likely will need significant revision.

3) Examinations must include both data disclosure and data retention laws, as well as data quality requirements under data protection principles.;

4) Given the dynamic nature of laws and questions concerning what controls discussions, the examinations be limited to provisions that have the force of law at any given time or authoritative statements from relevant governments about those provisions. If a decision is made to examine broader frameworks, those analyses must focus on what exists, not changes that may happen.

5) Some level of real world review of the efficacy of data protection provisions must occur as part of any reviews. As examples, a) what
is the real effect of data retention provisions or b) do safe harbor laws really provide data protection assurances>

As a final note, the WG has made every effort to examine thin vs thick registry models in a broad sense. However, any requirement that all registries use the thick model will require that existing thin registries move to thick environments. This situation will raise concerns that, while limited in the long run, are significant given the numbers of domains and registrants involved. First, we expect that data transfers will be in volumes unprecedented in Whois operations. While the information does exist in many locations and data movement involving thin registry data occurs regularly, we urge that safeguards are put in place that are appropriate to handle the volumes.

Second, some registrations may occur after consideration of local rules governing a registrar or registry. In that event, registrants' data protection expectations will be affected when publication of Whois data moves to a registry that is in a different jurisdiction from the relevant registrar. Thorough examination must be given to the extent to which data protection guarantees governing a registrar can be binding on a registry. Any analyses also would be important for any cross-boundary registry-registrar relationship.

Again, these questions must be explored in more depth by ICANN staff and the community. As an added benefit, analyses concerning change of applicable laws with respect to transition from a thin to a thick environment also may provide valuable in the event that a registry's management changes, presumably an increasing likelihood given the volume of new gTLDs on the horizon.