To: Expert Working Group on gTLD Registration Data

From: ICANN staff

Date: 29 August 2013

Re: Data Protection Considerations Applicable to the Collection of gTLD registration data in the Proposed Centralized and Federated Database Systems

This memorandum addresses general principles of international data protection laws with respect to the use, processing and transfer of personal data in connection with the implementation of a centralized or federated Whois database replacement platform. It is intended as an overview of such principles and obligations, and addresses the following: (i) how and to what extent such laws may apply to the Whois database replacement platform administration, (ii) general obligations under data protection laws, (iii) how restrictions on international personal data transfers are implicated, (iv) consequences for data protection law violations, (v) implications to the implementation of a centralized or federated Whois database model, (vi) general considerations for the location of the Whois database replacement platform, and (vii) other relevant issues for consideration. Lastly, this memorandum concludes with some relevant questions to better understand how data protection laws may be implicated by the implementation and administration of the Whois database replacement platform.

The data protection topics addressed in this memorandum are intended to facilitate discussion concerning the development, implementation, and administration of the Whois database replacement platform, as well as possible requirements to be imposed on stakeholders in connection with gTLD registration data access and use. This memorandum does not provide specific legal advice or render a legal opinion upon which any specific future action or decision should be taken. Furthermore, the present analysis is provided without respect to decisions made or contemplated by the Internet Corporation for Assigned Names and Numbers (ICANN) and is neither a detailed nor complete analysis of data protection laws within any particular jurisdiction. Rather, general principles of data protection that may apply are addressed in the context of certain local data protection regimes.

I. BACKGROUND

ICANN formed an Expert Working Group on gTLD Directory Services (EWG) to help resolve the nearly decade-long deadlock within the ICANN community on how to replace the current Whois system. EWG's mandate is to reexamine and define the purpose of collecting and maintaining gTLD directory services, to consider how to safeguard the data, and to propose a next generation solution that will better serve the needs of the global Internet community. EWG began by exploring and questioning fundamental assumptions about the purpose, use, collection, maintenance and provision of registration data, as well as accuracy, access, and privacy needs. After working through a broad array of use cases, and the myriad of issues they raised, EWG concluded the current Whois model—giving every user the same anonymous public access to gTLD registration data—should be abandoned. Instead, EWG recommended a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use. EWG proposed that permissible purposes include domain name control, domain name research, personal data protection, legal actions, technical issue resolution, regulatory/contract enforcement, domain name purchase/sale, individual Internet use, abuse mitigation, and Internet services provision.

As a result, EWG is considering the implementation of a new registration data directory service and database to replace the current Whois database, using either a centralized or federated model. Under a centralized model, data would be copied to a single, centrally-located data repository where it then would be organized, integrated, and stored using a common data standard. Registrars would receive and transfer to ICANN (or the designated operator of the centralized database) data—namely domain registrations and associated information—such that only the centralized database would be queried directly. Under a federated model, individual source systems would maintain control over localized data, but each would agree to share some or all of its data to other participating systems upon request. A centralized system would receive all user queries but in turn would query the individual source system servers to obtain and return query results. Queries would be limited by the access credentials provided to the requestor, based upon the requestor's stated purpose.

II. GENERAL DISCUSSION

The selection, implementation and use of a specific Whois database structure (i.e., centralized or federated) should be informed by applicable legal principles of "personal data" protection. No uniform definition of "personal data" exists, though much of the information proposed for collection in the Whois database replacement platform likely satisfies even the most restrictive meanings of the phrase. For instance, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) defines personal information as information "about an identifiable individual," but does not include employee names, titles, business addresses or telephone numbers. The E.U. more inclusively considers any factor specific to a data object's physical, physiological, mental, economic, cultural or social identity. The United Kingdom's Data Protection Act 1998 (DPA) defines "personal data" as any data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. By contrast, the U.S. does not provide a single, uniform definition of personal data. Rather, its approach is based on a patchwork of laws regulating types of personal data generally, such as an individual's Social Security number, financial information, health information, certain government issued personal identification numbers, or other information likely to be involved in identity theft.

Complicating the Whois database consolidation effort are the various disparities between existing regimes. These differences in data projection regulation raise significant jurisdictional concerns, as well as potential regulatory obstacles on the global collection, processing, and transfer of gTLD registration data that need to be considered when structuring, implementing, and administrating the Whois database replacement platform.

1. Legislative Approach to Data Privacy and Protection - Jurisdiction

Generally, data protection and security regulations are territorial in nature. That is, in most jurisdictions that adhere to principles of international law concerning local jurisdiction, data privacy laws apply to an entity to the extent that it is reasonable and fair given the nature and extent of activities in that country. Hence, in most countries, local data privacy laws will apply to any entity purposely engaged in local activity involving personal data collection and

processing, or where a foreign entity uses equipment located in the country for data processing, and not merely to transmit personal data.

Notwithstanding the territorial nature of data privacy laws, many such laws have extraterritorial reach. In other words, such laws attempt to regulate the processing of personal data within and outside such jurisdiction, such as by requiring data owners to impose adequate data security obligations on processing of personal data outside the jurisdiction, whether such processing is done by an affiliate or third party. The data protection regime in the E.U., for example, applies to all personal data that is processed from within the E.U. by private organizations, regardless of the relationship with the data subject. This means that personal data collected outside of the E.U. that is then moved into the E.U. becomes subject to E.U. rules. Other jurisdictions have similar provisions in place. In Canada, for example, PIPEDA is silent with respect to its extraterritorial application, but it reaches organizations, data, or data transfers that have a "real and substantial link" to Canada, including to a foreign organization's collection or transmission of personal data of a Canadian subject in Canada.

The administration of the Whois database may thus implicate the laws of (i) the country where the Whois database platform is located, (ii) the country where the data owner/licensor/controller (controller) is located (i.e., where the registrar, registry, and possibly the Whois database administrator are located to the extent such entities dictate the processing of gTLD registration data), and (iii) the country where the data subjects (e.g., registrants) are located.

Ultimately, however, the controlling and most relevant law to consider is the law where the data subject (i.e., registrant) resides, as the ultimate goal of data protection laws is the protection of individual personal data. Hence, the application of data protection laws will depend greatly on (i) where gTLD registration data will be located, (ii) whether ICANN (or the entity administering the database) will be viewed as a controller or processor of such data, and hence have direct compliance obligations, (iii) the obligations imposed on registrars/registries under their agreements with ICANN with respect to gTLD registration data, and (iv) the extent to which local data protection laws apply to registrants.

2. Data Privacy and Protection Principles

A controller generally is defined in the E.U. and elsewhere as any entity that determines the purposes and means of processing of personal data, as opposed to a processor that generally is defined as an entity that processes personal data for a controller. This distinction is important, as controllers are required to comply with applicable data protection laws, and must impose certain data protection obligations on data processors. Processors are required to abide by the instructions of controllers. The restrictions imposed on controllers in collecting and making available personal data, as well as restrictions imposed on controllers in providing for adequate data security, differ by jurisdiction, as do obligations of processors. This will influence the data location and transfer considerations for the Whois replacement platform, whether as a centralized or federated model, and whether the Whois replacement database administrator and/or registrars conduct themselves as controllers in connection with gTLD registration data.

The most comprehensive data protection and privacy compliance legal framework remains to be the E.U. Data Protection Directive (E.U. Directive), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Each E.U. Member State has implemented the E.U. Directive through local legislation. Other, non-E.U. jurisdictions impose data protection obligations that are similar to the E.U. Directive. Still others allow for some differing approaches to standard data protection principles and, contrary to such principles, distinguish between such things as personal data collected for commercial uses as opposed to non-commercial uses and personal data transferred in business-to-business transactions as opposed to business-to-consumer transactions. Generally speaking, however, the E.U. Directive imposes the most comprehensive and stringent standards on data collection, processing, and transfers. The E.U. Directive, until replaced by a new proposed E.U. data protection regulation, serves as an appropriate baseline for global data protection compliance.

A. General Principles

There are some common approaches to data protection regulation. Generally, and by way of summary, data controllers must process personal data in accordance with the following relevant data privacy and protection principles:

- Purpose limitation: Personal data may be processed and subsequently used or further communicated only for legitimate purposes for which it was originally collected or subsequently authorized by the data subject.

- Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected, transferred and further processed.

- Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given.

- Security and confidentiality: The data controller must take technical and organizational security measures that are appropriate to the risks, such as measures against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

- Rights of access, rectification, deletion and objection: Data subjects must, whether directly or via a third party, be provided with the personal information about them that an organization holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles.

- Sensitive data: The data controller shall take such additional security measures necessary to protect such sensitive data in accordance with data quality requirements.

- Direct marketing: Where data is processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having the subject's data used for such purposes.

- Data retention: Personal data may be retained by the data controller and its agents for a period no longer than necessary to satisfy the purpose for which the data was collected or further processed.

- Accountability: Data subjects should have a method available to them to hold data collectors accountable for following the above principles.

Thus, under the above principles, the threshold questions for the implementation of the new global gTLD registration data database platform are: (i) who are the relevant data controllers in connection with gTLD registration data collection and processing, (ii) who, in the gTLD registration data database processing ecosystem, are deemed mere processors, (iii) what is/was the stated purpose at the time of personal data collection, (iv) what notices and consents were obtained as required by local law at the time of collection, and (v) how is compliance with data security safeguards, proportionality, legitimacy, accountability, and other data protection principles ensured.

B. Application Considerations

Notably, the purpose for which data was originally collected is of greatest import and impacts the application of the remaining data privacy and protection principles. For example, the E.U. Directive requires that personal data be collected only for limited purposes, that collected data be relevant to and not excessive *for the specified purpose*, and that it not be processed in a manner that is *incompatible with the specified purpose* or for longer than is necessary to *achieve the specified purpose*. Schedule 1 of the United Kingdom's DPA embodies these principles, as do obligations imposed in Germany, France and other E.U. Member States. Canada's PIPEDA similarly limits the collection, use and disclosure of personal data to that necessary for the identified purpose, unless the data subject otherwise consents. These limits can also be found in other jurisdictions whose data protection laws are modeled after the E.U. Directive.

Certain data protection regimes may view EWG's list of proposed permissible purposes—domain name control, domain name research, personal data protection, legal actions, technical issue resolution, regulatory/contract enforcement, domain name purchase/sale, individual Internet use, abuse mitigation, Internet services provision—as excessive in nature and an overly broad attempt to legitimize the collection of a large amount of data, expand processing of the data, extend data retention periods, etc. They also may require the use of less restrictive data collection measures to accomplish certain purposes, to include for example the maintenance of the domain name registrant's personal data by local Internet Service Providers (ISPs) at the ISP level in lieu of an international or regional data repository, and regular efforts to verify its accuracy. On the other hand, the purpose principle favors a proposed move away from anonymous public access to limited disclosure for permissible purposes only, especially if coupled with special efforts to eliminate bulk access for direct marketing and other impermissible purposes.

The purpose principle also requires among other things that personal data be destroyed after the purpose for which it was originally collected and processed no longer justifies continued maintenance. For example, if gTLD registration data was collected and processed merely to provide an up-to-date registry, it likely should be retained only for the period of the registration and then destroyed. If, however, another purpose exists, such as to prevent Internet crimes, then gTLD registration data may be retained for a longer period. But the adequate and timely destruction of all copies of a subject's personal data across multiple registrars is in part a technical concern that may inform the decision to use a centralized or federated model.

Lastly, as Data Protection Authorities are not likely to treat the implementation of a centralized or federated Whois database replacement platform differently from the operation of localized ccTLD registries, consultation with operators of those registries on their application of the principles highlighted above may engender goodwill and a consistent approach across all platforms in a given jurisdiction.

3. Restrictions on Personal Data Transfers

The E.U. Directive and local implementing legislation further regulate the cross-border transfer of personal data by entities that establish a presence in an E.U. Member State, even

within the same organization, and impose restrictions on transfers to jurisdictions, such as the U.S., that do not have "adequate" levels of data protection under local law. Only the following countries have been found to have adequate levels of data protection: Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States (Safe Harbor), and Eastern Republic of Uruguay. Transfers of personal data to such jurisdictions for processing are not prohibited under the E.U. Directive, but are nevertheless subject to other Member State's local data protection obligations (e.g., obligations to enter into a data processing agreement governing the transfer and processing under Germany's data protection law). Also, mere "access" to personal data located in a Member State from a foreign jurisdiction is deemed a transfer under local data protection laws.

Where the E.U. Commission has not found a foreign jurisdiction as having an "adequate" level of protection, it is illegal to transfer personal data for processing to such jurisdiction unless an adequate measure is imposed. Practically speaking, adequacy can be established in one of five ways: (i) the data exporter in the E.U. and data importer in the foreign country can execute Standard Contractual Clauses (SCC's) approved by the European Data Protection Commission; (ii) with respect to the U.S. only, the data importer in the U.S. can certify compliance with the U.S./E.U.-Swiss Safe Harbor Principles; (iii) the organization of which the data exporter and data importer are affiliated can implement so-called "Binding Corporate Rules" for the transfer and processing of personal data by the entire organization; (iv) approval of the transfer can be obtained from the relevant Data Protection Authority in each relevant E.U. jurisdiction, or (v) individual data subjects consent to the transfer. However, implementation of the Binding Corporate Rules and obtaining country-specific Data Protection Authority consent can be onerous and time consuming.

Other jurisdictions similarly restrict the transfer of personal data by controllers outside their jurisdictions without (i) data subject consent, (ii) a written agreement between the domestic controller and the foreign importer imposing data security obligations, or (iii) in limited cases, after certification of compliance to the relevant data protection authority. For example, in Japan, the rules for transfer of personal data under the Personal Information Protection Act are identical for both domestic and cross-border transfers. With few exceptions, an entity may not transfer personal data to any third party without the prior consent of the data subject.

The transfer of personal data from registrars to ICANN or the designated operator under a centralized model, or the sharing of data between registrars under a federated model, will therefore likely require data subject consent. Data transfers between ICANN or a designated operator and the registrars likely also require that certain contractual obligations be imposed throughout the system.

These restrictions on data transfers will impact the implementation of a centralized or federated model. A centralized model may reduce the number of requisite contracts and corresponding negotiations, though a master agreement in the federated model may achieve the same goal. Nevertheless, data transfer restrictions and obligations under various data protection laws will need to be addressed under either model.

4. Data Protection Violations

Certain data protection regimes hold controllers liable for violating local data protection laws. This is true in the E.U., Canada and much of Asia. Under Canada's PIPEDA, for example, data controllers are responsible for the security of personal data transferred to third parties and must take all reasonable steps to protect the data after transfer. In the United Kingdom, domain registrants have already consented to the transfer of data outside of the E.U. for the purpose of providing the Whois service, but Nominet, which manages the .uk ccTLD domain space, will nonetheless remain liable to the data subject for data breaches. In Hong Kong, any breach of data protection obligations imposed by the Personal Data (Privacy) Ordinance by any data processor outside of Hong Kong, be it ICANN, the designated operator, or another trusted agent, will be treated as a breach by the local registrar. In Japan, registrars will likely be held liable for the acts of delegates located outside of Japan and must ensure that such third-parties adequately protect data.

The obligations incurred by ICANN or a designated operator for the centralized database and the registrars therefore will depend on the specific design of the Whois database replacement platform, the choice of one of the proposed models over the other, the degree to which the registrars act with autonomy (e.g., as controller) under the centralized model, the degree to which ICANN or the designated operator directs the actions of the registrars under the federated model, and other considerations.

In a centralized model, ICANN or the designated operator could be regarded in the E.U. and elsewhere as a data controller. The degree to which a local registrar also would be considered a data controller likely depends on the ability of the registrar to act on its own discretion and for its own purposes in the collection and processing of personal data. In a federated model, the local registrar will likely be viewed as the data controller. The degree to which ICANN or the designated operator also would be considered a data controller likely depends on its ability to exert direction, control and influence over the registrars and personal data processing.

Penalties for violations can include regulatory fines, criminal sanctions, and injunctions on data processing. International transfers of personal data in violation of local data protection laws could also lead to an injunction on data transfers, hampering the effectiveness of the Whois database replacement platform. The availability of such penalties under local data protection regimes will potentially fuel local registrar/registry opposition to a Whois database replacement platform under either of the proposed models.

5. Location of the Whois Database Administration

The location of the gTLD registration data database administration will greatly influence the applicable restrictions on data collection and processing of gTLD registration data. For example:

- With respect to E.U. gTLD registration data, where the database is located in the E.U. and the centralized database is also located in the E.U., E.U. data protection laws will apply to all processing, whether done by the controller, a co-controller, or a third party processor (Whois administrator) on behalf of a controller. However, there will be no restrictions on the flow of such personal data within Europe.

- With respect to E.U. gTLD registration data, where the data originates from the E.U. and the centralized database is located in a non-E.U. country that is not deemed to provide adequate levels of protection by the E.U. Commission, transfers are permitted (i) with notice to the data subject, (ii) only after the E.U. controller has imposed adequate levels of protection on the data importer of the foreign country, or (iii) with

respect to U.S. importers, where such importer has certified compliance with the U.S./E.U.-Swiss Safe Harbor Principles. Certification to the U.S./E.U.-Swiss Safe Harbor Principles is not available to all U.S. companies and organizations. For example, not-for-profit organizations that are not subject to the U.S. Federal Trade Commission's enforcement jurisdiction are not eligible, a prohibition that can be avoided by leveraging contractual relationships with third-party entities that are eligible for the U.S./E.U.-Swiss Safe Harbor certification.

- With respect to other gTLD registration data (non-E.U.), if the centralized database is located outside of the country where the data subjects reside, the transfer will be permitted only under a written agreement between the exporter and importer. Such agreements will need to address adequate personal data security measures and restrictions on use.

Again, in some countries the transfer of personal data from registrars to ICANN or the designated operator under a centralized model, or the sharing of data between registrars under a federated model, likely will require the consent of the data subjects. Data transfers between ICANN or the designated operator and the registrars likely also require that certain contractual obligations be imposed throughout the system.

6. Other issues

Though beyond the scope of this memorandum, other potential issues exist. For example, various registrars provide an upgraded fee-paying subscription service that addresses personal data privacy. Such registrars may wish to continue to do so, a factor that may impact the data protection approach under the chosen model. Similarly, depending on the model selected, issues involving potential rights to data may arise. Finally, the revised Whois database will need considerable secure storage capacity. Cloud computing may introduce heightened data security concerns and complicate proportionality in processing, international transfer restrictions, and data storage.

III. CONCLUSION

The proposed implementation of a centralized or federated Whois database replacement platform necessarily impacts general principles of international data protection and privacy, including those previously discussed. To provide detailed and specific guidance, more information is needed concerning specific decisions and actions taken in developing the desired platform—namely, decisions concerning the exact structure of the new Whois database platform, its specific location, and the obligations that will be imposed on registrars and registries. For example, will the new database platform utilize a centralized or federated model? Where will the data repositories under either model be located? Must ICANN operate any centralized data repository that is located in the U.S.? Can it instead leverage existing contractual relationships to allow for operation by a Safe Harbor qualifying entity? What new requirements will be created for registrars, and will registrars have autonomous control over processing of gTLD registration data? What specific data will continue to be collected? How will data be securely stored? Are each of EWG's suggested purposes for data collection equally important? Can the stated purposes for collection and processing be reduced? How long will collected data be maintained? What are other envisaged data transfers (i.e., beyond transfers from registrars to the replacement platform)? How will data accuracy be verified? Will queries to the database involve the collection of additional data from the searcher, and will that data be processed? How will access to the registrant data be given? What technical processes will exist to maintain data accuracy, including allowing data subjects the ability to correct their data? Will the data collected include any sensitive data or topics?

While technical, political and other considerations will inform the implementation of the Whois database replacement platform, both models under consideration raise critical data privacy issues that must be considered.