GBOC

March 10, 2018

GLOBAL BRAND OWNER AND CONSUMER PROTECTION COALITION (GBOC)
COMMENTS ON PUBLISHED ICANN PROPOSED INTERIM MODEL FOR GDPR COMPLIANCE

Introduction

The Global Brand Owner and Consumer Protection Coalition (GBOC) is an organization of global businesses and brand owners working together to address common concerns in the online consumer and brand protection space. Current members of GBOC include Adobe Systems Incorporated, Facebook, Inc., Marriott International, Inc., and Verizon Communications Inc. GBOC has been closely following ongoing discussions within ICANN relating to the implementation of the EU General Data Protection Regulation (GDPR), particularly as it relates to access to WHOIS data. As you know, most businesses, brand owners, consumer protection agencies, law enforcement agencies and cybersecurity professionals rely on access to this data to perform a variety of key functions in the public interest. GBOC previously provided public input on the draft proposed GDPR compliance models, as provided by ICANN and the ICANN community. GBOC appreciates the opportunity to submit its additional input on the recently-published ICANN proposed interim model for GDPR compliance in relation to the WHOIS system.

GBOC Comments

1. Territorial Scope

ICANN's proposed compliance model ("the Model") would allow contracted parties to apply the Model globally, without regard to any data processing nexus to the European Economic Area ("EEA"). The GDPR only applies to data processing with a nexus to the EEA. Accordingly, the Model is substantially overbroad in territorial scope. ICANN must limit application of the Model to data processing with an EEA nexus, and specifically prohibit its application to data with no such nexus (such as where neither the contracted party nor the registrant are within the EEA). Such a distinction could be implemented through automated mechanisms using the registrant country, state/province, or postal code data to determine whether the registrant is an appropriate territorial subject. Of course, all EU-based contracted parties would apply the model regardless.

2. Material Scope

The Model would apply to all registrations, regardless of whether the registrant is a natural person or a legal person. The GDPR only applies to the personal data of natural persons. Accordingly, the Model is substantially overbroad in material scope. ICANN must limit application of the Model only to personal data of natural persons, and specifically prohibit its application to non-personal data and non-personally identifiable information associated with legal persons. Such a distinction could be implemented through automated mechanisms using the registrant organization field as a proxy to identify the registrant as a legal person, or through a checkbox self-identification mechanism (similar to what many European ccTLD managers have implemented). The Model would require the ability for registrants to opt-in to full

publication of their data regardless of whether they are a natural or legal person, so it would not seem substantially more burdensome to provide a mechanism for making this distinction up front as well.

3. Data Elements

a. Proposed Public Elements

The Model would permit general publication of Registrant Organization (if any), Registrant State/Province, and Registrant Country. We support general publication of these elements. However, we believe the Model should permit the general publication of several additional key elements, as detailed below.

b. Registrant City

The Model proposes that Registrant City be a non-public data element. Even in conjunction with the other proposed pubic data elements, Registrant City is not personally identifiable information. Registrant City is a vital piece of information needed to identify an appropriate venue when filing a lawsuit against the Registrant, which can be done even where the actual Registrant Name is unknown (and can be revealed through further legal process).

c. Registrant Postal Code

Similarly, the Model proposes that Registrant Postal Code be a non-public data element. Even in conjunction with the other proposed pubic data elements, Registrant Postal Code is not personally identifiable information. Like Registrant City, Postal Code can be used to identify an appropriate venue when filing a lawsuit against the Registrant, which can be done even where the actual Registrant Name is unknown (and can be revealed through further legal process).

Ultimately, Registrant City and Postal Code should be included as public data elements.

d. Registrant Email Address

The Model proposes that Registrant Email be a non-public data element. However, Registrant Email is the primary means of contacting the Registrant, and Registrant contactability, for a variety of legitimate reasons, is one of the fundamental purposes of the WHOIS system. Registrant Email is also generally used to correlate different domain name registrations to an individual registrant, again, a process that is used in a variety of legitimate contexts such as law enforcement, cybersecurity, and intellectual property enforcement and other consumer protection functions.

The Model proposes to replace the actual Registrant Email with an anonymized email or web form. These methods are inadequate for several reasons. First, they are unlikely to be timely and uniformly implemented across all registries and registrars. Second, neither of these methods would provide appropriate email “bounceback” information if the communication to the Registrant were to fail due to an inaccurate underlying Registrant Email or for some other technical reason. Third, neither of these

methods would enable cross-domain registrant correlation as described above. Accordingly, the actual Registrant Email should be preserved as a public data element.

We would consider supporting a pseudonymous (not anonymous) Registrant Email if it were: (1) public; (2) tied to enhanced accuracy (operational and syntactic) requirements for the entire WHOIS record; (3) unique to each individual registrant based on the underlying Registrant Email; (3) unique to each individual registrant based on the underlying Registrant Email; and (4) consistent across all registrations where the same underlying Registrant Email was used.

4. Non-Public Data Access

a. Self-Certification

The Model indicates, "Should the accreditation program not be ready to be implemented at the same time as the layered access model, some commentators have suggested 'self-certification' as an "interim interim" solution, however this would raise a number of questions that would need to be addressed to comply with the GDPR. This will be a continued topic for discussion in the coming weeks."

We support self-certification as a stop-gap mechanism for access to non-public WHOIS data for legitimate purposes (until accreditation is in place for pre-approved bulk access to WHOIS information for all legitimate interests or purposes). Some specific suggestions for an interim self-certification process were discussed in prior input to ICANN, including from the IPC and COA, among others.

b. Self-Certification Plus

The concept of "Self-Certification Plus" was discussed during the meeting between contracted party representatives and intellectual property and business stakeholder representatives that took place on February 21, 2018. "Self-Certification Plus" means that a party desiring to "self-certify" would specify third-party credentials that it has received consistent with the stated purpose (such as membership in relevant associations) in addition to certifying that it is seeking access to certain non-public data in connection with a specified legitimate purpose.

We also would consider supporting some form of "Self-Certification Plus" as an interim mechanism for access to non-public data if pure self-certification is not acceptable.

c. Accreditation Program

The Model proposes to use an accreditation program as a means for access to non-public data. ICANN has asked the Governmental Advisory Committee ("GAC") to assist in developing the accreditation system, including by providing a list of law enforcement authorities who would be "white listed" for full access. The GAC would also advise on other third-party user groups, such as cybersecurity professionals or intellectual property attorneys, who could be accredited. The GAC has also been asked to develop codes of conduct for the various approved user groups.

i. Accreditation

We agree that ICANN needs to quickly develop and implement a true accreditation program for access to non-public WHOIS data. Such a program will need to facilitate quick and adequate access for purposes of law enforcement, cybersecurity, and consumer protection including intellectual property enforcement. However, this kind of program will not likely be implementable prior to May 25, 2018. Accordingly, the types of certification discussed above should be considered as a stop-gap measure until a full accreditation program can be designed and implemented.

ii. Codes of Conduct

We support the need for individual codes of conduct, but codes of conduct should apply to all parties in the WHOIS ecosystem (including ICANN, registries, and registrars) and not just third-party WHOIS users.

iii. Timing

Some system for accessing non-public data must be in place as part of the interim model – this data cannot be made private without any mechanism for access from the start. An operational system for non-public data access must be in place or the proposed model cannot be implemented.

iv. ICANN's Data Access

Under the Model, ICANN will continue to have access to all WHOIS data. ICANN must confirm that its access will be complete and automated, with no restrictions such as rate limitations. ICANN must continue to use such unrestricted access to carry out all of its obligations and operations that currently use, access, or process WHOIS data, such as contractual compliance, internet security and stability, Accuracy Reporting System (ARS), and all other internal look-ups done in service of ICANN's current WHOIS related obligations and its mission to support the security, stability, and resiliency of the DNS.

5. Data Accuracy

The Model indicates that existing data accuracy requirement found in the 2013 Registrar Accreditation Agreement ("RAA") will remain in place as part of the interim model. We appreciate that ICANN has expressly confirmed that existing data accuracy requirements from the 2013 RAA will remain in place. However, the proposed interim model significantly hampers third parties' ability to identify inaccurate data (as most such data will be non-public if the Model proceeds as-is), thus severely undercutting ICANN's accuracy requirements. Accordingly, ICANN must require that registrars validate all registrant contact data at the time of registration as a component of the Model. More specifically, the interim model must require registries and registrars to perform additional operational and syntactical verification/validation of all registrant data fields at the time of registration and periodically throughout the life of the registration to ensure it remains accurate. Today's tools for registrant contact data verification and validation are insufficient and must be enhanced, using the techniques already deployed by ICANN in other systems (such as the Accuracy Reporting System). If registrars and registries are not

required to perform additional operational and syntactical validation, then ICANN must do it independently of the contracted parties as a joint controller responsible for the quality of data.

We note that the GDPR does not generally apply to data that is false, inaccurate or fictitious, and such data should be thoroughly screened out. We also note that contracted parties and ICANN, as joint data controllers and/or data processors, may face independent liability for persistent and pervasive inaccurate data.

6. Bulk / Aggregated Data Access

The Model indicates that "Registrars would continue to follow their current practice of providing third-party bulk access to the limited set of registration data that would be available to the public" but that "the status quo would be maintained in that additional bulk access, searchable or historical WHOIS data would not be required features." We appreciate the explicit acknowledgement that registrars would continue to provide third-party bulk access to public data. This must require that port 43 or an equivalent protocol will remain an integral part of the WHOIS system, without throttling limits that restrict the ability of legitimate users to access this information. Such access would, at a minimum, include all public data.

ICANN must also explicitly confirm, however, that third parties who become accredited or otherwise approved to also access non-public data would be able to then gain port 43 to access the full WHOIS data sets (public and non-public). Finally, while we understand that registries and registrars themselves would not have any obligation to provide searchability and historical data (beyond the life plus two year retention period), third party service providers could provide these features, subject to their own GDPR compliance obligations.

Finally, it is critical that once a model is implemented, ICANN will ensure that appropriate bulk access is actually being provided by all registrars and registries. If bulk access is required, but individual registrars or registries are permitted to unilaterally mask certain data or throttle the service, the entire purpose of the service would be completely vitiated.

We reserve further comments on these issues pending clarification from ICANN on these points.

We appreciate ICANN's consideration of this input, and GBOC looks forward to continuing to engage in this issue as the community drives toward an appropriately balanced interim GDPR compliance solution that preserves as much of the current WHOIS system as possible while complying with the requirements of the GDPR.

Respectfully submitted,

GBOC

March 10, 2018

Brian J. Winterfeldt

Counsel to the Global Brand Owner and Consumer Protection Coalition