January 29, 2018

GLOBAL BRAND OWNER AND CONSUMER PROTECTION COALITION (GBOC)
COMMENTS ON PROPOSED INTERIM GDPR COMPLIANCE MODELS

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 appreciates the opportunity to submit its input on the proposed interim models for compliance with ICANN agreements and policies relative to WHOIS in relation to the GDPR.

Executive Summary

GBOC supports ICANN's stated goal of ensuring compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible. We believe this goal can best be achieved if ICANN adopts its proposed Model 1 with certain key enhancements: (i) registrant e-mail address should also be a public data element, and (ii) third-party access to non-public data on the basis of a legitimate interest should be facilitated through an automated self-certification system that does not require case-by-case review and response by contracted parties. If such a lightweight self-certification program were problematic from a GDPR compliance standpoint, GBOC would support the accreditation/certification proposal in Model 2, assuming this could be timely implemented.

GBOC Comments

General Comments

ICANN has repeatedly stated that its goal in pursuing an interim compliance solution ahead of the May 25, 2018 effective date of the GDPR is to "ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible." We support this goal both for the immediate interim solution and any long-term solution ultimately developed through the appropriate ICANN policy development process.

In addition, we support the statement of purposes that ICANN has proposed for the interim models, which explicitly includes "issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection."

We support the understanding that registrars and registries should obtain full informed consent from registrants as a means by which they may lawfully collect, publish, transfer (e.g. to registries or data escrow providers), and retain registrant data.

We also note that none of the models appear to address aggregated (bulk) access to WHOIS data. Such aggregated data access is often critical to law enforcement, consumer protection agencies, brand owners and others who are seeking to connect the dots tying different domains and websites involved

in criminal activity, fraud or phishing, or wide-scale infringement to individual registrants. Accordingly, any interim model should incorporate guidance regarding aggregated data access.

In addition, none of the models appears to address data accuracy, even though data accuracy is a fundamental principle of the GDPR: "Personal data shall be: . . . accurate and, where necessary, kept up to date." *See* GDPR, art. 5(d). Again, mechanisms for ensuring data accuracy, to the extent possible, should also be an element of any interim model.

GBOC's Preferred Compliance Model

GBOC generally supports ICANN's Model 1. Importantly, Model 1 correctly limits the scope of protection under the GDPR to natural persons, and would not apply to the data of legal persons.

We also note that Model 1 would limit the territorial scope of GDPR as follows: (A) the registrar and/or registry are established in the European Economic Area (EEA) and process personal data included in registration data; (B) the registrar and/or registry are established outside the EEA and provide services involving the processing of personal data from registrants located in the EEA; or (C) the registrar and/or registry are located outside the EEA and process non-EEA personal data included in registrations, where registry and/or registrar engage a processor located within the EEA to process such personal data. We wish to clarify that the territorial scope of GDPR, which we believe Model 1 is intended to track, is to (1) "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not," and (2) "the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union." *See* GDPR, art. 3. It may be helpful to confirm that Model 1 would only apply within the limitations of territorial scope under the GDPR.

In addition, we strongly encourage ICANN to adopt the two specific enhancements to Model 1 discussed below.

1. **Registrant e-mail address should also be a public data element.**

One of the key elements in ICANN's WHOIS purpose statement is "[e]nabling a reliable mechanism for identifying and contacting the registrant." An e-mail address is the most important means of contact, particularly in the context of an online domain name registration service. Generally speaking, an e-mail address is also the registration data element that is most likely to be accurate given that it is needed for the registrar to communicate with the registrant and verify information necessary to complete the registration process. The registrant's e-mail address is the primary means by which intellectual property owners, for example, would attempt to contact a registrant regarding concerns of infringement.

In addition, Model 1 would include publication of the technical and administrative contact e-mail addresses. These contacts are often the same as the registrant, so it is unclear why GDPR would permit their publication while not permitting the publication of the registrant e-mail field.

Accordingly, registrant e-mail should be a pubic data element as part of the interim compliance model.

2. **Third-party access to non-public data on the basis of a legitimate interest should be facilitated through an automated self-certification system that does not require case-by-case review and response by contracted parties.**

ICANN's Model 1 proposes that:

> [t]o access registration data not published in the public WHOIS, registries and registrars would respond to requests from third parties on a timely basis. The requestor would be required to submit an application to the registrar or registry stating the specific purpose for accessing the data. The requestor would self-certify that the requested access is necessary for the purposes of the legitimate interests pursued by the requestor, and would self-certify that the data provided would only be used for the limited purpose for which it was requested. The registry or registrar would consider the request, taking into account the required balancing of interests under the GDPR.

Although we support, in principle, a self-certification process for access to non-public data, the mechanism proposed in Model 1 appears to be unnecessarily burdensome for contracted parties. Instead, we would recommend an automated self-certification system that would not require – or would only require very minimal - case-by-case review by the receiving registrar or registry. At a minimum, a system akin to the self-certification system currently in place for the ICANN Centralized Zone Data Service (CZDS), which permits bulk review and approval or denial of access requests, could be used.

If such a lightweight self-certification program were determined by EU Data Protection Authorities to be problematic from a GDPR compliance standpoint, GBOC would support the accreditation/certification proposal in ICANN's Model 2, assuming this could be timely implemented.

In either case, we support some form of accreditation or certification that would still permit quick and reliable access to non-public WHOIS data for legitimate parties who need such access – especially for law enforcement, cybersecurity, and consumer protection purposes.

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 GDPR.

Respectfully submitted,

Brian J. Winterfeldt

Counsel to the Global Brand Owner and Consumer Protection Coalition