COMMENTS ON THE HAMILTON LEGAL ANALYSIS

January 9, 2018

The Intellectual Property Constituency (IPC) of the Generic Names Supporting Organization (GNSO) is pleased to submit public comments on the legal analysis provided by the Hamilton law firm, as reflected in a series of three memos, including the proposed layered access approach to WHOIS in order to comply with the European Union (EU) General Data Protection Regulation (GDPR), as described in Hamilton's third memo. We have not confined our comments to the layered access approach since we believe Hamilton's analysis and advice should be approached as a whole. Please find our comments below.

Intellectual Property Constituency Comments

As a threshold matter, we agree with ICANN's goal of "ensur[ing] compliance with the GDPR while maintaining WHOIS to the greatest extent possible."[1] While we wish Hamilton's advice would have been sought sooner, we believe Hamilton has generally provided useful guidance to comply with the GDPR requirements while recognizing the wide array of important purposes, as well as public and legitimate interests, that warrant access to and processing of WHOIS data. With that in mind, our comments on the analysis provided by Hamilton in its three memos focus mostly on areas where we think Hamilton's guidance either strays from that goal or can be expanded upon to embrace more fully the goal of maintaining the current publicly availability of WHOIS to the greatest extent possible, consistent with privacy laws.

1. Purposes

We agree with Hamilton on the need to set forth more clearly and fully all the purposes for which WHOIS data is used and the legitimate interests served by access to such data. We also agree with Hamilton's guidance to assess and determine the extent to which personal data need to be processed for each purpose. We acknowledge that Hamilton's identification of third party purposes is similar to that of the ICANN Governmental Advisory Committee (GAC) and that we endorse all the purposes that the GAC described in its Communiqué of November 1, 2017. (Note that the GAC adopted this list by consensus, and that the European Commission and virtually all EU Member States are represented in the GAC.) We strongly support Hamilton's non-exhaustive list of legitimate purposes, which specifically includes: use by law enforcement

[1] ICANN, Data Protection and Privacy Update – Plans for the New Year (Dec. 21, 2017).

agencies to investigate and counter serious crime, terrorism, fraud, consumer deception, intellectual property violations or other violations of law; use by intellectual property rights holders to investigate intellectual property rights infringements; use by general public to verify the identity of a provider of goods or services on the internet, including for consumer protection purposes; and use by third parties in general to identify the owner of a domain for business purposes, for instance in relation to a purchase of the domain name or other transactions.

As the GAC clearly stated in its November 2017 Communiqué, fulfilling these important purposes would be best accomplished by:

"1.Keeping WHOIS quickly accessible for security and stability purposes, for consumer protection and law enforcement investigations, and for crime prevention efforts, through user-friendly and easy access to comprehensive information to facilitate timely action.

2.Keeping WHOIS quickly accessible to the public (including businesses and other organizations) for legitimate purposes, including to combat fraud and deceptive conduct, to combat infringement and misuse of intellectual property, and to engage in due diligence for online transactions and communications."

In addition, we note that Hamilton appears to assume that—at least with respect to natural persons—their interests are always in having as little information publicly available as possible. Hamilton seems to overlook the purpose/interest of registrants themselves in having certain of their data publicly accessible as a means of proof and notice of ownership, promoting trust of their website's users, and other similar transparency and contact ability interests. In this sense, Hamilton may be overlooking the legitimate interests of the data subjects themselves by focusing on the data minimization provisions of the GDPR.

2. Scope

Hamilton seeks to treat "all types of data the same" and therefore apply the GDPR to all data irrespective of whether it falls within the scope of data to which the GDPR applies. While we appreciate efforts to reduce unreasonable burdens on registrars, we disagree with this GDPR-maximizing approach. We believe it is reasonable for registrars to set up collection of a registrant's data in a manner that readily separates out data identifiable to natural persons from other data unlikely to constitute personal data under the GDPR (e.g., thin WHOIS data). Focusing only on data falling within the provenance of the GDPR strikes the right balance between maintaining current WHOIS while taking into account the requirements of privacy laws, consistent with ICANN's long-standing consensus policy.

3. Consent

Hamilton suggests that consent is not a practical ground for processing personal data. While we agree it would be imprudent to rely on consent alone, we think Hamilton has failed to recognize that registrants should have the right to choose, and may see it in their interest, to have their personal data made publicly accessible in order to have public proof/evidence of their ownership

of a domain name, to facilitate contact by users of the website, to facilitate transactions involving the purchase and sale of domain names, etc. Moreover, permitting registrants to give consent to making their personal data publicly available while informing them explicitly and upfront of the various purposes (including access by third parties for legitimate interests) serves the "informed consent" foundational principle of the GDPR. Informed consent—recognizing that it may be withdrawn—is another path towards retaining the fundamental structure of WHOIS and therefore should not be taken off the table.

4. Data Elements

Hamilton states that domain names themselves can constitute personal data (e.g., if they contain a name that can be linked to a natural person) and we disagree with that assessment. Domain names by their nature are public-facing. Indeed, their very purpose is to serve as guideposts for internet users, and as such, are an integrally public element of the DNS. This would be akin to regarding a brand which incorporates a person's name (such as Calvin Klein, Michael Kors, McDonald's) as personal data that must be subject to the GDPR, which is not logical or practically tenable.

Hamilton states in some cases information regarding a legal person could be considered personal data and an analysis would have to be carried out in each case. This seems overly cautious. At a minimum, Hamilton should provide additional analysis regarding mechanisms for avoiding such a characterization, such as through the use of generic e-mail addresses (e.g. admincontact@company.example).

5. Public Availability and Model Based on other Public Registers

We support Hamilton's approach of continuing to make a subset of WHOIS data publicly available, even when that data constitutes personal data subject to GDPR, to fulfill a reasonable balance of interests and fundamental rights and to serve overarching public interest goals, integrity and transparency, and security and stability. Indeed, we urge that ICANN focus on this approach first as both an interim solution and then a model to be vetted with a DPA as Hamilton has suggested.

As a starting point for such an approach, we believe that thin WHOIS data does not constitute personal data and should always be made publicly available.

Hamilton suggests only the name and physical address of registrants be made publicly available under this approach and specifically counsels to exclude e-mail address where the registrant is a natural person. We believe e-mail address is critical to include to fulfill not only the specified legitimate interests, but also the general public interests as well as the interests of the registrants themselves. In its first memo where Hamilton discusses a path forward of continuing to make certain types of personal data publicly available, Hamilton suggests consideration be given possibly to excluding phone numbers of natural persons (See Par. 3.9.4 of October 17 memo) We think Hamilton's guidance in the third memo of including only the name and mailing address

of the registrant in a publicly available directory is overly conservative and that further data elements need to be included.

First, we disagree with Hamilton's assessment in Par. 2.7.4 that email addresses are not necessary for the purposes listed in the memo at Par. 2.7.1 (i)-(v). Hamilton does not provide a justification for this conclusion, other than it would be "sufficient" to use the registrant's name and address to contact the registrant. Many, if not most, who use WHOIS to contact registrants do so via email addresses, and experience has shown that it is far more common for WHOIS to include a valid email address (which the registrant needs to be able to communicate with their registrar) than a valid physical address, which can change from time to time without the registrant updating their data.

Furthermore, one of the most vital functions of WHOIS for purposes listed in Par. 2.7.1(i)-(v) is being able to ascertain whether illegitimate activity is part of a pattern, through "Reverse WHOIS" lookups. This functionality would become far less accurate or perhaps impossible if only names and addresses can be searched. (Some registrants may have the same name, and there may be more variability between how the same address is represented in the directory, while an email address is a more reliable common thread to link a single registrant across different domains.)

But beyond investigation and enforcement with respect to illegal activity, e-mail addresses are vital for fulfilling consumer, user and general public interest objectives, including those identified by Hamilton in Par. 2.7.1 (iv) and (v)—ability of consumers to verify identity of the provider of online goods and service, and maintenance of a secondary market for the purchase of domain names. In fact a variety of public interests, such as mitigation against fraud, consumer protection, and transparency, cannot be adequately met absent the public availability of an e-mail address. E-mail is the normal and expected avenue via which users and consumers at large are able to contact the registrant of the domain name for inquiries, verification of services, qualifications of the provider of services/products, and the like. Finally, public availability of the registrant's e-mail address also serves the registrant's own interests in terms of proof and notice of ownership, contact ability and other interests as stated above in Section 1 of these comments.

Given the balancing of interests involved in assessing the appropriate data to publish in WHOIS, we think Hamilton's guidance is largely on the right path in its recommendation for putting into place a WHOIS register that follows along the lines of the EU trademark register and other public registers in Europe. In particular, we note that the legitimate purpose of enabling consumers to know (and to seek to contact) those they are dealing with online can only be effectively facilitated through some form of public register of information relating to domain name registration. For this legitimate purpose, it is particularly important that the public data set should include more than just the name of registrant and physical address and, at minimum, must include the registrant's e-mail address as well.

6. Layered Access

In its third memo, Hamilton seems to reject layered access as not "practically feasible" to fulfill the legitimate interests of third parties as described in Paragraph 2.7.1 and seems to embrace layered access solely for contractual administrative and data/disaster recovery purposes (and potentially law enforcement purposes, subject to certain limitations).

This is too narrow. We recognize that for some legitimate purposes (e.g., the consumer example above) it may be too difficult to craft a layered access approach; but for other purposes, including IP enforcement, we believe that layered access for third parties can co-exist with—and is a necessary complement to—a publicly accessible register of WHOIS data that is more restrictive than today's WHOIS directory. Thus, we suggest pursuing the register model of publicly available WHOIS data as suggested by Hamilton to the greatest extent possible, while embracing a model of layered access to personal data that is not publicly available to fulfill the legitimate interests of third parties, including IP rights owners, for which a more complete set of personal data is required in order to serve those legitimate interests.

We agree with Hamilton's guidance that court orders are not necessary for IP rights holders to be able to access registrant data to investigate and assess potential infringements. IP rights holders respect data privacy, but in order to protect their rights, and to avoid infringing third parties' rights, they must have ready and simple access to domain name registration data. Therefore, we think a layered access approach to serve legitimate interests, such as IP rights enforcement that does not depend upon court approvals and exists alongside a publicly accessible register of WHOIS data should be pursued.

Hamilton views "automatically qualified parties" as one problem with the layered access model. We suggest that for at least some legitimate purposes, a qualification system based on self-certification, with appropriate safeguards be considered. The assertion that layered access requires a hands-on assessment in each individual case needs critical review based on real-life considerations. We note that certain registry operators, such as Nominet, already use this kind of system.

We believe a layered access model can be constructed compatible with the GDPR that offers a one-time process to identify and "pre-clear" IP rights holders. Such a layered access model would need to offer fast, free and simple access to registrant data, including personal data, in order to make direct contact to resolve a potential infringement, but also to establish patterns of abuse, and, where appropriate to file UDRP complaints or other enforcement actions.

7. Data Retention

In its second memo, Hamilton stated that "as a general rule [personal data] must be deleted when the domain name registration in question ceases, unless the data for some reason is needed for a longer period for a specific purpose. . . ." (See Par. 2.35.2 of December 15 memo)

For IP rights enforcement, law enforcement and other legitimate interests, historical WHOIS data is critical and therefore it is important for such data to be retained and made accessible to third parties for legitimate interests/purposes.

In referencing the EU trademark register and other existing public registers in Europe, Hamilton noted that entries are often kept for an indefinite period of time. We think this militates against the overly conservative data retention obligation that Hamilton seems to be suggesting for WHOIS data.

8. DPIA and Consultation with DPA

We agree with Hamilton's guidance of constructing a model, undertaking a formal Data Protection Impact Assessment ("DPIA") and consulting with relevant Data Protection Authorities ("DPAs"). However, we respectfully disagree with Hamilton's advice to "implement an interim solution based on a layered access model," particularly the very limited layered access model for administrative and data/disaster recovery purposes that Hamilton outlines in paragraphs 2.4 – 2.5. Instead, we urge that ICANN work on a model generally in accordance with Hamilton's guidance for maintaining a publicly accessible WHOIS directory that contains less personal data than today's WHOIS, and that ICANN implement such a model as an interim solution. We strongly recommend this course of action for several reasons:

First, as a practical matter, it is less complicated and more straightforward to implement a public register model (which is much closer to the current system) with a more limited set of personal data than constructing a layered access model. Hamilton itself acknowledges that layered access—even as an interim solution—is a model for which "the exact purposes and mechanics" would "need to be analyzed in depth." (See Par. 3.2.1). Therefore, a public register model makes more sense as an interim solution.

Second, the public register model (with more limited personal data) as an interim solution would better serve: (i) all the purposes and interests that Hamilton has correctly identified in Par. 2.7.1, (ii) the law enforcement purposes that Hamilton has acknowledged in Par. 2.6, and (iii) general public interests of transparency, contact ability, stability and security. It is logically inconsistent for Hamilton to (correctly) determine that such purposes are legitimate, but then to advocate for adoption of an interim layered access solution that by Hamilton's own assessment is not "practically feasible" to fulfill those purposes. Such legitimate interests and purposes will not go away and should not be thwarted for however long the undefined "interim" lasts.

Finally, we believe that a layered access model can be worked on as a necessary complement to the public register model and that both should be subject to a DPIA and consultation with relevant DPAs. But as an interim solution, a public register model that makes available a narrower set of personal data that includes at minimum registrant name, e-mail address and postal/physical address is more practical and better fulfills the broad array of public and legitimate interests and purposes, while conforming to the requirements of the GDPR, as Hamilton's legal analysis demonstrates.

****

Thank you for your consideration of these comments.

Respectfully submitted,

Intellectual Property Constituency