ICANN | GAC

Governmental Advisory Committee

Distribution	Public
Date	28 Jan. 2018

GAC Feedback on Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation

I. Introduction

The ICANN Governmental Advisory Committee (GAC) welcomes the opportunity to provide feedback on ICANN's Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation (GDPR)[1]. We are encouraged that "finding a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible is a high priority" for ICANN (Nov. 17th Blog[2], reiterated Dec. 21st Blog[3]).

We note that our comments on the proposed ICANN models are informed by the recently released Part 3 Analysis by the Hamilton law firm[4]. This analysis contained many facts and arguments that support ICANN's goal to maintain the WHOIS to the greatest extent possible, including recognition that:

- ICANN's Bylaws support the conclusion that the purposes for WHOIS services should serve the legitimate needs of law enforcement and promote consumer trust;
- The processing of WHOIS data for law enforcement purposes (including investigating and countering serious crime, fraud, consumer deception, intellectual property violations, and other law violations) should constitute a legitimate interest for processing of personal data under Article 6.1(f) of the GDPR, if it is not already necessary for the performance of the contract (Article 6.1(b)) in view of ICANN's Bylaws and the agreements between ICANN and the registries and registrars;
- Public access to (limited) WHOIS data (including Registrant name and address) should be maintained to the extent possible and only complemented by layered access where required; and
- Other EU mandated public registries demonstrate that the EU has considered it a public interest to keep a public record of the owners of EU trademarks, company registers, and domains in EU ccTLDs and hence "implicitly stated that such interests overrides the interests or fundamental rights and freedoms" of the individuals.[5]

[1] https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf
[2] https://www.icann.org/news/blog/data-protection-privacy-activity-recap
[3] https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year
[4] available at https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en
[5] See appendix for further information.

Our comments on ICANN's proposed models are also informed by several concerns and disagreements with the Hamilton Part 3 Analysis including:

- The suggestion that law enforcement requests for non-public WHOIS data processing would necessarily need prior court approval or legal process; and
- The unsupported conclusion that a registrant's email address should not be part of a publicly available WHOIS database.

Moreover, we emphasize that ICANN should:

- Keep non-personal data in the WHOIS database available to the public;
- Ensure that any interim model requires the collection and publication of WHOIS data rather than permitting Registries and Registrars to elect whether to comply with the chosen model (this comment is not intended to change the currently permissible use of privacy/proxy services)
- Ensure that the WHOIS system is maintained in a manner that supports the public interest, and maintains the balance between the fundamental rights of registrants and the interests of legitimate WHOIS purposes (including law enforcement and the public interest in "preventing fraud; "ensuring network and information security," and reporting possible "criminal acts or threats to public security" to authorities),[6] using the possibilities for balancing of interests built into the GDPR;
- Implement the GAC advice set forth in the Abu Dhabi Communiqué, including to maintain a WHOIS system that keeps "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" and keeps "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." This includes the needs of UDRP and URS providers who should be considered as having a legitimate interest in access to any non-public WHOIS elements necessary to ensure due process.[7]
- Carefully consider the details of layered access including practical details and mechanics so that the community can carefully assess the roles, responsibilities, and consequences for all parties involved and the fitness for use of possible interim models.

In the following submission, we 1) describe the general subject areas contained in ICANN's three proposed models; 2) list what we support and oppose within each model, and highlight the harmful consequences of implementing an unduly restrictive WHOIS model that goes beyond the requirements set forth within the GDPR.

In addition, we present a fourth model for consideration that selects the attributes from the three existing models that the GAC believes are the most effective in complying with the GDPR, while also maintaining as much of the existing attributes of WHOIS. Finally, we include a short Appendix commenting on the Hamilton Part 3 legal analysis, as it provides part of the rationale that drove our comments on the ICANN models.

---

[6] *See* GDPR Recitals 47, 49 and 50.

[7] It is noted here that the "ECO GDPR Domain Industry Playbook v.061" specifically states that disclosure further to a UDRP proceeding "may be disclosed on the basis of Art. 6(1)(b)." Note also that many global ccTLD policies are modeled on the UDRP, and as such employ similar notification/due process methods.

II. Subject Areas Included in ICANN Proposed Models

ICANN's proposed models modify four different areas in an effort to comply with the GDPR:

- who is covered by the model
- what fields/data are publicly displayed
- how third parties get access to non-public data
- data retention

We view these models as presenting a menu of possible options that can be combined to achieve a WHOIS system closest to the current one while complying with GDPR, which is the stated goal of ICANN.

We also note that there does not appear to be a consistent approach to ICANN's analysis of the issues created by the GDPR. For example, it is not clear why it is acceptable to display some data in one model but not in another. If the registrant's name can be displayed under Model 1, then it cannot also be true under the GDPR that it cannot be displayed as under Model 2. The law should be consistently applied.

In line with GAC Advice from ICANN 60 in Abu Dhabi which states, "the GAC should be fully involved in the design and implementation of any (including interim) solution", the GAC offers the following comments on each of the proposed models[8].

It remains important to emphasize ICANN's commitment to "ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible."[9]
This would require a measure of legal certainty; stating that the contracted parties "may" choose to collect and further process data cannot provide such certainty.

III. Model Analysis

The continued collection of full thick WHOIS registration data for legitimate interests is a welcomed decision.

[8] Governmental Advisory Committee Communiqué – Abu Dhabi, UAE. Nov 1, 2017. Page 14.
[9] Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation. Page 2.

Model 1

We are encouraged to see that Model 1 has the largest amount of data fields displayed publicly.

Concerns:

- The lack of registrant email is still problematic.
    - Registrant email is necessary to contact victims of malware campaigns and for analysis of patterns among malicious registrations.
- Self-accreditation that permits the registry and registrar to only "consider" and have the ability to deny the request without any clearly defined and agreed criteria defeats the purpose of a self-accreditation process and would prevent the quick and easy access called for by the GAC in its advice set forth in the Abu Dhabi Communiqué. Additionally:
    - Self-accreditation cannot occur on a per query basis as it would be too burdensome and prevent fast access to critical information.
    - This model would encourage inconsistent policies and provide no incentive for a Registry or Registrar to accept requests; each company's internal policy would likely differ.
    - A criteria for denying access should not be based on jurisdiction of the request/requestor.
    - There is no clear guidance or requirement for Registry or Registrar to provide access.

Recommendation:

- We propose a true self-certification process whereby Registries and Registrars are required to provide additional access to non-public WHOIS for self-certified applications for legitimate uses. As noted in footnote 15 of ICANN's draft, the self-certification and approval process would be similar to the process registries currently use to approve access to Zone File Data.[10] We disagree with Model one's language stating, "Registries and registrars **may, but would not be required by ICANN** to provide additional access to non-public WHOIS (emphasis added)."[11]

[10] The Registry Agreement states in section 2.1.1 that "**Zone File Access Agreement**. Registry Operator will enter into an agreement with any Internet user, which will allow such user to access an Internet host server or servers designated by Registry Operator and download zone file data. The agreement will be standardized, facilitated and administered by a Centralized Zone Data Access Provider, which may be ICANN or an ICANN designee (the "CZDA Provider"). Registry Operator (optionally through the CZDA Provider) will provide access to zone file data per Section 2.1.3 of this Specification and do so using the file format described in Section 2.1.4 of this Specification. Notwithstanding the foregoing, (a) the CZDA Provider may reject the request for access of any user that does not satisfy the credentialing requirements in Section 2.1.2 below; (b) Registry Operator may reject the request for access of any user that does not provide correct or legitimate credentials under Section 2.1.2 below or where Registry Operator reasonably believes will violate the terms of Section 2.1.5. below; and, (c) Registry Operator may revoke access of any user if Registry Operator has evidence to support that the user has violated the terms of Section 2.1.5 below." Additionally, the Agreement states in section 2.1.5 that "**Use of Data by User**. Registry Operator will permit user to use the zone file for lawful purposes; provided that (a) user takes all reasonable steps to protect against unauthorized access to, use of, and disclosure of the data, and (b) under no circumstances will Registry Operator be required or permitted to allow user to use the data to (i) allow, enable or otherwise support any marketing activities to entities other than the user's existing customers, regardless of the medium used (such media include but are not limited to transmission by e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts of mass unsolicited, commercial advertising or solicitations to entities), (ii) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar, or (iii) interrupt, disrupt or interfere in the normal business operations of any registrant".

[11] Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation. Page 7.

Model 2

We note that formal accreditation/certification program may mitigate concerns over inconsistent policies and practices implemented by Registrars and Registries. However, we note that reaching agreement on such a program would be difficult to achieve in the near term.

Concerns:

- The conflation of natural and legal persons in Model 2 and the uniform approach to data fields for both of these parties represents a significant overreach in terms of ICANN's stated goals to be in line with GDPR.
    - Legal persons are not protected by the GDPR. Not displaying their data hinders the purposes of WHOIS without being required by the GDPR. The GDPR only applies to the personal data of natural persons.
- Retaining data for just 1 year is not in the public interest in that it limits looking at prior WHOIS data for investigative purposes. Investigations are often global, involve many parties, and therefore often take significant amounts of time that exceed one year.

Recommendations:

- The GAC should maintain its strong role in the development of accreditation/certification requirements.
- Any ICANN and GAC consultations on formalized accreditation must include accreditation/certification not just for law enforcement, but all legitimate users of WHOIS including cybersecurity researchers, anti-abuse firms, intellectual property rights holders, consumer protection enforcers and others involved in investigations, crime prevention efforts, combating fraud and deceptive conduct, and due diligence for online transactions and communications.
- A centralized access system for WHOIS data should be hosted by a third party such as ICANN.

Model 3
While the case-by-case assessment of the presence of personal data is helpful, the GAC does not support the access to non-public data set out in Model 3.

Concerns:

- The requirement of access through legal process would in most cases prevent timely access to WHOIS information for the majority of legitimate purposes outside of those involving a crime. Namely, cyber security research, prevention, and mitigation efforts; consumer protection; and others.
- Requiring data to be accessed by legal process is an unreasonable burden on both the contracted parties involved and the requestor of the information. Access to data would be significantly slowed down and halt investigations.
    - Some law enforcement agencies make tens of thousands of WHOIS queries per day.
    - Registries and Registrars would face an avalanche of requests to review.
    - An international request for registrant information would require a mutual legal assistance treaty request or letters rogatory, processes that take months and sometimes years. In certain situations, where countries do not maintain any diplomatic relations, it may be impossible to obtain this crucial investigative information.
    - This requirement would cripple law enforcement and other public safety users' ability to maintain the security and stability of the internet.
- There are jurisdictional issues with the requirement that data be accessed only through legal process:
    - A number of jurisdictions do not provide for a court order to require the production of such data. ICANN cannot require legal process to access such data where no such required legal process exists. Where such requirements exist, they apply independently of any choice made by ICANN.
    - Such a requirement would be difficult for registrars and third parties to implement because it is not clear whose law would apply to the request for non-public information.
- The requirement of access through legal process has no basis in the GDPR; any such need should be left for the national law of the requesting authority to determine.
    - The laws of most EU Member States do not require judicial review of requests for subscriber information. Furthermore, the European Court of Justice has not required it, contrary to the assertion in the Third Hamilton Memorandum.
    - The EU maintains several registers that make nearly identical information publicly available. These analogous publicly available registries and compilation will not be altered under the GDPR.
- Retaining data for 60 days after expiry of the registration is entirely too short to effectively conduct investigations, solve crimes and settle disputes.

IV. GAC's Proposed Model

The GAC considers that the best approach from a public policy perspective consists in a combination of elements from the three models set out by ICANN:

A. **Fields and necessary data elements** – The data fields should be based on Model 1. However, instead of the automatic "Do not display", the relevant fields should be "Display[ed] unless field includes personal data", as set out in Model 3. The Model would require a registration-by-registration, field-by-field assessment about whether personal data is included or not. Accredited actors should have access to all WHOIS data necessary for the fulfilment of their task. This includes all current registration information available, public and non-public, personal and non-personal, collected by registries and registrars. Collection and processing of the data in those data fields should not be left to the discretion of the registrar but should continue to be mandated.

B. **Retention** – In order to ensure the availability of historical WHOIS data, two years as proposed in Model 1 is most ideal. However, this could be too short as it might not give full proof of ownership so an adequate retention policy is needed. The data retention period for the different categories of personal data should be based on individual business needs and a proper data protection assessment. Certain industry practices suggest that a 5-year retention might be appropriate under certain circumstances.[12]

C. **Third Party Access, Accreditation and Authentication** - The concept of accreditation as called for in Model 2 is preferable as an ultimate outcome. We emphasize that there will need to be systems that allow ALL legitimate parties (*e.g.,* law enforcement, consumer protection authorities, cybersecurity firms, IP rights holders, and other public safety agencies as well as other relevant actors) access to non-public WHOIS data.

   Such accreditation systems need to consider the distinct categories of users and the possibility that they may want to develop themselves the accreditation/certification processes and mechanisms. For example, IP rights holders should have the ability to consider how they accredit/certify themselves. The same would be applicable to national governments and law enforcement.

   Recognizing that the development of such an accreditation/certification system would take time, a true self-certification system should be utilized in the interim that requires Registries and Registrars to accept and take action on requests except under limited and clearly defined circumstances, similar to the process used for Zone File Access articulated in the Registry Agreement.

   Access to WHOIS data needs to be maintained regardless of location of storage. This should be achieved in practice through a centralised access system hosted by ICANN.

D. **Covered parties** – As in Model 2A, this model should apply strictly to those parties (registrars and registries) covered within the scope of the GDPR while non-affected parties should retain existing open WHOIS policies and procedures. This could be done under the RDAP protocol.

[12] Best practices seem to range from 2 or 6 years minimum (depending on the industry), to 15 years. See *e.g.*, www.sec.gov/rules/final/33-8180.htm, www.lsuc.on.ca/with.aspx?id=2147499150 and www.vantageinsurance.co.uk/assets/files/atrisk/September%202011.pdf.

Appendix – Considerations on Part 3 Analysis by the Hamilton law firm

Legitimate Interests in Public Access

Law enforcement is not the only interest at stake; as recognized in the ICANN Bylaws, consumers also benefit from access to WHOIS data for commercial websites. Where a website does not contain contact information, consumers can go to the WHOIS databases and find out who is operating the website. Because a website has no obvious physical presence, consumers are deprived of many of the usual identifying characteristics that help instil trust in a traditional retailer. Easy identification of online businesses is a key element for building consumer trust in the electronic marketplace.

EU law recognizes this legitimate interest in several contexts. The EU's Directive on Consumer Rights recognizes the public's right to know the identity and contact information of those with whom they contract, requiring in distance contracts that a trader must provide the consumer with the trader's phone number, fax, and email address.[13] Further, the EU directive on electronic commerce provides:

> . . . Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:
> (a) the name of the service provider;
> (b) the geographic address at which the service provider is established;
> (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner . . . .[14]

In addition, EU law recognizes the public's legitimate interest in the security of the Internet and its essential infrastructures such as registry and registrar services in the Network and Information Security Directive, which states that "Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market."[15] This is also a legitimate interest in public access, as cyber security professionals, including but not limited to computer emergency response teams (CERTs), rely on publicly available WHOIS data to quickly identify and respond to threats to DNS infrastructure.

Similarly, the recent OECD Recommendations on Consumer Protection in E-Commerce also recognize the importance of the public's ability to access information about the entities with which they transact business online, including "appropriate domain name registration information."[16]

The public also relies upon WHOIS to gather information in order to report a complaint. The Federal Trade Commission, the United States' leading consumer protection law enforcement agency,

---

[13] *See* Directive on Consumer Rights §6 (1)(b)(c) Consumer Information for Contracts, available at http://ec.europa.eu/consumers/consumer_rights/rights-contracts/directive/index_en.htm.

[14] Council Directive 2000/31/EC ("Directive on Electronic Commerce") 2000 O.J. (L 178) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML , Article 5.

[15] Directive 2016/1148/EU concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1, Recital 3.

[16] *See* https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf at ¶¶ 28-30, Information about the Business.

conducted a search of its complaint database over the last five years. This search revealed over 4,000 fraud-related complaints that referenced the use of WHOIS data for the public's own investigation of, among other topics: unsolicited email, spyware, malware, imposter scams, advanced fee loans, debt collection, mortgage refinance offers, tech support scams, sweepstakes and lotteries, and counterfeit checks.

Hence, we were pleased that the Part 3 analysis recognized the public's interest in WHOIS data. *See* ¶ 2.7.1. We also agree that "public access to (limited) WHOIS data would be preferred over layered access." See ¶¶ 2.7.10; 2.8.1.1-1.2.

Other Legally Available Public Databases in the EU Support Availability of a Publicly Available WHOIS Database

We welcome the Part 3 Analysis discussion of other publicly available EU directories as examples of personal information that is legally available and serves the public interest. § 2.8. These directories provide similar information to the public without requiring any legal process. In particular the Part 3 analysis recognizes that the availability of these public registries (for example the EU Trademark Register and ccTLD Registers) demonstrate that the EU "has considered it a public interest to keep a public record of the owners of EU trademarks" and hence "implicitly stated that such interests overrides the interests or fundamental rights and freedoms of the trademark registrants." ¶2.8.2.6. The Part 3 analysis also points to the EU regulations applicable to the .EU ccTLD. ¶2.8.3.1. EU Regulation 733/2002 requires public query services akin to the WHOIS database for .EU domain names and notes that these databases are "an essential tool for boosting user confidence." Id. The Hamilton lawyers admit that they "have difficulties" seeing the difference between a trademark register and a domain name register "from a public interest and integrity protection perspective." ¶2.8.2.6.

Therefore, the requirement in Model 3 is excessive given that even EU states do not usually require legal process to access subscriber information and many EU systems display similar data without requiring legal process. Such a requirement would do significant harm to law enforcement and the security and stability of the internet because of the enormous increase in the time it would take to acquire non-public WHOIS information. If law enforcement cannot quickly and effectively access WHOIS information to assist in pinpointing who owns or controls a domain, it is the public, who are at risk of being victimized, that will suffer. As the GAC has noted in its Aby Dhabi advice, ICANN should use its best efforts to maintain a WHOIS system that keeps "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." The EU Council has also recognized the importance of "ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names so that law enforcement capabilities and public interests are safeguarded."[17]

We also note the other examples in EU law listed above that require disclosure of personal information to the public for various legitimate purposes. Hence, we agree with the Part 3 Analysis that arguments in support of maintaining a publicly available WHOIS database are consistent with other EU laws and in the public interest, and that these issues require further discussion and analysis by the DPAs charged with enforcing the GDPR.

[17] Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defense: Building strong cybersecurity for the EU at ¶44. Available at http://www.consilium.europa.eu/media/31666/st14435en17.pdf.