Date: 29 January 2018

TO: ICANN Org

FROM: Greg Aaron, iThreat Cyber Group

RE: Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the GDPR

This document is a public comment regarding ICANN's three proposed models for interim compliance with the GDPR.[1] ICANN Org stated that its main goal is "to identify the appropriate balance for a path forward to ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible." Only Model 1 accomplishes ICANN's stated goals. Models 2 and 3 have fatal flaws and fall far short. Below we examine the three models and comment on the other content in ICANN's document.

Model 1

By far, Model 1 has the most virtues.

First, it is the only solution that is appropriately scoped and satisfies the goal of ensuring "compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible." It provides a balanced, appropriate (and according to Hamilton, legally compliant) set of data fields in publicly accessible WHOIS. And it protects the parties (and only the parties) that GDPR is meant to protect: natural persons in the EU.

Community members have provided ample use cases and legitimate purpose justifications to support the publication of the minimum data fields listed for Model 1.

Model 1 can be technically implemented in the short time period available, and is commercially reasonable. To implement, registrars can flag a domain record to indicate when the registrant is a natural person in the EU. This can be accomplished via a simple EPP extension and an additional field in the registry database. If the flag is present, then data in sensitive fields (per Appendix 2) will not be published in WHOIS output. The contracted parties can agree to a common EPP extension, and the necessary code changes are not difficult. Registries such as .AMSTERDAM and registrars such as GoDaddy have recently implemented this kind of code change.[2]

[1] https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf

[2] Regarding .AMSTERDAM, see http://nic.amsterdam/whois-privacy/ and https://www.icann.org/en/system/files/correspondence/jeffrey-to-sprey-01nov17-en.pdf . GoDaddy is reportedly withholding contact data for queries made on port 43, but does provide contact data for port 43 queries made via white-listed IPs and via web-based WHOIS; see http://domainincite.com/22510-godaddy-and-domaintools-scrap-over-whois-access and https://domainnamewire.com/2018/01/12/godaddy-start-masking-whois-data-port-43/

The self-certification program in Model 1 is the only practical approach in the short term. Later it may be possible to shut down the self-certification program and replace it with the formal accreditation/certification program proposed in Model 2. It is clear that creating and implementing an accreditation/certification program will take years. In the meantime, Model 1 provides some public contact data that parties need for various legitimate and pressing uses, including combating cybercrime, cybersquatting and intellectual property abuses, and for compliance issues.

Model 1's self-certification program has one major flaw: participation is optional, and registrars and registry operators may simply ignore or turn down legitimate data requests. We know this will happen because registrars and registry operators often ignore subpoenas and court orders from outside their jurisdictions, and some ignore requests and complaints recognized the ICANN contracts.[3] If at all possible, ICANN must establish clear obligations and a compliance regime here. Without some compliance mechanism the self-certification program will be toothless and of limited utility.

Model 1 states a data retention period of two years beyond the end of the domain name registration. This default seems reasonable. Contracted parties could still use ICANN's existing exemption process to reduce the length of the period. In no case should ICANN approve retention periods of less than a year; that would unreasonably hamper legitimate interests such as contractual compliance and financial auditing.

Model 2

Model 2 is fatally flawed, for two main reasons.

First, the solution is out of scope. The task at hand is to comply with GDPR "while maintaining the existing WHOIS system to the greatest extent possible." But instead, Model 2 extends protection far beyond GDPR. Model 2A extends protection to both natural *and* legal persons in the EU, and Model 2B extends protection to all natural and legal persons *across the globe*. This amounts to a new international privacy rights regime created by ICANN. Such a decision is not necessary for GDPR compliance. And it is possibly outside of ICANN's remit—it is ICANN's job to help facilitate compliance with laws, not to advocate for or impose a new legal standard worldwide. Such a discussion would certainly require a formal community process such as a PDP, and is not appropriate to make during the hurried process we currently find ourselves in.

Model 2 is also unbalanced, and maintains the existing system to much less of an extent than possible. Model 2 will hide much more data than Model 1, and since an accreditation/certification program cannot be available for years, Model 2 will deprive a wide range of legitimate users of most contact

[3] For example see https://www.huffingtonpost.com/john-horton/if-icann-doesnt-keep-regi_b_6101536.html and https://www.icann.org/news/blog/update-on-steps-to-combat-abuse-and-illegal-activity and https://www.icann.org/en/system/files/files/sac-097-en.pdf

data.[4] Model 2 make things extremely difficult for many legitimate use cases, including for security providers and everyday Internet users.

Model 2 would not be easier to technically implement than Model 1. Like Model 1, it would require registrars and registry operators to modify their WHOIS code.

Model 3

Model 3 is a non-starter. It has drawbacks of Model 2, plus:

- A registration-by-registration, field-by-field assessment about whether personal data is included in a domain record may be impractical to implement, especially in the short term. It may be beyond the capabilities of many registrars.
- It unbalances the playing field far into the favor of criminals, cybersquatters, and shady registrars. Non-public data would be extremely difficult to obtain – it would only be available by a formal legal order issued within the jurisdiction of the registry operator or registrar. This would turn GDPR into an opportunity to create havens for bad behavior, to the detriment of the safety of Internet users everywhere.
- The data retention period of 60 days is so short that it will create problems. It effectively closes off the contractual compliance tools present in the 2013 RAA and registry contracts. It is barely longer than the RGP/RHP period.

Other Comments

Cost, and the Public Good

ICANN's registry contracts have always reflected the view that WHOIS is a public resource, provided for a wide variety of legitimate uses and necessary for the stability, security, and trustworthiness of the namespace and the Internet in general. As such the registry contracts and the RAA have always stated that providing WHOIS is a core service, and they do not allow contracted parties to charge users for access. These things should not change.

GDPR will impose certain new costs on registrars and registry operators. That is a simple consequence of the legislation, and part of doing business with registrants in the EU. It would be appropriate for contracted parties to pass the cost onto their paying customers—such as the EU registrants who are buying the domains, or to registrars who choose to serve the EU market. But GDPR should not become a reason for contracted parties to turn WHOIS into a new profit center, to unduly restrict legitimate

[4] Admin and Tech contact email addresses would be displayed under Model 2, but those are of limited use especially in the case of bad actors, who often use free, throw-away, unmonitored email addresses. For this reason email addresses are useful for anti-abuse and reputational scoring only when they can be paired with other pieces of data, such as a name.

access (to data that should be published, or access to WHOIS service itself), or to shirk their responsibilities to participate in the thick registry model, etc. We must all remember that WHOIS data is used to protect most Internet users from abuse by the criminal registrants who register literally millions of gTLD domains every year. This protection is notably provided through the reputation systems that guard against malware, phishing, and related threats.[5] We should not allow the cost of GDPR compliance to be shifted from attackers to the victims and defenders.

Purpose Description

The listed purposes are all legitimate and do not merely reflect existing *uses* of registration data. The Description's provisions parallel some purpose descriptions in use by ccTLD registries in the EU.

Compliance with Laws

We encourage ICANN to continue its compliance efforts, and to spell out compliance requirements clearly for whatever interim solution is chosen. Contracted parties must be allowed to comply with applicable laws. But they should also be required to demonstrate if and why their solutions *must* deviate from the base model that ICANN chooses. Requests for variances should be subject to community notice and comment, and ICANN Org must be able to defend to the community its decisions about whether specific deviations are justified.

When does a variance become too much to allow? ICANN may have to make some difficult decisions in the future as governments continue to regulate within their jurisdictions. There may be places in the world where the local laws become too far out of synch with ICANN's core values and contracts. ICANN's Bylaws enshrine "promoting competition in the registration of domain name", but only "*where practicable* and *beneficial to the public interest*." (Emphasis added.) Selling gTLD domains is not a right—ICANN accreditation is a privilege that comes with certain obligations. And an unfortunate reality is that the Internet allows a malicious registrant in a poorly-managed jurisdiction to harm parties in other jurisdictions with impunity. Registrants will not be unduly harmed if ICANN declines to accredit parties in unconducive places. Registrants can choose from among hundreds of registrars located in many jurisdictions, with varying commercial terms of service; they can obtain privacy and proxy protection; they can register ccTLD domains if they do not like gTLD policies; and ICANN has procedures to protect and transfer registrants when a registrar or registry is deaccredited.

Consent

ICANN's memo notes that:

> registrars must request from registrants specific and informed consent that is freely given, unambiguous, withdrawable at any time, and is otherwise consistent with the

[5] https://www.icann.org/news/blog/reputation-block-lists-protecting-users-everywhere

GDPR for publication of full Thick data. If the registrant does not provide its consent, or later withdraws its consent, the minimum public WHOIS data that should be displayed is outlined in each model.

Many registrars will want to improve their consent practices to bring them up to GDPR standards. However, this should not be an excuse for registrars to delay the work of getting consent or to over-block data publication. Registrars might state that the consent they have gathered thus far – for all existing registrations—have not been up to GDPR standard, and therefore all relevant contact data must be masked (not displayed). This will effectively undercut Model 1, reducing the display of data to a bare minimum of thin data. Therefore, the way forward must include provisions that registrars get their contact practices up to speed as soon as possible, and that they seek GDPR-compliant permissions for existing registrations. Registrant consent for publication per Model 1 should be on an *opt-out* basis (published by default), rather than an opt-into publication basis.[6] Compliance exemptions should not be granted if registrars are not diligently pursuing the work.

Commonalities Across All Models

The assumptions in the "Commonalities Across All Models" are reasonable. Points 1, 2, and 3 note that registrars may collect data from registrants and may transfer that data to registries and escrow providers. Cross-border transfers of personal data are allowable under GDPR with the appropriate provisions. The thick registry model appears to be completely tenable under GDPR, and can serve legitimate interests such as those identified in ICANN's recent Thick WHOIS PDP.

Interestingly, the European ccTLD registries are thick, sell domains to registrars and registrants both inside and outside the EU, and these parties will continue to do so under GDPR. If the thin registry model was the best way to deal with GDPR, or if data transfers were a difficult problem, we would see ccTLDs significantly changing their business and operational models…but they are not.

Account Holder and Transaction Data

Appendix 1 is missing references to certain pieces of data that must be *collected* by registrars, but are not *displayed* in WHOIS. ICANN should clarify that these collection requirements will continue to be in force. They are found in the 2013 RAA's WHOIS Accuracy Program Specification and the Data Retention Specification, and include information about account holders (which are different from registrants), payment details, and communication records.

[6] For example, opt-out of publication is the standard for .UK