From: Robert Rutkowski
Sent: 19/04/2018 04:11
To: globalsupport@icann.org
Subject: Privacy as an Afterthought: ICANN's Response to the GDPR

Göran Marby, President ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
Phone: +1 310 301 5800 Fax: +1 310 823 8649
Email: globalsupport@icann.org

Re: Privacy as an Afterthought: ICANN's Response to the GDPR

Dear President:

Almost three years ago ICANN[eff.org] chartered a working group to consider how to build a replacement for the WHOIS database, a publicly-accessible record of registered domain names. Because it includes the personal information of millions of domain name registrants with no built-in protections for their privacy, the legacy WHOIS system exposes registrants to the risk that their information will be misused by spammers, identity thieves, doxxers, and censors.

But at the same time, the public availability of the information contained in the WHOIS database has become taken for granted, not only by its regular users, but by a secondary industry that repackages and sells access to its data, providing services like bulk searches and reverse lookups for clients as diverse as marketers, anti-abuse experts, trademark attorneys, and law enforcement authorities.

The working group tasked with replacing this outdated system, formally known as the Next Generation gTLD RDS to Replace WHOIS PDP Working Group did not get far. Despite holding 90 minute weekly working meetings for more than two years, deep divisions within the group have resulted in glacial progress, even as the urgency of its work has increased. A key privacy advocate within that Working Group, EFF Pioneer Award winner Stephanie Perrin, ended up resigning from the group in frustration this March, saying "I believe this process is fundamentally flawed and does not reflect well on the multi-stakeholder model."

With the impending commencement of Europe's General Data Protection Regulation or GDPR on May 25, which will make the continued operation of the existing WHOIS system illegal under European law[eff.org], ICANN's board has been forced to step in. On April 3, members of the Working Group were informed that it had been "decided to suspend WG meetings until further notice while we await guidance from the Board regarding how this WG will be affected by the GDPR compliance efforts."

ICANN Board Cookbook

With this, the Board has floated its own interim solution aimed at bringing the legacy WHOIS system into compliance with the GDPR. The ingredients of this so-called "Cookbook" proposal[icann.org] are drawn from responses to a call for public submissions, to which EFF contributed[eff.org]. In short, it would make the following changes to the WHOIS regime:

- Although full contact information of domain name registrants will still be collected, most of this information will become hidden from public view, unless the registrant affirmatively "opts in" to displaying that information publicly. A tiered access model will be put in place to ensure that only parties who have a "legitimate interest" in obtaining access to a registrant's address, phone number, or email address, will be able to do so.
- Although email addresses will not be displayed in the public WHOIS data record, they will be replaced by a contact form or anonymized email address, which would still allow members of the public to make contact with a domain owner if they need to. (This idea is one of those that EFF had suggested in our submission, with the additional suggestion that the contact form be protected by a CAPTCHA to minimize the potential for misuse.)
- No differentiation is attempted to be made between domains registered to individuals, and those registered to companies. This makes sense, because many company domain records do include personal contact information for individuals who act as the administrative or technical contacts for the domain. In practical terms, it would be impossible to weed out the entries that do contain such personal information from those that don't.

The board proposal is an improvement on the status quo, but doesn't go as far in protecting privacy as we would like it to. For example, it leaves it up to individual registrars as to whether they should apply these privacy protections to all domain owners worldwide, or attempt to limit them to those within the European Economic Area. It also contains a too expansive suggested list of acceptable purposes for the collection and processing of WHOIS personal data, including "to address issues involving domain name registrations, including but not limited to:

consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection."

The ICANN board's Cookbook proposal was submitted to the European Data Protection Authorities, who come together in a group called the Article 29 Working Party, for consideration at its next meeting which took place on April 10-11. The board had hoped to receive[icann.org] the group's agreement to a moratorium of enforcement of the GDPR over WHOIS until ICANN is able to get its act together and establish its interim accreditation program. But the Working Party's reply of April 11[icann.org] offers no such moratorium, and instead affirms that the purposes for data collection listed by the board are too broad and will require further work if they are to comply with the GDPR.

Another fundamental limitation of the Cookbook proposal is that while it sets up the idea that there should be an accreditation program for "legitimate" users, it leaves unanswered key questions about how that accreditation program should operate in practice, and in particular how it would assess the legitimacy of claimants seeking access to user data. Since there is not enough time to develop an accreditation system before May 25, the board floats the option of an interim self-accreditation process, which somewhat undermines the purposes of limiting access. The other option is that, by default, access to WHOIS data would "go dark" for all users, until a suitable accreditation system was in place.

Business and IP Constituencies Accreditation and Access Model

This prospect has disturbed stakeholders accustomed to receiving free access to registrant data; one goes so far[riskiq.com] as to describe the Cookbook proposal as "the most serious threat to the open and public Internet for decades." ICANN's Business and Intellectual Property constituencies have responded by proposing an accreditation and access model[ipconstituency.org] aimed at keeping the WHOIS door open for three loosely-defined categories of actors: cybersecurity and opsec investigators, intellectual property rights holders and their agents, and law enforcement and other government agencies. It attempts to fill in the gaps of the Board's proposal by suggesting how these users might be accredited.

The biggest problem with the Business and IP constituencies' proposal is that the bar for accreditation to access full registrant data would be set so low that it would become essentially meaningless, while still managing to exclude the wider public and keep them in the dark about who might be viewing their personal data. For example, it could allow anyone

who has registered a trademark to enjoy *carte blanche* access to the entire WHOIS database. In a token effort to prevent misuse of WHOIS access there would be random audits, but penalties for misuse might be limited to de-accreditation.

The proposal would structurally elevate the financial interests of intellectual property owners above the privacy and access rights of ordinary users. While the GDPR does allow data sharing that is necessary for the purposes of legitimate interests of third parties, these interests must be balanced with and can be overridden by the interests, rights or freedoms of the domain name registrant. This proposed accreditation and access model doesn't even attempt to strike such a balance.

Although EFF would have preferred[eff.org] a model requiring a court order or warrant for access to such personal information, it seems inevitable that tiered access will be based on some kind of ICANN-administered accreditation system. Community discussions on what that accreditation program should look like continue on a new ICANN discussion list, using the Business and IP constituencies' proposal as a starting point. But this is work that should have been finished long ago. The commencement date of the GDPR has been known since the rule was adopted on April 27, 2016. Although its edges will be difficult for ICANN to navigate, its basic outlines are not rocket science; it has been obvious for over two years that more would need to be done to secure the personal information of domain name registrants.

Unfortunately, ICANN's version of a multi-stakeholder process has broken down over this contentious issue of registrant data privacy. It therefore falls to ICANN's board to make the interim changes necessary to ensure that the WHOIS system is brought into compliance with European Union law. While this interim model may be replaced by a community-based access model in the future, institutional inertia is likely to see to it that the Board's "interim" policy constrains the outlines of that future model. This makes it all the more important that the ICANN Board listens to all segments of its community, and to the advice of the Article 29 Working Party, in order to ensure that the solutions developed strike an appropriate balance between stakeholders' competing interests, and that the human rights of users are put first.

Thank you for the opportunity to bring this EFF post to your attention.

Yours sincerely, Robert E. Rutkowski