Writer's Direct Cell: (206) 556-0118

From the desk of
Jonathan Matkowsky, VP – IP & Brand Security
Certified Information Privacy Technologist (CIPT)

THREAT SEVERITY:HIGH
TIME-SENSITIVE

May 11, 2018

EMERGENCY TEMPORARY POLICY RE GDPR

VIA EMAIL <*goran.marby@icann.org*>, <*cherine.chalaby@icann.org*>

Mr. Cherine Chalaby
Chair
ICANN Board

Mr. Göran Marby
ICANN President and CEO

Dear Members of the Board:

We understand that the ICANN Board of Directors will meet this weekend to discuss GDPR-related advice from the GAC, and will consider, and likely vote on a temporary specification for gTLD registration data and GDPR implementation matters. This has been a learning experience for all of us involved, and I want to share with you my current perspective:

Privacy By Design Is a Critical Component of GDPR.

In early March, I was under the mistaken impression that an accreditation model is required for enforcing layered or tiered-access; my views have changed since our April 20 letter. As I alluded to yesterday on the *CyberWire Podcast* (6:56-11:32), according to the Centre for Information Policy Leadership GDPR Implementation Project (Hunton & Williams) as of April 2017, the absence of accreditation or certification under GDPR is supposed to have no negative effect. DPAs are incentivizing and publicly affirming certifications and codes of conduct as a recognized means to demonstrate GDPR compliance, as they should. This does not mean that legitimate interests that override the rights of the individual can be ignored merely because accreditation schemes or codes of conduct are not available just yet. In late March, I confirmed in the context of discussing ICANN and GDPR after the Fireside Chat with the Chair of the Article 29 Working Party at the IAPP's Global Privacy Summit, that everyone agrees that privacy

by design is a critical component of GDPR. Privacy by design is required even without accreditation schemes. Tiered access is available currently--whether it is via IP-based whitelisting as discussed by FIRST, M3AAWG and APWG, or possibly even a federated authentication for RDAP using OpenID Connect that the community has started to examine (I have not had a chance to inspect its features yet).

gTLD WHOIS database operators implementing privacy by design principles must ensure that rate-limiting does not frustrate the functionality of gated access requests. When the balancing act favors, based on a legitimate interest, providing gated access to the requested data, and a WHOIS database operator's rate-limits prevent the disclosures from functioning as intended, that is just a defective system--a flaw in the requirements, design or implementation, which will lead to system failure, and is **dangerous**. This is not in the spirit of GDPR, because such a system is designed to *appear* as if requests are manifestly excessive, which actually serves to weaponize GDPR to potentially undermine network and information security, combating fraud, and consumer protection and safety (much like GDPR has the potential to be weaponized to stifle freedom of press)**.**

ICANN should make sure that newly registered corporate gTLD domains after May 25 do not collect personal data to avoid creating unnecessary conflict between Thick WHOIS and GDPR. If this is not realistic because it is too risky or burdensome to implement, than there at least needs to be a system in place for an organization or individual to check what domain names have been registered in its name to avoid unnecessarily harming network and information security, protection from financial or other fraudulent use of services, and trust and safety of Internet users (perhaps similar to auDA, although I am only now first becoming familiar with this policy). Otherwise, tiered-access will require the gTLD WHOIS database operator to increase the rate limits to accommodate that, which may cause system overload in the aggregate, and therefore, be used from the outset as an excuse to make it look like it would be manifestly excessive, impossible to accommodate. This would be a failure of ensuring that corporate domain administrators understand that no personal data is required to register a corporate domain, and making sure that they understand if they prefer to do it anyway, they will not be able to exercise their rights to object to processing as easily under Article 21, etc. It also means ensuring individuals understand their information will be shared with not only the Czech Arbitration Court, WIPO, the FORUM and any other UDRP/URS Provider upon receipt of a registrar verification request, but also, *with the complainant* upon request to consider it for evidence, or to make a motion to amend or consolidate etc. In addition, upon receipt of a final draft complaint of a UDRP or URS, all accredited registrars must cooperate to try and provide evidence from their WHOIS databases consistent with applicable law, which requires taking the individual registrants' freedoms and rights into account. Respondents participate in these administrative proceedings, and are aware of what's happening with an opportunity to object.

ICANN's temporary policy should require gTLD Whois database operators to inform new registrants in a GDPR-compliant manner about the legitimate interests that provide the basis for potentially sharing WHOIS personal data with third parties.

We appreciate that WHOIS database operators need to be careful in assessing if a legitimate interest exists by taking into account, amongst other things, the registrant's reasonable expectations *at the time that processing takes place* per Recital 47, and the specific examples that the GDPR lists when such legitimate interest may arise. Because the WHOIS database has evolved, of course not every individual would have expected WHOIS to be used for ensuring network and information security (e.g., preventing, detecting and mitigating security incidents), combating financial or other fraudulent use of services, protecting corporate and consumer trust and safety, which may include intellectual property rights protection and its mechanisms, legal *or* administrative-related cases or proceedings, and/or compliance auditing, monitoring, and/or enforcement-related activities (e.g., ICANN Compliance).

That said, given the public nature of WHOIS, and increasingly available use of privacy and proxy registration services over the years, a substantial number of registrants would have presumed--and it would be reasonable to expect--that these kinds of processing activities take place. These processing activities are expressly contemplated by ICANN's Bylaws, which requires ICANN to perform its technical SSR mission for the benefit of the Internet community, taking into account consumer protection, malicious abuse issues and rights protection. (Sec. 1.2; Sec. 4.6(e)(ii); 4.6 (d);1.1(a)(i) and Annex G-1 and G-2). Many individuals being opted out of public WHOIS may actually be relying on it (whether they can articulate it) as part of the technical and organizational measures ensuring a level of protection appropriate for the risk of registering a commercial gTLD as discussed.

Therefore, ICANN's temporary policy should require gTLD Whois database operators to inform new registrants in a GDPR-compliant manner about the legitimate interests that provide the basis for potentially sharing WHOIS personal data with third-parties.

The temporary policy must hold gTLD Whois database operators accountable for failing to respond to, or appropriately consider, Thick gTLD Whois data requests.

If ICANN doesn't also hold its gTLD WHOIS database operators accountable (unless it demonstrably conflicts with applicable local laws of the WHOIS database operator) for abusing their discretion, or intentionally failing to assess legitimate interests in Thick WHOIS data requests, or on other grounds recognized by GDPR, there will be significant foreseeable damages caused by omitting these controls from a temporary policy.

There is already a process in place under the 2013 RAA for registrars that fail to respond to, or appropriately investigate, reports of abuse. So, the framework exists. It may be used as part of a temporary policy to ensure that there is accountability on a high level. Under certain circumstances, DPAs may need to get involved to protect the rights of the individuals, as well as the WHOIS database operators to exercise their reasonable discretion.

Some may argue that a temporary policy from ICANN will need to be extremely narrow in scope, and that what I am proposing is significantly broader than what could fit into a temporary policy. They may see it as not only going beyond GDPR compliance, but adding requirements for both registries and registrars that do not exist. They also may argue that I'm ignoring the fundamental fact that the bulk of domain names are with VeriSign, which does not use Thick Whois.

As far as I can tell, if a temporary policy is adopted by the Board based on a reasonable determination that it is necessary to maintain the stability or security of the registrar services, registry services, or the DNS or the Internet (collectively, or any individually, "Public Interest"), than the proposed specification only has to be narrowly tailored as feasible *to* achieve *those objectives*. If the Board passes a temporary policy that requires its gTLD Whois database operators to assess legitimate interests under GDPR for Thick Whois data requests (some of these requests may be broader than others with respect to the fields being requested, depending on the context), then gTLD Whois database operators that *don't* assess legitimate interests weighed against the registrant's rights per GDPR would, in essence, be undermining the Public Interest. It is reasonably inferred that unless prohibited by local law from conducting the assessment to begin with, an abuse of discretion performing such assessment--or intentionally failing to perform the assessment--is substantially equivalent to failing to take legitimate interests for processing into account. And if a temporary policy is needed in the first place to avoid harm to the Public Interest by requiring this assessment be conducted, than *not also* providing a means for reporting abuse to ICANN is the same thing as not requiring the assessment to begin with.

Furthermore, the goal of a temporary policy need not be limited to not *violating* GDPR. The goal is to comply with the letter and spirit of GDPR. So, the fact a temporary policy goes beyond GDPR compliance is irrelevant, as long as it's consistent with GDPR and does not conflict with local laws governing the gTLD WHOIS database operators. It does add requirements that do not exist, but that is the point---given the changes to public WHOIS, new requirements are needed to not undermine the Public Interest. With respect to the fact the bulk of domains are with VeriSign, which does not use Thick Whois, VeriSign stated on April 13 that it has completed all technical and operational work necessary to begin accepting thick data from registrars this month.

The work of significant segments of the community on a tiered access/accreditation model and the security mechanisms available provide *guidance* for assessing whether a WHOIS database operator abused its discretion or intentionally did not adequately respond to a gTLD WHOIS data query. Additional resources available include CIPL's github repository, and I am happy to

provide others, including taxonomies and classification schemes to ensure the system is not being abused.

The ultimate decision whether a legitimate interest exists remains with the WHOIS database operators; however, by holding them accountable, ICANN also avoids unnecessarily fragmenting the gTLDs, which ICANN is well aware is an SSR risk.

It seems to me that most DPAs map their priorities to a strategic plan. I would guess all of them share the goal of increasing the public's trust and confidence in how data is used and keeping pace with evolving technology similar to ICO. ICANN must take this opportunity to issue a temporary policy that reflects not only compliance with GDPR, but a genuine commitment to the spirit of GDPR. **Without holding the WHOIS gTLD database operators accountable for implementing privacy by design, so that it is actually designed to protect data subjects without harming legitimate interests under GDPR and the Public Interest, ICANN will cause tremendous damage, on a massive scale.**

ICANN must have the vision to be proactive, and ensure the system will actually operate to mitigate risk by ensuring the contracted parties are looking at the features and context of each case not to increase the risk of potential or actual harm to people with legitimate interests and the Public Interest, similar to what has been described about the ICO's Regulatory Action Policy. From the ICO's Regulatory Action Policy, it seems that GDPR provides ICANN with an opportunity to implement a bold plan that considers the Public Interest, SSR, and also the rights and freedoms of individual registrants. Look at the seriousness of what's at stake if you pass a policy that does not hold WHOIS database operators responsible to exercise good-faith and due diligence to meet legitimate interests, when those interests clearly outweigh the affected level of privacy interference to an individual registrant. This requires tiered access, even though acceptable forms of accreditation are not yet available. It takes a lot of work to design a system that is capable of meeting legitimate needs, but if ICANN expects to invite the DPAs to support this important work, ICANN must not sabotage GDPR the way it would be doing by continuing to threaten to implement a policy that would cause such massive financial, psychological, and potentially physical damage. ICANN needs to ensure that the WHOIS technological security measures are adequate. The cost of holding gTLD WHOIS database operators accountable to make tiered-access available to meet legitimate interests is nominal when compared against the massive public harm that would be caused by not doing so.

CONCLUSION

As Michael Hausding, SWITCH-CERT stated: "Based on the current issue of WHOIS privacy, my opinion is that privacy and security are not antagonists, but two important and correlated properties that are both essential for a safe Internet....the loss of Internet security through WHOIS privacy will most likely result in more privacy violations by criminals...This is an serious issue, and we need a solution that is protecting both, the security of the Internet users and the privacy of legitimate domain name registrants."

We thank the Board, in advance, for carefully examining and considering these thoughts. Please do not hesitate to contact us at any time.

Sincerely,

cc:

SSAC
GAC Chair
PSWG
EU Commission Article 29 Working Party
APWG
FIRST
INTA
IPC
M3AAWG
ACC-MODEL