C O A L I T I O N F O R O N L I N E A C C O U N T A B I L I T Y
WWW.ONLINEACCOUNTABILITY.NET

C/O MITCHELL SILBERBERG & KNUPP LLP ● 1818 N STREET N.W., 8TH FLOOR ● WASHINGTON, D.C. 20036-2406
TEL: (202) 355-7900 ● FAX: (202) 355-7899 ● E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

MEMORANDUM

TO: Goran Marby, ICANN CEO
John Jeffrey, ICANN General Counsel
Akram Atallah, GDD President

FROM: Steve Metalitz, Counsel to COA

RE: ICANN Interim WHOIS model to comply with GDPR

DATE: February 16, 2018

Dear Goran, John and Akram:

As ICANN org continues its work of selecting an interim WHOIS model to comply with the GDPR, we want to bring to your attention the critical importance of one data element that should remain in public WHOIS for a variety of important reasons. That data element is the real registrant e-mail address as supplied by the registrant to the registrar and verified by the registrar. While some may posit that an anonymized, masked or message relay link e-mail address will serve as an adequate substitute, this simply is not the case. Our purpose in writing to you is to explain briefly the reasons behind the foregoing statements and to urge ICANN org to consider them carefully as it finalizes its work on the interim model.[1]

Justifications for Continuing to Include Registrant E-mail Address in Public WHOIS

As stated in the IPC Comments on the proposed interim models, "the registrant's e-mail address is typically the most important data point to have available" not only for IP enforcement purposes, but also for law enforcement, consumer protection and cybersecurity/anti-malware purposes as well. See: https://www.icann.org/en/system/files/files/gdpr-comments-ipc-icann-proposed-compliance-models-29jan18-en.pdf. This data element is likely to be more accurate than others—particularly for bad actors—since registrars first must validate the e-mail address and thereafter a working e-mail address is necessary for the registrar and registrant to communicate about payments, expirations, etc.

[1]We believe ICANN has sought or may seek the input of the Article 29 Working Party on this question of the inclusion of registrants' email addresses in public WHOIS. We trust that ICANN will fully brief the Article 29 Working Party on the numerous vital legitimate and public interests served by the inclusion of email address in public WHOIS. We hope this letter, Brian Krebs' recent comments in the article cited in this letter, and the related IPC/BC letter to the Art. 29 Working Party, provide the necessary details on this crucial data element. COA stands ready to participate in such briefings if this would help increase understanding on this crucial point.

Keeping the registrant e-mail address in public WHOIS allows: (i) a broad array of threats to be recognized and addressed quickly, and (ii) damage from such threats to be contained, particularly where the abusive/illegal activity may be spawned from a variety of different domain names on different gTLDs.

On February 15, 2018, world-renowned cybersecurity expert Brian Krebs posted a blog about the potential impact of the GDPR on security. See: https://krebsonsecurity.com/2018/02/new-eu-privacy-law-may-weaken-security/#more-42552. In this piece Krebs states, "I can say without hesitation that few resources are as critical to what I do here at KrebsOnSecurity than the data available in the public WHOIS records. WHOIS records are incredibly useful signposts for tracking cybercrime . . . ." From discussions not only within the COA membership, but also with cybersecurity and anti-abuse experts and law enforcement personnel, it is clear that generally the most critical data element for discovering and mitigating against a wide range of abuse and illegal activity is the registrant e-mail address. And the imperative for the registrant e-mail address to remain in public WHOIS is so that it can facilitate the rapid enumeration and correlation of information that is so vital to mitigating illegal and abusive online activity in a timely manner. See e.g., https://www.domaintools.com/resources/white-papers/how-whois-data-ensures-a-safe-and-secure-internet.

But keeping registrant e-mail address in public WHOIS doesn't just serve third-party, public consumer protection, law enforcement and security interests. It also is important for protecting registrants themselves. As Brian Krebs notes in the above-referenced blog, "the overwhelming majority of phishing is performed with the help of compromised domains, and the primary method for cleaning up those compromises is using WHOIS data to contact the victim . . . ."

Because the registrant e-mail address is typically one of the most accurate data elements of WHOIS, maintaining it in public WHOIS serves the data accuracy principle of the GDPR. (See Article 5(d): "Personal data shall be: . . . accurate and, where necessary, kept up to date.") Finally, the fact that an e-mail address of a natural person registrant constitutes personal data does not automatically exclude it from display in public WHOIS. As the European Commission noted in its Technical Input on Proposed WHOIS Models on behalf of the European Union, "the Article 29 Working Party, in its correspondence with ICANN, does not exclude a possible publication of some personal data, as long as this is justified in light of the legitimate purposes pursued with the WHOIS directory and can be validly based on the legal ground of performance of a contract or the legitimate interests pursued by the controller or by a third party." See: https://www.icann.org/en/system/files/files/gdpr-comments-european-commission-union-icann-proposed-compliance-models-07feb18-en.pdf.

Under the GDPR, registrars and registries have a legitimate interest to process WHOIS data including email address as part of registration for a domain name. The legitimate interest pursued by registrars and registries is to process this data in order to maintain a safe and secure Internet including protecting the registrants themselves from fraudulent activities. As noted above, the processing (and public display) of email address of the registrant is necessary to support that interest in order to provide the ability to contact victims and other affected parties, identify cyber criminals, and thwart widescale fraud. The legitimate interests of these goals and necessary uses is appropriately balanced against the registrant's individual interests, as required

by GDPR; in these instances, the registrant knowingly engages in a transaction to obtain a domain name, knowing that the internet ecosystem relies on transparency and maintaining a safe and secure Internet. The registrant's privacy interest is genuine, but in this discrete situation, the legitimate interests—of the data controller, of a wide range of third parties, and indeed of registrants themselves—in maintaining a safe and secure Internet by providing registrant email address in public WHOIS outweighs that individual privacy interest.

Thus, we strongly believe that the strength and breadth of the legitimate interests that depend upon the registrant e-mail address remaining in public WHOIS justify its continued inclusion in public WHOIS under the ICANN interim model, and that such inclusion would be compliant with the GDPR.

Reasons Why Anonymized or Message Relay Link E-mail Does Not Suffice

Substituting an anonymized, masked or message relay link ("anonymized e-mail") instead of the registrant's actual e-mail address in public WHOIS will thwart a number of critical legitimate purposes. While such an anonymized e-mail, if properly and consistently implemented, may facilitate communication with the registrant, it prevents the ability to readily investigate and link domains and actors together that are involved in abusive and illegal activity. Furthermore, where the message relay system fails or a registrant's e-mail address does not function, a third-party will have no way to know that, unless the registrar is required to communicate that fact back to such third-party. This would not only place a new burden on the registrar, but also it would delay investigative and enforcement work.

Requiring registrars to transition to an anonymized e-mail system within the next 3 months will likely lead to chaos and inconsistencies. It is unrealistic to assume that all registrars will fulfill this additional obligation in this time frame. By contrast, simply populating public WHOIS with the e-mail address that the registrar has already received from the registrant and verified would impose no additional burden on registrars. The burden on ICANN to monitor and enforce compliance with the transition to anonymized e-mail will be far greater as well than it would be if registrant e-mail remained in the publicly accessible WHOIS.

Furthermore, it is unlikely that any single particular form or method of creating such anonymized e-mail addresses will be implemented consistently across gTLD registrars. Therefore, no unique identifiers—even in anonymized fashion—will exist on a registrant-by-registrant basis across domains. As a result, investigation and mitigation of abusive and illegal online activities—particularly those that are supported from a large number of domains—will be crippled.

Thank you for your consideration of this letter. We hope that the articulation of the important reasons for continuing to include the registrant's e-mail address in public WHOIS will be well-received and accommodated in the interim WHOIS model that ICANN settles upon. We remain at your disposal to discuss these issues and we have raised them with other members of the ICANN community as well.