



Etienne Sanz de Acedo
Chief Executive Officer

655 Third Avenue, 10th Floor, New York, NY 10017-5646, USA
t: +1-212-642-1776 | f: +1-212-768-7796
inta.org | esanzdeacedo@inta.org

Submitted to: gdpr@icann.org

March 10, 2018

Mr. Goran Marby
Chief Executive Officer
ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Re: Proposed Interim Model for GDPR Compliance (the “Calzone Model”)

Dear Mr. Marby:

The International Trademark Association (“INTA”) appreciates this opportunity to comment on the Proposed Interim Model for GDPR Compliance (the “Calzone Model”) published by ICANN Org (“ICANN”) on February 28, 2018.¹ INTA’s views on the merits of the Calzone Model are informed by its mission as an association “dedicated to supporting trademarks in order to protect consumers and to promote fair and effective commerce.”² This belief that trademarks protect consumers is itself based on a more fundamental conviction that attribution fosters accountability.³

Dating back to stonecutter signs and cattle brands (hence the word “brand”), trademarks have always been, at their core, source identifiers: they are designations used to identify and distinguish the goods or services of one person or entity from those of another. This attribution fosters accountability, creating an incentive for sellers to maintain a predictable, consistent quality for their products. That consistency, in turn, protects consumers, who can rely on trademarks to make quick, confident, and safe purchasing decisions. That accountability also protects consumers by assigning responsibility to brand owners. Without trademarks, a seller’s low-quality products would be untraceable, leaving consumers without any recourse for faulty, deficient, or unsafe goods.

¹ <https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf>.

² <http://www.inta.org/About/Pages/Overview.aspx>.

³ The link between transparency and accountability is a fundamental tenet not just for INTA but also for ICANN, as reiterated in Article III of the ICANN Bylaws and the 2009 Affirmation of Commitments with the United States Department of Commerce. See <https://www.icann.org/resources/pages/governance/bylaws-en/#III> and <https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en>.

The existing WHOIS system (“WHOIS”)⁴ has for many years performed a similar function to that performed by trademarks – specifically, fostering accountability through attribution – which has in turn helped to ensure the stable and secure operation of the Internet’s unique identifier systems. Access to registrant data in WHOIS is a fundamental tool that is universally used to detect, prevent, and address a wide range of harms, including: 1) sites that offer counterfeit goods and services; 2) sites that support schemes that perpetrate identity-theft, steal credit card information, and divert funds to large-scale criminal enterprises; and 3) domains/sites that cloak themselves with the legitimacy of a familiar brand like that of a trusted financial institution or retailer (or offer access to infringing music, movies and other content) as a means to distribute malware and perpetrate fraud.

Access to accurate WHOIS information also supports a range of other activities necessary for the conduct of business and facilitation of commercial, social, and economic activities, including those that support democracy and access to accurate information (*i.e.*, helping media consumers to identify fake news). Without access to reliable and accurate WHOIS data, efforts to protect consumers will be thwarted, leading to a rise in abusive activity, damage to cybersecurity, diminished trust in online marketplaces, and increased costs and burdens for public law enforcement agencies, cybersecurity professionals, registrars, registries, and consumers.

INTA strongly supports ICANN’s stated desire “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.”⁵ However, we are concerned that the Calzone Model falls short of that worthy aim in at least three ways that we discuss below.

1. The Proposed Model Over Applies the GDPR

The proposed model over-applies the GDRP in that it would apply globally to all registrants whether natural or legal persons. As noted in various community conversations about GDPR compliance, while it makes sense that any compliance model would be applied to all contracted parties and registrants within the European Economic Area (“EEA”), it does not follow that the Calzone Model (or any interim compliance model) “may” also then be applied globally. Nor does it follow that the Calzone Model would apply to registrations of both natural and legal persons, given that data of legal persons (to the extent such data does not reflect “personal data”) is not within the scope of the GDPR (as ICANN’s own legal advice and many other authorities have noted).⁶

ICANN concedes that there are concerns that the Calzone Model is an over-application of the GDPR, and is inconsistent with ICANN’s stated objective to maintain the existing WHOIS system to the greatest extent possible.⁷ Yet in both cases, ICANN’s response to valid concerns is simply

⁴ As in the Calzone Model, this document uses the term “WHOIS” for ease of reference, but is intended to cover Registration Data Directory Services generally. Calzone Model at pg. 1 fn. 1.

⁵ See, *e.g.*, <https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance>; <https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year>.

⁶ See, *e.g.*, <https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf>; <https://www.icann.org/en/system/files/files/gdpr-comments-gac-icann-proposed-compliance-models-29jan18-en.pdf>.

⁷ Calzone Model at pg. 5.

to assert that “it may be difficult in practice” for registries and registrars to do otherwise.⁸ INTA members are puzzled by this response. Even if the assertion is true,⁹ it is not dispositive. INTA supports the position of the Intellectual Property and Business Constituencies that contracted party expediency is not an adequate justification for substantially overbroad application of a model that goes well beyond the scope of the GDPR and is contrary to ICANN’s aim of preserving the existing WHOIS as much as possible.

2. An Actual Email Address is Not Included in Public Facing Whois Data

The Calzone Model proposes that the public WHOIS no longer include the registrant’s actual email address (as supplied by the registrant to the registrar and then verified by the registrar).¹⁰ This represents a significant change to the existing WHOIS, and would detrimentally impact law enforcement, consumer protection, and cybersecurity/anti-malware efforts. As others have noted,¹¹ the registrant’s email address is typically the most important data point to have for those efforts. It is often the most accurate data point (since a working email address is necessary for the registrar and registrant to communicate about payments, expirations, etc.). It enables investigators to link domains and actors together that are involved in abusive and illegal activity (for example, through Reverse WHOIS). And it enables investigators to identify the victims of phishing scams performed with the help of compromised domains.

The Calzone Model’s response to these concerns (and others) is to offer a purported compromise whereby the public WHOIS would, instead, include an anonymized email address or a web form from which messages could be forwarded to the registrant’s email address.¹² But that solution, even if ICANN assumes that it is practically feasible, is not a valid substitute for publication of the registrant’s verified email address. As others have noted,¹³ while an anonymized email may facilitate communication with the registrant, there is no way for an investigator (whether it be for a brand owner, or law enforcement, or otherwise) to know if that communication was received by the registrant (unless the registrar is required to communicate that fact back to the sender). Moreover, unless these anonymized emails will exist as unique identifiers on a registrant-by-registrant basis across all domains and across all registrars and registries (which seems unlikely), the Calzone Model’s proposal will not allow investigators to link together domains and actors that are involved in patterns of abuse and illegal activity.

⁸ *Id.* (“Furthermore, **it may be difficult in practice** only to apply the changes to collection and processing linked to the European Economic Area depending upon how an individual registry or registrar has set up its systems.”); (“Also, **it may be difficult in practice** to check millions of registration records and distinguish between registrations of legal and natural persons.”) (emphasis added).

⁹ ICANN provides no support for its assertion that preserving the existing WHOIS as much as possible may be “difficult in practice” for registrars and registries – which makes evaluating or responding to this *ipse dixit* challenging. How difficult will it be? According to whom? Based on what evidence?

¹⁰ Calzone Model at pg. 6.

¹¹ See, e.g., <https://www.icann.org/en/system/files/files/gdpr-comments-coa-icann-proposed-compliance-models-16feb18-en.pdf>; <https://www.icann.org/en/system/files/files/gdpr-comments-ipc-icann-proposed-compliance-models-29jan18-en.pdf>.

¹² Calzone Model at pg. 6.

¹³ See, e.g., <https://www.icann.org/en/system/files/files/gdpr-comments-coa-icann-proposed-compliance-models-16feb18-en.pdf>.

The biggest flaw in the Calzone model’s “anonymized email” compromise is that ICANN has not provided any evidence that the solution can plausibly be implemented in the next three months. To the contrary, ICANN concedes that “It should be noted that there are concerns regarding the timeline for implementation of anonymized email or web forms.”¹⁴ To put in another way, it will be “difficult in practice” for registrars and registries to transition to the anonymized email system in time. That assertion seems correct and it also begs the question as to when ICANN thinks that contracted party expediency (“difficult in practice”) should be material to the interim compliance model and when it should not.

In the context of the EEA vs. global and natural vs. legal person distinctions that were discussed above, ICANN apparently concluded that “difficult in practice” should be dispositive. But then in its analysis of its anonymized email proposal, ICANN apparently concluded that “difficult in practice” is merely a point that “should be noted.” INTA urges ICANN to address this discrepancy.

3. Continued Access to Whois is Not Well Defined

The third and most concerning shortcoming of the Calzone Model is that it does not answer what may be the most important question of any interim compliance model, “who can access non-public WHOIS data, and by what method”. Instead, the Calzone Model only notes that registrars and registries would provide access to non-public registration data “for a defined set of third-party requestors certified under a formal accreditation program” that would be “based on pre-defined criteria and limitations.”¹⁵ But the Calzone Model does not define: 1) who would be included in that set of third-party requestors (although apparently at a minimum it would include law enforcement groups and intellectual property lawyers); or 2) what the criteria and limitations would entail.¹⁶ Nor does the Calzone Model provide a timeline for when the accreditation program would have to be finalized or the process by which it will be developed. Instead, the Calzone Model notes only that the accreditation model would be developed in consultation with the GAC.

And what happens if, as seems certain, the accreditation program that the Calzone Model envisions is not finalized by the time that layered access is to be implemented? The Calzone Model does not say.¹⁷ That omission is glaring and highly problematic.

To take only one example, ICANN’s legal counsel has advised ICANN that there is a legitimate interest for trademark owners to be able to identify (not merely to contact) a domain name holder in the event of potential trademark infringements.¹⁸ In such cases, it is necessary to verify the identity of the domain name holder so that the business for which the domain name is used can be identified and assessed in relation to the holder’s trademarks.¹⁹ Under the Calzone Model, in which the registrant’s name, email address, phone number, and fax number would not be publicly available, this legitimate interest would be thwarted unless trademark owners have access to non-

¹⁴ Calzone Model at pg. 6.

¹⁵ *Id.* at pg. 7.

¹⁶ The Calzone Model does provide in Attachment 2 the outlines of a “possible approach” for an accreditation program. Calzone Model at pgs. 12-15. But that is only one “possible” approach.

¹⁷ All that the Calzone Model says on this question is that “self-certification” as an “interim” solution “would raise a number of questions that would need to be addressed to comply with the GDPR.” Calzone Model at pgs. 7-8.

¹⁸ <https://www.icann.org/en/system/files/files/gdpr-memorandum-part3-21dec17-en.pdf> at pg. 9.

¹⁹ *Id.* Note that this is not the only legitimate interest – or even the only legitimate interest related to intellectual property – identified by ICANN’s counsel.

public WHOIS data via an accreditation program. ICANN has not committed that the accreditation program will be implemented as of the date that the Calzone Model goes into effect. It is of little consolation that such a gap may be remedied by some undefined program at some indeterminate date in the distant future. The legitimate interests of trademark owners and the consumers they protect will not go away and should not be impeded however long an undefined “interim” may last.

20

4. Recommended Improvements to the Calzone Model

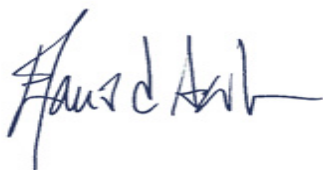
To address the aforementioned concerns, INTA recommends that any interim compliance model should:

- 1) Be applied to contracted parties and registrants within the EEA.
- 2) Distinguish between registrations of natural and legal persons.
- 3) Allow for publication in the public WHOIS of the registrant’s actual email address (as supplied by the registrant to the registrar and then verified by the registrar).
- 4) Include a specific “Day One” solution for accessing non-public WHOIS data. INTA understands that ICANN will need to eventually develop and implement a true accreditation program. However, there must be some alternative mechanism in the interim. INTA supports some form of self-certification plus credentialing as an interim mechanism.
- 5) Address the need to search across data sets using email addresses or maintain port 43 and bulk access to identify patterns of domain name abuse
- 6) Prescribe a compliance remedy for contracted parties who decline to follow the proposed model such as de-accreditation.

INTA thanks ICANN org for its consideration of this submission.

For more information about INTA and its policies, you may contact Lori Schulman, Senior Director for Internet Policy, lschulman@inta.org.

Sincerely,



Etienne Sanz de Acedo
Chief Executive Officer

²⁰ <https://www.icann.org/en/system/files/files/gdpr-comments-ipc-hamilton-analysis-part3-09jan18-en.pdf>.