



Saturday, March 10, 2018

By Email

Mr. Göran Marby
ICANN President and CEO
goran.marby@icann.org

Mr. Cherine Chalaby
Chair, ICANN Board
cherine.chalaby@icann.org

Mr. Rod Rasmussen
Chair, SSAC
rod@rodrasmussen.com

Ms. Manal Ismail
Chair, GAC
manal@tra.gov.eg

Re: Critical RAA Violation; GoDaddy Port 43 Whois Masking & Throttling Programs

Dear Cherine, Manal, Rod and Göran:

A matter of urgency requires your immediate attention and ICANN Org action. In violation of the RAA, over the past few months GoDaddy has unilaterally significantly reduced access to Whois data that the global Internet community relies on to investigate and enforce against criminal activity, malicious conduct and intellectual property infringement online. ICANN Compliance has not appropriately enforced GoDaddy's contractual obligations and we ask that you ensure they do so, immediately.

On 12 January 2018, GoDaddy, the world's largest domain name registrar, announced its intention to [mask registrant, technical and administrative contact details](#) across all "non-white-listed" port 43 Whois queries. Entities must now submit a specific "white-list" request to GoDaddy to access port 43 Whois data, which is granted—or modified or denied (as repeatedly has been the case)—at GoDaddy's sole discretion. Whether someone accesses port 43 directly, or relies on third party tools that depend upon unfettered automated access, this unilateral change has had a profound and negative impact on the ability to detect and remedy illegal activity. In short, the tools that we depend upon to do our jobs on a daily basis are now compromised or broken.

The recent changes constitute several clear and direct violations by GoDaddy of their contractual obligations to ICANN.¹

GoDaddy has repeatedly asserted that these changes were made to "slow the flood of spam" to their customers. However, the changes apply by default and across the board to all domain names sponsored by GoDaddy, without any regard to the actual identity of requestors for port 43 access, or the actual bad actors who perpetrate spam. On the contrary, nothing in their contract permits GoDaddy to mask data elements, and evidence of illegality must be obtained before GoDaddy is permitted to throttle or deny port 43 Whois access to any particular IP address.

Our initial outreach to the ICANN Contractual Compliance Department on this matter was met with a dismissive template response replete with irrelevant references to web-based Whois access, as well as an inexplicable suggestion that we reach out to GoDaddy for placement on their port 43 whitelist. To be clear, web-based Whois access is completely irrelevant, since law enforcement, anti-abuse and intellectual property communities all depend upon automated access through port 43. Whitelist access is also completely irrelevant for the vast array of those in the community who depend upon third party

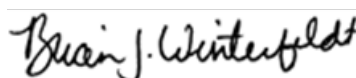
research and analytical tools. Moreover, the placement of unmasked port 43 Whois data behind a whitelist constitutes a contractual violation in and of itself.

The GoDaddy whitelist program has created a dire situation where businesses dependent upon unmasked and robust port 43 Whois access are forced to negotiate wholly subjective terms for access, and are fearful of filing complaints with ICANN because they are reticent to publicize any disruption in service, or because they fear retaliation from GoDaddy.

Continued outreach to the ICANN Contractual Compliance Department on this matter has been met with assurances that compliance inquiries have already been made, but that they are currently stalled in view of purported “cooperation” from GoDaddy and the sustained “anti-spam” justification. However, with knowledge of these obvious black-letter contractual violations, ICANN must simply enforce the contract, rather than engage in any protracted dialog with GoDaddy about the reasons why they feel these violations might be justified. That sort of dialog belongs squarely in the contractual amendment and policy development processes.

This is a very serious contractual breach, which threatens to undermine the stability and security of the Internet, as well as embolden other registrars to make similar unilateral changes to their own port 43 Whois services. It has persisted for far too long, having been officially implemented on January 25, 2018. The tools our communities use to do our jobs are broken. Cybersecurity teams are flying blind without port 43 Whois data. And illegal activity will proliferate online, all ostensibly in order to protect GoDaddy customers from spam emails. That is completely disproportionate and unacceptable and we ask for your commitment to take all steps necessary to force GoDaddy to immediately cure these blatant contractual violations, in service of ICANN’s mandate to act in the global public interest.

Sincerely yours,



Brian J. Winterfeldt
Winterfeldt IP Group, PLLC

-
- ⁱ With respect to any gTLD operating a ‘thin’ registry, GoDaddy must provide a port 43 WHOIS service for free public query-based access to up-to-date data concerning all active registered names sponsored by GoDaddy in any gTLD, to include at a minimum the name and postal address of the registered name holder, as well as the name, postal address, email address, and voice telephone number of the technical and administrative contacts.
 - GoDaddy must avoid placing any terms and conditions on the use of the data provided, except as permitted by ICANN, including unlawful uses for spam and denial of service attacks.
 - GoDaddy must also maintain availability of port 43 WHOIS and web-based WHOIS services with less than or equal to 864 minutes of downtime per month, and respond to port 43 WHOIS and web-based queries within 4000 milliseconds for at least ninety-five percent of queries.

See [Registrar Accreditation Agreement](#), §§ 3.3.1, 3.3.1.7-8, 3.3.5, and Registry Directory Service (Whois) Specification § 2.2 (Sept. 2015).

BRIAN J. WINTERFELDT