

2018-10-21

To:

Goran Marby, CEO, ICANN
Cherine Chalaby, Chair, ICANN
Jamie Hedlund, VP Compliance, ICANN

Re: Third Party Requests to Registrant Data

Dear Goran, Cherine, and Jamie:

Tucows would like to address the issues regarding third-party access to data raised by AppDetex from the perspective of a Registrar. First, we should note that Tucows understands that there are reasonable and legitimate needs for third parties to gain access to our Registrants' data. We have provided Registrant data for over one hundred requests to numerous third parties where our requirements for disclosure have been met. These requirements are not an outrageously high bar, indeed, some may argue they are too permissive. A generic version of our typical data request response has been included as an appendix to this letter.

We were quite pleased to read in the letter to Goran and Cherine dated October 12th, 2018 that AppDetex has begun to rework their processes. It has been frustrating for us to operate as their external quality assurance team, as it's not typically part of our business strategy to assist other companies in this manner. AppDetex has submitted (as of this letter) 1273 requests for Registrant data to Tucows-family registrars. Up until October 9th, 2018, we responded with our requirements template to all of them and had not received a single reply. The claim in their letter of contracted party failures to respond in a reasonable time frame is *outrageous* as they have failed to further their own requests for months. This alone should be reasonable grounds for us to ban AppDetex permanently as a vexatious reporter, a course of action we're considering.

Digging into some of these requests for Registrant details reveals an alarming lack of care. Registrant information for domains like "lincolnstainedglass.com" and "griffinstafford.com" was requested, presumably because they homographically contain a similarity to a portion of Facebook's trademark "instagram". That no human reviewed these domains was obvious, as the above examples are not isolated.

Further, literally hundreds of requests were sent multiple times, further burdening our team. In a number of examples, we even have Registrant data requests being submitted for the same domain by multiple domain protection services. Some requests for Registrant data also veer into dangerous territory, where they are for domains like "facebookucks.org" which is a clear domain example of fair-use. We would be extremely alarmed to be implicated in a scheme to limit free speech.

AppDetex has also not limited themselves to the Registrant data that would have been available via Whois prior to GDPR. For example requesting reverse lookups, a service for which we have always required a subpoena. This is not, as they proclaim, a problem. This is, rather, appropriate due process.

On October 9th, 2018, AppDetex began including *some* of the information requested in our template response, including a specific person to whom we could grant access to our [Tiered Access Compliance and Operations](#) portal, which we have created expressly to facilitate the provision of data when appropriate. This tool supports “tiers” of access for law enforcement, security researchers, and commercial litigation, each upon a showing of legitimate use.

We are also concerned that, given the clear lack of human-review and due care presented by the requests we have received from AppDetex, they are simply creating algorithms to identify *potential* infringements and demanding personal Registrant data for these potentialities wholesale. The examples we have noted above—and many others—could have been easily identified by AppDetex prior to submitting to Tucows if they had included the *reason* that the domain was suspected to be infringing, rather than the mere assertion that it “misuses one or more of the following trademarks” and then listing seven trademarks. We require that requests for personal data include the reason for the valid request.

AppDetex has yet to demonstrate that they are compliant with the GDPR, specifically Chapter V, which addresses how to accept transfer of data from the EU. Indeed, AppDetex has no DPO listed on its website, a glaring lack for an entity intent upon receiving so much data. We are concerned about sending data outside of the EU without such guarantees in place.

Lastly, we should point out the timing of AppDetex’s letters and process changes. Our first batch of hundreds of requests arrived just prior to ICANN 62—just in time for AppDetex to make a presentation to the GAC and the Board, painting Registrars as bad actors. We have waited literally months for any reply to our requests for assurances and somehow, less than two weeks before ICANN 63, and a mere three days before AppDetex sent you a letter decrying contracted parties, we receive responses. That would have been just three days to work through the more than 1200 long request backlog they created. It is apparent to us that the concern here is not for the trademarks of Facebook, or any other customer, but for generating baseless noise and attempting to shift public and government perception of Registrars.

Regards,

Elliot Noss,
CEO, Tucows

Appendix A: Tucows Generic Data Request Response

To Whom It May Concern at [REDACTED]

Thank you for contacting us. We acknowledge receipt of your request for underlying whois data for the following domain name(s):

[REDACTED]

In order to maintain compliance with our obligations under the GDPR, before we can respond to your request, we will require the following:

1. Your full name and contact details.
2. A statement, on the letterhead of the party you represent, that you represent them and their interests with regard to this request. If you are that party, a statement on your own letterhead indicating that the email address used is authoritative with respect to this request. If you are a private person acting on your own behalf, a statement of that.
3. A statement, under penalty of perjury, that the information in your request is accurate.
4. A statement, under penalty of perjury, that requested data are related to a good-faith belief that the rights of you or the party you represent have been violated and the data you are requesting is required to further pursue assertion of those rights.
5. A statement, under penalty of perjury, that the personal data that you receive will be processed in a legally-compliant manner at all times, not stored, transferred, or otherwise shared without legitimate interest, and deleted as soon as it is no longer needed to pursue this assertion of rights.
6. Your electronic signature.

Sincerely,
the Tucows GDPR Team