ICANN | IPC

RE: ***Internet Corporation for Assigned Names and Numbers vs. EPAG Domainservices GmbH (LG Bonn, 10 O 171/18)***

INTRODUCTION

As a member of the Internet Corporation for Assigned Names and Numbers (ICANN) multistakeholder community, the Intellectual Property Constituency (IPC) respectfully requests that the Court consider the following submission in support of ICANN's request for an injunction against EPAG Domainservices GmbH to mandate the continued collection of Administrative and Technical Contacts for the WHOIS/Registration Data Directory Services (WHOIS/RDDS).

On May 30, 2018, the German Regional Court (LG Bonn) ruled in the Internet Corporation for Assigned Names and Numbers (ICANN) vs EPAG Domainservices GmbH (LG Bonn, 10 O 171/18) that ICANN did not demonstrate that it is necessary to collect additional data elements for these contacts beyond what is provided by the Registrant in other data fields. The court did not rule that collection was a violation of GDPR, but rather that mandating the collection of this data was essentially superfluous and therefore beyond the scope of what is necessary to achieve the purpose of data collection for WHOIS/RDDS.

The IPC wishes to draw the Court's attention to several reasons why it is necessary for registries and registrars to collect additional data elements beyond what is provided by the Registrant in other data fields – whether to themselves or a third party – and why doing so serves a legitimate purpose that does not violate the privacy rights of the Registrant. For this reason the contractual provisions that mandate the collection of these data fields by domain name registrars are not in violation of the General Data Protection Regulation (GDPR), (EU) 2016/679, and accordingly should be preserved, in order to serve various legitimate interests as discussed further below.

Respectfully, the Court may not have taken into full account the additional utility and importance of the Administrative and Technical Contact details and ICANN's stated purpose for processing, namely "contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name."[1] We write today to provide additional context about the

[1] *See e.g.,* 2013 Registrar Accreditation Agreement, Section 3.7.7.3, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa (Retrieved July 10, 2018).

importance and purpose of the collection of this data, especially to ensure a secure domain name system that "enable[s] legitimate uses by relevant stakeholders," a key function of WHOIS/RDDS as acknowledged by the European Data Protection Board (EDPB)[2] and why collection of this data is "adequate, relevant and limited to what is necessary" in accordance with Article 5, para 1(c) of GDPR.

THE IMPORTANCE OF WHOIS/RDDS DATA

As acknowledged by the EDPB's predecessor, the Article 29 Working Party (WP29), in a statement later endorsed by the EDPB on May 27, 2018,[3] WHOIS/RDDS fulfills important purposes, and indeed is necessary for a number of critical functions related to cybersecurity and the protection of Registrant interests, ICANN's interests, and various other legal interests.

Access to WHOIS/RDDS information is a critical tool for many stakeholders in the Internet community that support vital public and private interests, including but not limited to law enforcement, cybersecurity research, intellectual property rights enforcement and consumer protection. The Governmental Advisory Committee (GAC) of ICANN, the IPC, the ICANN Business Constituency, and the Internet security community, among others, have written extensively about this topic.[4] Given the global, distributed and decentralized nature of the Internet (a "network of networks") that extends beyond traditional jurisdictional boundaries, the ready and efficient ability to identify and contact individuals associated with a domain name registration, and with appropriate facility to timely resolve any problems that arise in connection with a domain name, is key to the continued safety, security, stability, accountability and resiliency of the Internet and its users.

THE IMPORTANCE OF ADMINISTRATIVE AND TECHNICAL CONTACT DATA

Domain name registration information collected and made available via the current WHOIS system, as required by ICANN, allows for the identification of two role-based contacts, Administrative and Technical, in addition to contact information associated with the domain name owner (Registrant) itself. These contact fields allow for the Registrant to designate additional suitable points of contact for these functions, adequate to facilitate timely resolution of any problems that arise in connection with his/her/its domain name. Administrative and Technical Contacts are also vitally important to a number of ICANN consensus policies developed by the global multi-stakeholder community over the last two decades that aim to protect the Registrant, and facilitate the efficient resolution of domain name disputes. Those policies are listed below.

---

[2] "*The European Data Protection Board Endorsed the Statement of the WP29 on ICANN/WHOIS*", https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en (Retrieved July 9, 2018).

[3] *Id*.

[4] *See e.g.*: Intellectual Property Constituency Comments to ICANN Board regarding GDPR Compliance Models, 11 May 2018, https://www.icann.org/en/system/files/files/gdpr-comments-ipc-icann-proposed-compliance-models-11may18-en.pdf (Retrieved July 9, 2018); GAC Communiqué – San Juan, Puerto Rico, 15 May 2018, https://gac.icann.org/contentMigrated/icann61-san-juan-communique (Retrieved July 9, 2018).

Typically a Registrant will specify a separate Technical Contact when the responsibility for the technical infrastructure used to service a domain name is managed by a separate entity or organization, or another individual within an organization with information technology (IT) expertise that the Registrant does not have, or prefers to outsource. Often, Registrants will delegate technical responsibility to a third-party domain name service provider such as their Registrar, web hosting provider, or another third party that specializes in providing such technical web management services. When a technical issue with the domain name arises, the ability to contact the entity or individual who has the technical ability to quickly and directly address and correct the issue is necessary to ensure the security and stability of the domain name system. An example of this is the unauthorized usurpation of a domain name by a third-party hacker for the distribution of malicious software or launching of cyberattacks. Such dangerous takeovers usually occur without the knowledge of the Registrant.[5]

Similarly, a mechanism to specify a separate Administrative Contact ensures the proper delegation of requests associated with domain name management, such as registration renewals or cancellations, purchase or sale-related inquiries or efforts, and other similar kinds of issues relating to the status, disposition, or control of the domain name.

The ability to designate separate Technical and Administrative Contacts is necessary for the stable and secure functioning of the domain name system so that the designated contact may adequately facilitate the timely resolution of any problems that arise in connection with a domain name. While the Registrant may have the facility to resolve all issues itself, that is not always the case. Requiring the Registrant to affirmatively declare themselves as able to resolve administrative or technical issues, or designate additional contacts for the timely resolution of those issues, is necessary for ICANN's stated purpose and, thus, militates collection of those data points.

Consider a small business owner with a successful online presence. To allow the owner to focus on their core business, they designate an accountant or attorney to manage and respond to the administrative issues associated with their domain name. To ensure the continued operation and availability of their web presence, including the domain name, they can designate their hosting provider or outside IT support to respond to technical issues when they occur.

In the same manner, a large Internet service provider, servicing billions of users, is well served by specifying distinct contacts. For example, they may designate their legal entity name as the Registrant, a particular individual or general point of contact in their domain name management division as the Administrative Contact and a separate individual or general point of contact in their corporate IT department as the Technical Contact. This ensures the right point of contact is notified depending on the nature of a particular issue or problem, allowing for efficient and

[5] *See e.g.*: https://krebsonsecurity.com/2018/02/domain-theft-strands-thousands-of-web-sites/ "Domain hijacking is not a new problem, but it can be potentially devastating to the victim organization. In control of a hijacked domain, a malicious attacker could seamlessly conduct phishing attacks to steal personal information, or use the domain to foist malicious software on visitors."

effective resolution and fulfilling ICANN's purpose of ensuring an adequate contact to facilitate timely resolution of any problems that arise in connection with a domain name.

The availability of Administrative and Technical Contacts also has important functions to security professionals and consumer protection organizations. For example, a cybersecurity professional can quickly identify an appropriate Technical Contact to resolve a concern that a domain name might be used in spreading malicious software (malware), or an intellectual property owner can follow up directly with an Administrative Contact to coordinate the transfer of a domain name whose acquisition was negotiated as part of a trademark enforcement settlement. Without these direct contacts, law enforcement or security professionals (for example) may suffer unnecessary delays that result in harmful consequences because the Registrant, not capable of providing timely resolution of these problems, was not required to declare the appropriate Administrative or Technical Contacts (in other words, the domain name registrar was not required to collect this information at the time of registration).

The Security and Stability Advisory Committee (SSAC), which "advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems"[6] addressed the importance of administrative and technical contact roles for maintaining control of a domain registration in its advisory, "SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts."[7] SAC044 specifically noted, among other things, that maintaining administrative and technical contacts plays a role in reducing single points of failure or attack.[8] This report was adopted by the ICANN Board and provides justification for mandating collection of this data from ICANN's perspective and from a Registrant perspective – in line with ICANN's purpose of ensuring contacts adequate to facilitate timely resolution of any problems that arise in connection with a domain name.

Even if the Registrant chooses identical contact details as their own for the purposes of Administrative and Technical functions, the fact of their self-designation for such functions serves its own purpose: it signifies that they should be treated as the relevant point of contact for technical and administrative issues. The fact that such data may be the same as the Registrant's information does not therefore render it "superfluous," since the Registrant is making an affirmative choice to specify certain details for different functions related to the operation of the domain they have registered (or affirmatively identify itself for all such points of contact).

The importance of these functions are not outweighed on their face by the privacy concerns of the contacts, especially since the contact details need not include personally identifiable information and are only provided at the designation of the Registrant itself (i.e. the Registrant can instead choose to populate these fields with its own information, thereby consenting to their processing, if it feels it is capable of adequately facilitating timely resolution of any problems that arise in connection with the its domain name and does not otherwise wish to designate alternative contacts). For example, a Registrant can insert domainadmin@company.com or

---

[6] *What is the SSAC?* https://www.icann.org/groups/ssac (Retrieved July 9, 2018).
[7] *SAC044: A Registrant's Guide to Protection Domain Name Registration Accounts*, 6 November 2010, https://www.icann.org/en/system/files/files/sac-044-en.pdf (Retrieved July 9, 2018).
[8] *Id*. at 15.

technicalsupport@company.com to avoid publishing personally identifiable information in these WHOIS contacts.

Additional information about these data fields and the legitimate uses of this data can be found in the ICANN community-developed *gTLD Registration Dataflow Matrix and Information*,[9] which highlights the uses of each data field in WHOIS/RDDS.

ADMINISTRATIVE AND TECHNICAL CONTACT DATA IS USED TO FULFILL THE FOLLOWING ICANN CONSENSUS POLICIES

- ICANN Transfer Policy, which supports robust competition in the domain name industry. Confirmation of a request to transfer a domain name from one registrar to another prevents domain name "hijacking" or unauthorized theft of the domain name.
- ICANN's Transfer Dispute Resolution Policy grants administrative contacts the right to contest an unauthorized transfer of the domain name. This serves a similarly important "consumer protection" safeguards for the registrant.
- ICANN's Expired Domain Name Recovery Policy specifies that notice of expiration can be sent to the administrative contact for a domain name.
- ICANN's WHOIS Data Reminder Policy is sent to administrative contacts annually to ensure that the domain name registrant's contact data is up to date and accurate.
- ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) and Uniform Rapid Suspension (URS) system are domain name dispute resolution mechanisms to resolve cyber-squatting, and which require that service of process of the complaint be made on the administrative contact and the technical contact in WHOIS, in addition to the registrant. By requiring service on all of the contacts in the WHOIS, registrants are better protected in terms of due process and notice of service, and are less likely to fail to receive a complaint or ignore the complaint, which could result in a default judgment that could cause them to lose their domain name.

CONCLUSION

The collection of WHOIS/RDDS data is mandated by contracts carefully considered and developed by the ICANN multistakeholder community to benefit ICANN, Registrants and third parties with legitimate interest in the maintenance of WHOIS/RDDS. Each data element is relevant and serves an important function and purpose to ensure contacts adequate to facilitate timely resolution of any problems that arise in connection with a domain name -- furthering the stable and secure operation of the domain name system as a whole. In addition, each of the data elements fulfills a legitimate interest for ICANN and for an array of Internet stakeholders, many of whom are acting in the public interest. Since the collection of the data elements at issue are not in violation of the GDPR, ICANN's stated purpose for processing, being "contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name," must be fully considered before allowing contracted parties such as EPAG to restrict such data collection and processing in the name of GDPR compliance.

[9] *gTLD Registration Dataflow Matrix and Information,* 6 November 2017, https://www.icann.org/en/system/files/files/gdpr-dataflow-matrix-whois-06nov17-en.pdf (Retrieved July 9, 2018).