LOEB & LOEB LLP

Brand Protection

MAY 2018

Who is Responsible for the Privacy of Domain Name Contact Information?

Anyone who has tried to take down an infringing website or obtain transfer of an infringing domain name understands the value of the WHOIS service. Prior to last Friday, any internet user could obtain the identity and contact information of any domain name registrant by checking the WHOIS database, with the exception of registrants who used a privacy service to shield that information. Due to the implementation on May 25 of the European Union's General Data Protection Regulation (GDPR), ICANN has had to reexamine the collection and processing of personal data of Data Subjects, by registry operators and registrars, among others in the domain name ecosystem. This Alert discusses ICANN's proposal for bringing the WHOIS service into compliance with GDPR, and provides some guidance for brand owners and others who have historically relied upon the WHOIS service for enforcement of intellectual property rights online.

ICANN's Plan for Complying with GDPR

ICANN – the Internet Corporation for Assigned Names and Numbers – is a nonprofit organization responsible for Internet Protocol (IP) address space allocation and generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, among other internet functions. Historically, ICANN has required that ICANN-accredited domain name registrars (such as GoDaddy and Network Solutions) ***collect the personal data of every domain name registrant***, provide it to the registry operator and a data escrow provider, and ***publish the information*** through a WHOIS lookup service. Typically, the WHOIS data for a domain name includes the registrant's name, email address, phone number and mailing address. Although ICANN provides its own WHOIS lookup tool, the WHOIS data is managed at the level of each registry, and is not stored by ICANN in a centralized database.

ICANN faces two separate issues in light of GDPR: the scope of the data collected for a domain name registration (personal data of the registrant, admin and tech contacts) and the publication or sharing of such personal data through ICANN's gTLD Registration Directory Service (RDS) or a registrar's WHOIS service. The European Commission's data protection advisory body informed ICANN in April that ICANN's earlier proposed adjustments to the RDS and its practice of collecting personal data of domain name registrants were both incompatible with GDPR.

On May 17, ICANN announced temporary restrictions on the disclosure of WHOIS data. According to ICANN's Temporary Specification for gTLD Registration Data (Temporary Specification), registrars and registries will continue collecting the same registration data from individuals and legal entities in connection with a domain name registration. ICANN submits that there are at least 13 justifications for continuing the collection and processing of personal data in addition to intellectual property protection, including ensuring contractual compliance by registries and registrars, investigation of cybercrime and domain

name system (DNS) abuse, and ensuring that a domain name registrant can exercise its rights with respect to its domain name.

The Temporary Specification directs all registries and registrars to restrict the publicly accessible WHOIS data to technical data sufficient to identify the sponsoring registrar, the status of the registration, and creation and expiration dates for each registration, ***but not to identify personal data***. ICANN still requires the collection of a registrant's personal data so that users "with a legitimate purpose" may have access to this data. ICANN has mandated that each registrar and registry comply with GDPR requirements during the gathering, processing and escrowing of the personal data of registrants. Because limiting personal data handling requirements to the European Economic Area (EEA) may be impractical for non-European registrars, the Temporary Specification permits registrars to apply the requirements to domain name registrations on a global basis. While easing the burden on registrars, this means that WHOIS data is likely to be shielded from public access in a much wider scope than GDPR would require.

Even though, in most cases, brand owners will not have access to an email address, street address or phone/fax number that would ***identify*** domain name registrants, they will still be able to ***contact*** a registrant by using an anonymized email address or a web form (which will replace the "email" field of every contact for a domain name registration).

In addition, the Temporary Specification indicates the following:

- ICANN will amend the Registry and Registrar Accreditation with Registry Operators, Registrars, Data Escrow Agents, and any other parties handling personal data to ensure compliance with GDPR.
- Registries and registrars must redact the following information ***unless*** the registrant has provided consent to publish the data: registry registrant ID and registrant's name, street, city, postal code, phone and fax. The same information will be redacted for the Admin/Tech/Other contact for a domain name registration.
- A tiered/layered access framework for the processing of personal data will be implemented to reduce the risk of unauthorized processing of personal data.
- Registrars/registries established in the EEA or who use a processer located within the EEA to process personal data must comply with ICANN's GDPR compliance proposal.
- The new requirements will apply to both legal and natural persons.

Because there is not a uniform procedure in place to access personal data stored in RDS and WHOIS, ICANN is developing an accreditation program for a broader scope of access to the stored personal data of domain name registrants. ICANN plans to publish the specifics of its "Registration Data Access Protocol" on July 31, 2018. Until that time, however, registries and registrars will individually determine which requests are permissible under GDPR.

Impact on Domain Name Dispute Proceedings

Both the Uniform Rapid Suspension (URS) and Uniform Domain Name Dispute Resolution Policy (UDRP) provide avenues for brand owners to submit a complaint that a domain name is infringing upon the brand owner's registered mark. Historically, the UDRP and URS rules have required complainants to serve the complaint upon the domain name registrant at the contact information provided through the WHOIS service. ICANN's Temporary Specification now supersedes the UDRP and URS rules with respect to issues addressed in the Temporary Specification. UDRP and URS complaints will not be deemed defective if the name or other contact information of the domain name registrant is not included due to the inavailability of such data in RDS or WHOIS, and if such information is not otherwise available to

the complainant. In such situations, a complainant may opt to file a “Doe” complaint. The Temporary Specification further requires that registries and registrars provide full domain name registration data (including personal data) to the URS or UDRP provider upon being notified of a complaint, and the provider must then provide the contact information to the complainant.