

Preparing for Drastic Changes to Availability of “WHOIS” Information About Domain Names

April 18, 2018

A public “WHOIS” system has been available for use by law enforcement, intellectual property owners, security researchers, domain name owners, and myriad of other Internet users to retrieve domain name ownership information for over two decades (and much longer in other forms). When the European General Data Protection Regulation (GDPR) takes effect next month, it could have a drastic effect on the availability of such information for Internet users from around the world, notwithstanding the fact that less than 10% of the world’s population resides in the European Union (EU). Internet security experts and government officials have predicted that the impending elimination of the public WHOIS system will have a significant impact on Internet security issues, and it is important for trademark and domain name owners to understand and prepare for the changes.

The EU adopted the GDPR in April 2016 to protect the privacy rights of EU citizens and residents. Under the GDPR, all companies processing and holding the personal data of subjects residing in the EU must take certain steps to protect “personal data” when it is held within Europe or when transferred to third countries. The GDPR defines “personal data” as “any information relating to an identified or identifiable natural person (a data subject).” Under Article 5 of the GDPR, personal data may only be processed for specified, explicit, and legitimate purposes.

Although the May 25, 2018 due date for GDPR compliance is fast approaching, how the GDPR applies to WHOIS data remains subject to significant debate. ICANN has declared that it has “no indication that abandoning existing WHOIS requirements is necessary to comply with the GDPR.” At the same time, ICANN has recognized that

Authors

David E. Weslow
Partner
202.719.7525
dweslow@wiley.law
Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law
Ari Meltzer
Partner
202.719.7467
ameltzer@wiley.law

Practice Areas

Cybersquatting & Internet IP
Intellectual Property
Privacy, Cyber & Data Governance
Trademark

“registries and registrars are developing their own models for handling registration data that they believe will comply with the GDPR.” Although ICANN contracts require registries and registrars to make WHOIS data publicly available, ICANN indicated that it will defer taking action against any registry or registrar that does not comply with its contractual obligations related to the handling of registration data as long as the non-complying registry or registrar: (1) shares its model with ICANN, and (2) the model reflects a “reasonable accommodation” or existing contractual obligations and the GDPR.

In response to ICANN’s guidance, several registry operators announced that they planned to suspend publication of WHOIS data, and at least one major registry operator has announced plans to begin charging fees for access to WHOIS data.

On March 8, 2018, ICANN published an *Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union’s General Data Protection Regulation*, which is available here. Under the interim model, registrars would continue to collect registrant, administrative, and technical contract information. Unless the registrant opts-in to publication of full contact details, registrars and registries would only provide meaningful WHOIS data to users with accreditation for full WHOIS access. Users without accreditation for full WHOIS access would only have access to anonymized contact information (such as a proxy email, web form, or other means). An April 11 letter from the EU’s Article 29 Working Party (a group consisting of the heads of data protection authorities from EU member states), reiterated its position that ICANN must limit public WHOIS access to comply with the GDPR, but ICANN has not yet created a process for becoming accredited to view full WHOIS data—suggesting that full WHOIS data will not be available from many registries and/or registrars after May 25.

It also appears that many registries and registrars are planning to restrict access to WHOIS data for all domain name registrations without regard to the location of the registrant, registry, registrar, or processor of the registration data. If registries and/or registrars proceed to remove the names and contact information for all registrants from the public WHOIS, this could make it significantly more difficult to research the history and ownership of domain names whether to confirm ownership for a purchase, to inquire about buying the domain name, or to pursue legal remedies for cybersquatting, security breaches, or other domain name misuse.

There are several actions trademark and domain name owners should take to mitigate the potential effects of the GDPR.

1. **File Comments with ICANN Regarding Its Interim Compliance Model.** ICANN is seeking community feedback on the proposed interim compliance model and has expressly labeled the current version a “working draft for continued discussion.” Interested parties should consider commenting on everything from the legal requirement under the GDPR to refrain from public posting of full WHOIS data, the scope of the GDPR, the proposed multi-tier access model, and the requirements for accreditation. Although there is no formal deadline to provide feedback, comments should be filed as soon as possible to ensure they are fully considered – particularly given the imminence of the May 25, 2018 GDPR enforcement date.

2. **Conduct Reverse WHOIS Research Now on Domain Names of Concern.** Recognizing that some registries and registrars may disable access to full WHOIS records on or before May 25, 2018, domain name owners should conduct searches in advance of that date on any domain names of concern (whether because they may be the target of an acquisition or because they may be the subject of legal action).
3. **Insist on Pre-Purchase Due Diligence Documents.** An unfortunate side defect of the GDPR could be an opportunity for fraudulent domain name sales to increase. If access to WHOIS records becomes restricted, it may become more difficult to confirm a seller's proper ownership of a domain name. When purchasing a domain name, the buyer should insist on receiving extensive due diligence documents, including purchase invoices, account screenshots, and other documents that confirm the seller's ownership of the domain name.
4. **Consider Creative Litigation Options.** It is currently unclear whether even licensed attorneys will be able to obtain accurate WHOIS information for domain name registrants. While this may not affect actions against a domain name under the UDRP or the ACPA's in rem procedures, it may make it more difficult to identify and seek damages against the registrant of a domain name. To the extent it is impossible to identify the true owner of a domain name, litigants may still be able to proceed either with a "John Doe" action (where the domain name registrant can be revealed through discovery) or an action against a service provider for contributory infringement. The facts of each case will dictate which approach is best under the circumstances.

If you have questions about the impending "WHOIS blackout," please contact one of the attorneys listed on this alert.