Expert Q&A: WHOIS Blackout – The GDPR's Effects on UDRP Proceedings

PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

Search the Resource ID numbers in blue on Westlaw for more.

An expert Q&A with Gregory S. Shatan of Moses & Singer LLP on the blackout of domain name registrant information from WHOIS databases in light of the recently enacted EU General Data Protection Regulation (GDPR) and its effect on UDRP Proceedings. It includes useful tips for investigating potential cybersquatting claims and enforcing domain names without access to WHOIS information.

The enactment of the European Union (EU) General Data Protection Regulation (GDPR) on May 25, 2018, has made it increasingly challenging for brand owners to investigate and substantiate claims under the Uniform Domain Name Dispute Resolution Policy (UDRP).

Practical Law asked Gregory Shatan, partner at Moses & Singer LLP, for his insight on these challenges and practical suggestions for brand owners trying to protect and enforce their trademarks and domain names.

Greg is a partner in Moses & Singer's Intellectual Property group and a member of the firm's Internet & Technology practice. He focuses on intellectual property and technology transactions, counseling, and litigation, and internet and domain name law and policy. Greg has extensive experience advising and assisting with domain name and social media portfolios and regularly helps clients police and enforce their IP rights online.

HOW DOES THE GDPR AFFECT THE UDRP PROCESS?

The GDPR, enacted on May 25, 2018, governs how third parties can collect, use, analyze, display, store, retain, transfer, and delete the personal data of EU data subjects, that is, citizens and permanent residents. Protected data includes names, addresses, phone numbers, and email addresses in addition to medical, financial, and other personal details. (For more on the GDPR, see Practice Note, Overview of EU General Data Protection Regulation (W-007-9580).)

WHOIS databases are the only public source of owner information for domain names. These databases are maintained by domain name registrars and sometimes registries as part of their contractual obligations to the Internet Corporation for Assigned Names and Numbers (ICANN), which administers the domain name system (DNS). Before the GDPR, the public had easy access to WHOIS records, which contained names and contact information for domain registrants, and the domain's administrative, technical, and billing contacts. Where information was protected by privacy services, under the terms of most privacy service agreements, registrars typically facilitated communication or even provided the full WHOIS record when appropriate.

However, once the GDPR took effect, this information disappeared from public WHOIS databases around the world. This information blackout extended beyond EU data subjects, who are expressly covered by the GDPR. Records for legal entities, as well as natural person registrants who are not EU data subjects, disappeared too, because registrars and registries declined to separate GDPR-protected records from those not covered by the regulation.

Brand owners had long relied on WHOIS information for domain name protection and enforcement. In particular, WHOIS was a key source of information for investigating and pursuing cases under the UDRP. Without WHOIS access, a brand owner considering domain name enforcement may not be able to:

- Identify, investigate, and locate domain registrants who may be cybersquatters.
- Get facts about a domain name registrant that could influence whether to bring a UDRP case.
- Contact the registrant to pursue possible settlement.
- Consolidate UDRP cases where the same registrant owns multiple domain names.
- Develop the facts needed to substantiate a UDRP claim.

For more on preparing a UDRP complaint, see Standard Document, Domain Names: UDRP Complaint (0-557-3507).

HOW HAS THE LACK OF ACCESS TO WHOIS INFORMATION AFFECTED THE SUBSTANCE OF UDRP COMPLAINTS?

Without basic information like the domain name registrant's name and address, brand owners have trouble establishing the elements of a UDRP claim.

For example, it can be impossible to show that the registrant lacks rights or a legitimate interest in a domain name, a required element. Without knowing who the registrant is, a would-be complainant cannot rule out that the registrant:

- Is commonly known by a term in the domain name.
- Is one of the complainant's licensees, franchisees, or distributors.
- Has its own valid claim to the subject domain name.
- May be preparing to legitimately use the domain name in connection with a bona fide offering of goods or services in a way that does not infringe the complainant's rights.

Arguing that the registrant has registered and is using a domain in bad faith, another element of a UDRP claim, has also become much harder. Without the registrant's identity, it can be impossible to discern:

- The registrant's intent.
- Whether the registrant is a competitor.
- If the registrant is misdirecting users to its own site.
- If the registrant has a history of bad faith registration and use of domain names, such as repeatedly acquiring domain names identical to or incorporating established or well-known marks.

In some cases, brand owners or their counsel can obtain this information in other ways, including by using private investigators and following other data and internet clues. These are often more difficult, expensive, and time-consuming. Then, even if the registrant is identified, the ability to confirm this information against the WHOIS record is gone.

HAS THE NUMBER OF UDRP FILINGS DROPPED SINCE THE GDPR TOOK EFFECT?

In terms of raw numbers, there has been no noticeable decrease yet. It may be some time before we can see the true effect of the WHOIS blackout. Cases that were filed in the first few months after May 25 may have been developed before the GDPR, or perhaps the complainants relied on third-party databases built from information gathered before that time. However, these databases become increasingly obsolete every day.

It is also possible that there has been a decrease in typical UDRP filings but that it has been counterbalanced by an increase in cases where, for example:

- Amicable settlement before filing was impossible because there was no effective way for the complainant to contact the registrant.
- It was impossible for the claimant to discern, before filing, that the registrant might have a legitimate interest in the domain name.
- A complainant has filed multiple cases unknowingly against the same registrant, which could have been part of a single complaint.

HOW HAVE DOMAIN NAME REGISTRARS AND REGISTRIES RESPONDED TO THE WHOIS BLACKOUT?

Days before the GDPR took effect, ICANN issued the Temporary Specification for gTLD Registration Data (Temp Spec), guidance that established temporary rules that adjusted domain name registrars' and registry operators' WHOIS-related contractual obligations to avoid conflicts with the GDPR. Specifically, these rules:

- Allowed registrars and registry operators to limit public access to many fields of the WHOIS database.
- Required registrars and registry operators to give WHOIS users:
  - "reasonable access" to non-public WHOIS data for legitimate purposes; and
  - the ability to contact a domain registrant or its administrative or technical contact through an anonymized email or web form.
- Authorized brand owners to file UDRP complaints without including the domain registrant's identity.
- Required registrars, after a complaint is filed, to provide the domain registrant's identifying information to the UDRP provider (the neutral arbitrator deciding the claim), who then provides that information to the brand owner.

Following the Temp Spec, the most popular UDRP provider, the World Intellectual Property Organization (WIPO), prepared an Informal Q&A on the relationship between the UDRP and GDPR and how WIPO UDRP panelists will adjust to the challenges raised by the GDPR's effect on WHOIS and UDRP procedure.

HOW IS THIS WORKING?

While the Temp Spec approach is a somewhat effective stopgap measure, its rollout was bumpy. One reason for the frustration is the vagueness of some of its language, which causes significant differences in interpretation and implementation. For example, the Temp Spec states that domain name registrars and registry operators must provide "reasonable access" to registrant contact information when requested by third parties with "legitimate interests," but fails to define those terms. As a result, registrars have offered inconsistent responses, with many taking a conservative view of what level of access qualifies as reasonable, and what purposes are legitimate, under the Temp Spec.

Some domain name registrars have provided access very slowly and rejected a significant portion of requests. In many cases, requests have received no response at all. While these registrars may have legitimate concerns about GDPR compliance, some practitioners have speculated that this approach is intended to create a precedent of minimal access after the Temp Spec is replaced with a long-term solution. So far, registrars appear more responsive to requests for information after a UDRP complaint has been filed. Yet even these responses have involved significant delays.

Because of these challenges, practitioners are turning to other avenues and tools.

HOW CAN A BRAND OWNER INVESTIGATE A POTENTIAL UDRP CLAIM WITHOUT ACCESS TO WHOIS INFORMATION?

Brand owners and their counsel should first search the WHOIS database of the applicable registrar to see if registrant information is still available. If not, there are several second-best methods available. For example:

- **Legacy WHOIS databases.** Many third-party WHOIS database providers opted to retain WHOIS information that was current when the GDPR took effect. However, these databases are no longer accessible without a fee and do not reflect newer domain registrations and domain transfer and other information updated after May 25.
- **Private investigators.** However, using investigators may be cost-prohibitive, especially in light of the large number of domains that often need to be explored in any given case.
- **Tech investigation.** Tech-savvy counsel, brand owners, and investigators may be able to use the limited information remaining in public WHOIS databases to learn the nameservers hosting the domain name at issue. Also, zone files, which map all IP addresses associated with a domain, can be researched through look-up tools widely available online to reveal the website's host and mail servers. These data points may provide useful clues about the domain registrant's identity or location.
- **The domain holder's website.** There may be contact information on the website associated with the offending domain name. For example, the registrant may be operating a business with a Contact Us page or may have posted contact information for offers to buy the domain name. Information about the domain name owner might also be discernible through website metadata or by viewing the website source code file. An email addressed to postmaster@ or admin@ the offending domain may be another way to contact the registrant directly.
- **Registrars.** Brand owners should not give up trying to get contact information and reach the registrant through the registrar, as contemplated by the Temp Spec. The methods available vary a great deal, and in some cases, there may be an email or web form for an anonymous inquiry, as authorized by the Temp Spec. However, regardless of method, there is no way to ensure that the registrant will respond (or that the brand owner communication will be passed on to the registrant in a meaningful way).
- **Due process.** Some registrars and other ICANN stakeholders suggest using subpoenas or warrants to obtain registrant information. These methods are largely unrealistic because they typically require commencing legal proceedings in a court of law, which defeats one of the most appealing features of the UDRP process, providing a quicker and less expensive alternative to litigation. These methods are also ill-suited to cross-border investigations, which are common in UDRP situations.

The bottom line is that it is increasingly difficult for a would-be UDRP complainant to investigate and then substantiate its case.

HOW CAN A BRAND OWNER SUPPORT ITS UDRP CLAIM WITHOUT ACCESS TO WHOIS INFORMATION?

The brand owner initially can file a John Doe complaint if the registrant's identity is unknown. Complainants should be prepared to amend complaints and possibly consolidate claims once registrant information becomes available.

To support its claim, a complainant should make the most of the content of the website associated with the offending domain name. If the website is hosting links relating to the complainant's business or field, this should be sufficient for a prima facie showing of bad faith, which shifts the burden to the registrant to rebut this prong of a UDRP claim. While this is standard operating procedure in many UDRP cases, the complainant will need to rely on this more than before, absent WHOIS information.

Complainants should also consider registrant bad faith demonstrated in emails. Email addresses using the challenged domains may be involved in phishing attempts, malware, fraud, spam, and other abusive activity.

Complainants also may have to rely on circumstantial evidence to make their case, for example, by trying to establish connections between multiple domains. This can be shown or suggested by:

- Common DNS information, such as name servers, website hosts, and mail servers.
- Common registration dates.
- Similar *modus operandi*, such as use of a particular new gTLD or specific typosquatting strategy or the appending of words to a trademark in a domain name in a recognizable pattern or method.

ASIDE FROM THE UDRP, WHAT OTHER OPTIONS DO BRAND OWNERS HAVE?

In the US, the brand owner can bring a federal lawsuit under the Anticybersquatting Consumer Protection Act (ACPA) (15 U.S.C. § 1125(d)). However, ACPA cases are likely to have limited feasibility. Federal court proceedings are far more expensive and time-consuming than UDRP cases. The US court system also is not available in many situations, for example, where the defendant is not present in the US and personal jurisdiction is lacking. Even where a foreign defendant is present in the US for jurisdiction purposes, they may not have a location or contact for service of process, which necessitates service under the Hague Convention, further increasing time and cost. Even then the defendant may not appear, and enforcing relief under the ACPA can be problematic if the court lacks jurisdiction over the registrar. (For more on ACPA claims, see Practice Note, Brand Protection Online: The Anticybersquatting Consumer Protection Act (6-503-4780)).

The ACPA does offer an interesting alternative, which is the option of bringing an *in rem* action naming the domain name, rather than the registrant, as the defendant. Already useful against foreign registrants using US registrars, this option is gaining more attention

in light of the WHOIS blackout. However, an *in rem* action must be brought in the home district of the registrar, which may be inconvenient for the plaintiff. For example, prominent registrar GoDaddy is headquartered in Scottsdale, Arizona, and its only East Coast offices are in Massachusetts and Virginia. GoDaddy is also located in Hiawatha, Iowa, so the Southern District of Iowa in Cedar Rapids may be an option, but certainly not a convenient one for most people.

Other alternatives include suing in the country where the registrant can be found, based on city and country information sometimes still available through WHOIS. This entails hiring local counsel, translating documents, conducting proceedings in the local language, international travel, and other added expenses. Differences in local jurisprudence can also be a significant issue, depending on the jurisdiction and the brand owner's case. While local civil actions should always be considered, the likelihood that they are a viable alternative is small.

In cases where the registrant's actions are particularly egregious, a criminal complaint or referral may be appropriate, for instance, where fraud or malware distribution is part of the registrant's overall scheme.

ARE THE DISPUTE RESOLUTION SERVICE PROVIDERS, SUCH AS WIPO, DOING ANYTHING TO HELP?

The responses from the dispute resolution service providers most commonly used by US trademark owners, specifically WIPO and FORUM, have varied.

For example, WIPO has been very active on this issue and has come out with a series of adjustments, set out in an Informal Q&A on its website, for post-GDPR UDRP filings, including guidance for:

- Submitting a complaint without identifying or contact information for the domain registrant.
- Obtaining registrant information post-complaint.
- Consolidating complaints after obtaining identifying information.

By contrast, FORUM has not provided its own guidance. Its website instead directs users to the ICANN website and to the Temp Spec.

HOW HAVE ICANN AND OTHER STAKEHOLDERS ADDRESSED THESE ISSUES?

ICANN has convened an Expedited Policy Development Process (EPDP) working group to review, revise, and replace the Temp Spec. However, the EPDP is focusing more on the collection and processing of domain registrant data than on access to it. ICANN has also released a draft framework for a Unified Access Model (UAM), which proposes a system of authenticated WHOIS users. ICANN has requested public comments on the UAM on its website, which are currently trickling in.

The GDPR, the Temp Spec, and the EPDP were the center of attention at the October 2018 ICANN meeting in Barcelona, and EPDP work picked up again almost immediately after the meeting closed. Numerous issues remain up for debate in the EPDP, including whether registrars must distinguish between natural persons and legal persons and between EU registrants and non-EU registrants. Brand owners should be concerned about these questions because the outcome affects the availability of registrant information from registries and registrars worldwide, even where the WHOIS information is not protected by the GDPR.

Efforts in and around the EPDP are also ongoing to better define "reasonable access," the current standard for all access to non-public WHOIS information. Hopefully, these efforts will bring an approach to access requests that is reasonable to all parties. The legitimacy, scope, and legal basis of various purposes of collection and processing are also being hotly discussed. The outcome of these discussions will shape later discussions on access within the EPDP.

Specific to the UDRP, the EPDP's efforts to crystallize the purpose, basis, and access for pre-UDRP investigations and fact-finding are still in flux. If pre-UDRP data requests can receive the same treatment as data requests in the context of filed UDRP proceedings, the chances for broad useful access will greatly increase.

The EPDP expects to publish an Interim Report for public comment around November 19, 2018, which will include many of these unresolved issues. Hopefully, brand owners will come out in force and file public comments to guide the EPDP toward results that will benefit brand owners and consumers, rather than protect alleged cybersquatters and other bad actors.

WHAT DOES THE FUTURE HOLD FOR UDRP COMPLAINANTS AND RESPONDENTS?

It will be a long time before any structured and regularized form of access to the once-public WHOIS information emerges. While many stakeholders desire to improve circumstances for brand owners, there are no easy solutions.

It seems likely that brand owners and their counsel will begin to investigate options beyond ICANN, including:

- Exerting more pressure on domain name registrars, resellers, ISPs, hosting companies, and DNS providers to disable access to websites.
- Pressing domain name registrars, resellers, ISPs, hosting companies, and DNS providers to assume responsibility for the use of domain names where WHOIS information is not publicly available. This third-party or secondary liability is highly controversial. However, there may be an increasing willingness to test these boundaries, at least where third-party action or inaction appears designed to shield the domain registrant from liability.
- Improvising and adapting their strategies to make good use of the UDRP, despite GDPR-created obstacles.

In addition to participating in ICANN efforts relating to the EPDP and the Temp Spec, brand owners are likely to push for the development of a WHOIS access model, such as the UAM.

At the same time, domain registrants are likely to shift their behavior. For example, since UDRP cases will contain less information, brand owners may more often find themselves the targets of "reverse domain-name hijacking" claims (claims alleging abuse of the UDRP

process to seize legitimate domain names). Brand owners are cautioned to be aware of this possibility and to amend or withdraw their cases, if necessary, as domain registrant information and other data come to light.

Additionally, the WHOIS blackout will likely result in some weaker UDRP complaints, making it easier for domain registrants to defend against claims. As a result, more domain registrants may opt to respond to claims rather than defaulting, which has traditionally been the most common response. The resulting increased demand for UDRP provider panelists to weigh arguments from both sides may lead to a backlog of cases awaiting decision.