OPINIONS

Navigating the WHOIS Blackout

Lauren Somers
Trade Mark Attorney, HGF Ltd, Manchester

Following the implementation of GDPR in the EU last year, the majority of WHOIS data was redacted. The loss of this previously freely accessible data has had ramifications for IP owners seeking to enforce their rights against domain name squatters and online fraud. The domain name registrars, national EU domain name registries and the World Intellectual Property Office ("WIPO") have each responded to the "WHOIS blackout", providing mechanisms to obtain registrant data on request, although procedures and willingness to disclose registrant data vary. The ability of IP owners to satisfy the Uniform Dispute Resolution Policy ("UDRP") has also been affected in the absence of the identity of the respondent to any complaint.

On 25 May 2018 the majority of previously freely available WHOIS data went dark. The implementation of GDPR meant that domain name registrars, in fear of the much publicised GDPR sanctions, in most cases redacted all registrant information from the online public databases.

The data had previously proven a useful tool for IP owners. When faced with a concerned website, and domain name registration and contact information was not provided on the site itself, IP owners or their representatives could look to WHOIS. Now, unless the registrant has specifically consented to the publication of its data, the WHOIS data result for any domain provides little insight. Generally, all that remains is the name of the responsible registrar, the creation, update and expiry date of the domain name registration, plus an "abuse" contact email.

Prior to the "blackout", natural person registrants could shield their information behind a privacy protection screen. So, some have asked, how does this situation post-GDPR differ from that beforehand, in which a growing number of registrants opted to privacy protect their data? For one, privacy shields were only available to natural persons, whereas *the redaction post-GDPR has been applied equally to domains owned by individuals and legal entities. Secondly, given the fear of sanctions, domain name registrars have become even more reluctant to release registrant data at the request of IP owners.

Differing registrar practice

While ICANN has stipulated that registrars must provide IP owners (and other interested parties) with access to the registrant either via an anonymised email or an online contact form, these access routes have to date proven unreliable. Further, it is now necessary to convince registrars that a "legitimate interest" is present to warrant disclosure of any registrant's data: legitimate interest being one of the permissible reasons to process personal data under GDPR. ICANN's limited guidance has led to varying approaches to data release and how requests are handled by registrars, creating added uncertainty for IP owners and their representatives.

For gTLDs, the registrars responsible for providing access to data, such as Gandi, Web.com, Enom and GoDaddy, each handle requests for registrant data in different ways. For example, Gandi provides an anonymised email for contacting the registrant within its WHOIS data. However, undeliverable notifications are frequently received from such email addresses. Web.com and others provide users with an online form, but technical difficulties are common.

So, IP owners or their representatives are forced to then persistently contact the registrar, typically via their "abuse" email address, requesting that their complaint is forwarded to the registrant or that the registrant's data is provided.

Turning to ccTLDs, there is a little more procedural clarity. Taking first the registry for .uk domains, Nominet: this operates its own WHOIS database. Nominet has provided a Data Release Request form via which interested parties can submit a request for registrant data. The form requires the requesting party to outline their details, the domain concerned, the information being sought and details of their legitimate interest in having access to the desired data.

A similar form has been produced by the French, German, Dutch and Belgian national domain name registries. However, not all ccTLD registries within the EU have followed suit. For example, the Austrian registry will accept less formal requests for data via email, while the Bulgarian registry will only provide a third party with access to registrant data within court proceedings. So, practice is again varied.

WIPO and the UDRP

The World Intellectual Property Office ("WIPO") has acknowledged the difficult position in which IP owners have been left following GDPR within its Uniform

Dispute Resolution Policy ("UDRP") guidance. UDRP complaints filed without details of the registrant will not be treated as deficient. Rather, WIPO will, on receipt of the complaint, provide the details of the registrant to the complainant who is given a short period of time to amend their complaint. This amendment may be in terms of simply adding in registrant details to the UDRP complaint form, but can also include wider amendments to the complaint in light of the registrant data being provided.

Alternatively, should the complainant no longer wish to pursue the complaint on learning the identity of the registrant, it may withdraw the complaint and will receive a partial refund of the WIPO fee—US$1,000 of the total $1,500 fee.

Still, the procedure does not favour IP owners. Either they must file the complaint "blind" and then, once provided with the registrant's identity, spend the time and incur the cost of amending the complaint to fully particularise their case. Or, if the domain transpires to be owned by, for example, an authorised licensee, they must withdraw the complaint, having already incurred a partial fee, plus any legal fees associated with submitting the initial complaint.

Turning back to the amendments to the complaint that may be required in light of the belatedly provided registrant information, the absence of registrant information when preparing a UDRP complaint can be extremely limiting to IP owners seeking to make their case under the policy. The UDRP requires that (1) the complainant should have rights in a mark identical or confusingly similar to the domain name; (2) the registrant has no legitimate interest in the domain name; and (3) the domain name was registered and is being used in bad faith. Both the second and third of these elements are affected by the WHOIS blackout.

In terms of legitimate interest, in the absence of the registrant's identity no such legitimate interest may be inferred. While this arguably makes the complainant's case for no legitimate interest more straightforward, it means that the complainant cannot anticipate any reasoning that may be put forward by the registrant and seek to shut down these claims at the outset.

Typical arguments that the registrant lacks a legitimate interest in the domain name include: the registrant is not an authorised licensee or reseller of the complainant; the registrant would have been aware of the complaint and its rights owing to the registrant's location and the reputation of the complainant's mark; and that the domain name is not being used in connection with a bona fide offering of goods and services.

However, if the registrant's identity is unknown, it is not possible for the complainant to be certain of any relationship with the registrant, point to the location of the registrant and claim with conviction that it would have been aware of the complainant's rights and reputation when registering the domain; nor can the complainant see whether the domain has been registered by a legitimate company which may have a genuine intention to use the domain, or whether it has been registered by, for example, an individual whose name is connected with phishing emails.

In terms of the third element of the UDRP, bad faith registration and use, again the complainant is less able to make its case in the absence of the registrant's data. Common arguments for bad faith include: the domain was registered for the purpose of selling the domain to the trade mark owner at an excessive cost; the domain was registered to prevent the trade mark holder reflecting its name in a corresponding domain name, provided there is a pattern of such conduct; the domain was registered to disrupt the complainant's business; or the domain is being used in a commercial capacity to confuse consumers.

Considering the first line of argument, given that it is now harder to contact registrants before filing a complaint, IP owners potentially lose the opportunity to obtain useful evidence indicating the intentions of a registrant. Pre-May 2018, the response of many registrants to a request for transfer prior to a UDRP complaint was to seek an excessive payment. This could then be used as evidence of bad faith in any complaint. However, obtaining such evidence is now much more difficult.

In terms of showing that the registrant is engaged in a pattern of abusive registrations, this was previously demonstratable by providing reverse WHOIS search results pointing to other domains registered by the registrant corresponding with the IP of the complainant or other third parties. While reverse WHOIS searches are still possible, the reliability of this data is questionable post-GDPR, and only once the complaint has been filed and the registrant details provided would such a pattern be able to be investigated and added to the complaint.

Finally, again, as the geographical location and identity of the registrant are not known, the complainant can less convincingly argue that the registrant would have known about its IP when registering the domain, and therefore the only intention behind the domain name registration and its use is to disrupt its business and confuse its consumers.

The impact of this shift in complainant position post-GDPR does not yet appear to have had an impact on WIPOUDRP decision statistics. In 2017 and 2018, approximately 16–17 per cent of all complaints were terminated (withdrawn) before a decision was issued. In 2019 to date, approximately 23 per cent of decisions have been terminated before decision. It may be that this figure is brought down as decisions continue to be issued throughout the year. However, regardless of the statistics, satisfying the criteria of the UDRP has become more difficult for IP owners following the implementation of GDPR in the current WHOIS blackout.

Accreditation model

ICANN, in recognition that the current position for IP owners is far from ideal, is considering a standardised system for access to WHOIS data for third parties with

a legitimate interest. Such a system would be available to law enforcement, consumer protection agencies, IP owners and their representatives and cybersecurity organisations under an accreditation framework.

The Generic Names Supporting Organisation (GNSO) council within ICANN has been tasked with debating the model, and it recently concluded "phase one" of its discussions. A report on this phase made specific mention of IP right holders having a legitimate interest in access to WHOIS data to ensure their IP is enforced and not abused. However, it also warned that any legitimate interest must outweigh the interests of the individual concerned, and that IP owners would need to be prepared to fully substantiate their rights and legitimate interest.

So, while the GNSO council and ICANN are committed to "finding a timely and workable solution" to access to registrant data for IP owners and others with a legitimate interest, both remain torn between this need and the need to comply with GDPR. "Phase two" of the council discussions is set to begin shortly. In the meantime, the WHOIS blackout continues.