RESOLVED, That the American Bar Association supports a right that would legally compel the disclosure of internet domain name registrant contact information by any U.S. entity that administers and maintains such contact information, upon receipt of a notice alleging a legitimate interest based on the registrant’s violations of applicable laws relating to intellectual property protections.
REPORT

This Resolution supports a public access system ensuring the right of intellectual property owners to access contact information for registrants of domain names in the WHOIS database\(^1\) administered by the Internet Corporation for Assigned Names and Numbers (ICANN), for the limited purpose of enforcing rights against violations of applicable law relating to intellectual property protections. Under such an access system, relevant entities maintaining domain registrant contact information would be legally compelled to disclose pertinent contact information once an intellectual property owner establishes a legitimate interest in a legal right potentially violated by the domain registrant at issue.

For decades, a straightforward process was available to intellectual property owners to obtain the contact information for an entity that registered a domain name confusingly similar to a registered trademark, or whose website offered counterfeit, pirated or otherwise infringing content, products or services. After the May 25, 2018 effective date of the European Union’s General Data Protection Regulation (“GDPR”), it has become difficult, if not impossible, to locate such information even from registrars and registry services located outside of the European Economic Area.\(^2\)

The GDPR set a precedent in data privacy law, and a number of states in the U.S. have since introduced new legislation inspired by the GDPR.\(^3\) However, the GDPR and other similar legislation overlook the need for intellectual property owners, among others, to identify and contact entities engaging in infringing activities online that violate applicable intellectual property laws.

Congress appears to be considering comprehensive federal legislation regarding data privacy and the processing of personal information.\(^4\) Discussions are still in the early stages, yet a complicated patchwork of state laws is emerging in the area of data privacy. The new California Consumer Privacy Act (“CCPA”), effective 2020, figures to be a prominent component of this patchwork. Similar to the GDPR, the current version of the CCPA overlooks the need for intellectual property owners to enforce their rights against online infringers. The CCPA does allow the state’s attorney general to adopt regulations establishing “any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.”\(^5\) However, the initial set of proposed regulations for the CCPA were released in October 2019, and the regulations do not address intellectual property in any way.\(^6\)

\(^1\) See generally https://whois.icann.org/en/about-whois.

\(^2\) The European Economic Area includes the twenty-seven European Union Member States, Iceland, Lichtenstein and Norway.

\(^3\) For example, Illinois H.B. 3358, Massachusetts Bill S.120, Minnesota H.F. 2917, New Jersey A-4902, Pennsylvania H.B. 1049, and Hawaii S.B. 418.


\(^5\) Cal. Civil Code § 1798.185(a)(3).

Any forthcoming data privacy legislation should consider the right of intellectual property owners to have access to registrant contact information upon the showing of a legitimate interest in enforcing intellectual property rights against a registrant engaged in violations of applicable law relating to intellectual property protections, including, but not limited to, cybersquatting, trademark or copyright infringement, dilution, piracy, counterfeiting, or unfair competition. For example, under trademark law, such a legitimate interest could be established by showing ownership of a name or mark that is confusingly similar to the domain name at issue with the relevant registrar or registry service. Under copyright law, an individual or entity could establish a similar legitimate interest by showing ownership of a copyright protected work that is copied in website content available through the domain at issue, along with any other claims or evidence necessary to make the disclosure of registrant information permissible under applicable law.

**Impact of Data Privacy Regulations on the Enforcement of Intellectual Property Rights Online**

The WHOIS database is a protocol administered by ICANN and used to make a variety of information about a given domain name available to the public. For example, most WHOIS queries disclose the date a domain name was registered, the date it was last updated with the registrar, and the date the domain’s registration will expire if not renewed.

Until the GDPR’s effective date in May 2018, contact information for most domain registrants was also generally available to the public unless the registrant paid for a privacy or proxy service. Privacy services have allowed persons or entities to be listed as the registered domain name holder, but alternative and reliable contact information such as an anonymized mail-forwarding email address is substituted for the true registrant’s personal contact information. Proxy services similarly have provided alternate contact information for the registrant, but proxy service providers also are listed as the registered domain name holder. Both privacy and proxy services are still available to domain registrants after the GDPR.

**Settlement Discussions Only Occur When the Domain Registrant Can Be Contacted**

When a privacy or proxy service is used, the registrant at least can be notified of the trademark or copyright owner’s concerns about any alleged violations of applicable law relating to intellectual property protections. Communications with such registrants can often lead to a cost-effective settlement of the matter.

Such settlement of a trademark dispute might include a transfer or cancellation of the domain registration, without any need for costly litigation or the filing of a complaint under ICANN’s Uniform Domain Name Dispute Resolution Policy (“UDRP”), which requires a fee of at least $1,500 USD. Further, a successful UDRP proceeding is determined based on a record set forth solely by the complaint and any formal response...
by the registrant. Therefore, a UDRP complaint should include evidence establishing that, among other things, the registrant had no rights or legitimate interest in the domain name, and that the domain name was registered and used in bad faith. The content of communications with domain registrants, among other evidence that could only be accessible after learning the registrant’s email address, can be important to proving such factors in a UDRP proceeding. For example, communications can reveal whether the registrant has plans to use the domain name in connection with a bona fide offering of goods or services in a way that could show registrant has a legitimate interest in the domain. Similarly, communications revealing the registrant’s location in a jurisdiction where the complainant is not active may indicate the domain was not registered in bad faith because the registrant may not have been aware of the complainant’s mark when the domain was registered.

With respect to online copyright violations, communications with a domain registrant are crucial for copyright owners to protect their exclusive rights and exercise the notice and takedown procedure available under the Digital Millennium Copyright Act (“DMCA”) in a cost-effective manner. When a copyright owner simply wants infringing content removed from a website, oftentimes a letter or email correspondence to the domain registrant is enough to cause the removal. If the registrant posted the infringing content, the registrant may not know such content violated someone’s copyright and be more than willing to remove it to avoid ongoing liability. If a user of the registrant’s website posted the infringing content, then the DMCA provides for immunity from copyright infringement for website operators removing infringing content upon receipt of a formal notice from the copyright owner. Accordingly, registrants operating websites with infringing user-generated content are incentivized to comply with copyright-based takedown requests. However, these simple options are not available if the registrant cannot be contacted by a copyright owner concerned about infringement. If a copyright owner is unable to contact a registrant potentially involved with infringing content, litigation becomes the only recourse even if a simple takedown is all the copyright owner seeks. Such litigation leads to additional legal measures, such as a subpoena or other court order, to compel disclosure of a domain registrant’s contact information, often accompanied by a significant financial burden in comparison to a simple exchange of correspondence between cooperative parties.

Before the GDPR, even if the registrant paid for a privacy or proxy service, such services would list an anonymized email address that could be used reliably to direct communications to the registrant. While there is no guarantee the registrant would respond, these anonymized email addresses still provide a means to communicate concerns over an alleged dispute before initiating costly legal action that may not be necessary.

---

8 Uniform Domain Name Dispute Resolution Policy, Paragraphs 4(a-c).
9 See 17 U.S.C. § 512(c).
Unavailability of Domain Registrant Information After the GDPR

Due to large potential penalties under the GDPR for the unauthorized disclosure of personal data, numerous registrars now automatically hide or redact registrant names and contact information entirely. ICANN also is struggling to implement a GDPR-compliant replacement access model for the WHOIS database.

Without any clear obligation to disclose registrant contact information, obtaining access to such information is now at the discretion of each of the thousands of ICANN-accredited registrars and registry services. Some registrars, such as eNom, an affiliate of the Canadian company Tucows, provide a tiered access system where enforcement entities can provide “name, legitimate interest for access, and domain name(s) for which access is desired” as part of an application process to request access to a “tiered registration directory.” Other registrars, such as the French company OVH, use anonymized email addresses to direct communications to registrants without disclosing their identity, similar to how many paid privacy services work.

Other registrars are less forthcoming about an alternate means of accessing registrant information and may bury trademark and copyright complaint procedures in website policies and agreements. Certain registrars expressly prioritize the privacy concerns of customers over the interests of intellectual property owners and other enforcement entities. For example, Namecheap has a published policy stating it will forward “a valid and formal notice of a trademark complaint,” provided the notice meets five specific requirements, to the allegedly infringing customer. However, Namecheap is also clear that after the GDPR, it “will not disclose any personal information about our customers unless required by law or pursuant to a court order or subpoena.”

---

10 Council Regulation 2016/679, General Data Protection Regulation, art. 83, 2016 O.J. (EU) (“Non-compliance … shall … be subject to administrative fines up to 20 000 000 EUR, or … up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher”).
11 Examples include Alibaba Cloud, DENIC, EURid, Namegear, Namecheap, Network Solutions and OVH.
13 Id. (“Many registrars are not even complying with the continuing mandatory minimum information requirements of ICANN … many have redacted every single WHOIS data field relating to registrant contact information as the default”).
14 https://www.enom.com/help/abusepolicy.aspx#fragment-4
15 See, e.g., https://www.ovh.co.uk/domains/owo_service.xml.
17 https://www.namecheap.com/about/privacy-commitment/.
Emerging Patchwork of State Consumer Privacy Laws and Registrar Access Models for WHOIS Information

In the wake of the GDPR, at least nineteen states in the U.S. have introduced legislation or enacted broad data privacy laws that could have a similar impact on the availability of contact information through WHOIS in the U.S., to the extent it was not already affected by the GDPR. Consent requirements in these new state laws generally rest on opt-outs rather than the affirmative opt-in consent required under the GDPR, but in theory would still provide violators of intellectual property rights with a cost-free means of avoiding detection for acts violating federal or state law should they choose to exercise the opt-out.

There is a reasonable compromise between the interests of intellectual property owners and privacy rights with respect to domain registration and the information available through the WHOIS protocol. The many competing ways in which registrars handle this issue have caused WHOIS, administered by ICANN since 1998, to become far less useful for the enforcement of intellectual property rights.

The table below illustrates representative samples of the numerous ways registrars in jurisdictions around the world use different models for granting access to domain registrant contact information since the GDPR became effective. ICANN still contractually requires accredited registrars to provide an email contact for reports of abuse, including illegal activity such as violations of applicable intellectual property laws, but it does not compel registrars to do anything more than a cursory investigation based on such reports. Some registrars seem to have no intention of cooperating with access requests based on intellectual property violations, and advise intellectual property owners to initiate a UDRP proceeding or seek a subpoena or court order if there is interest in obtaining an infringing registrant’s contact information. The tiered access model offered by eNom and Tucows appears to be the most practical compromise between privacy and intellectual property interests, but very few registrars appear to have adopted such an access model.

<table>
<thead>
<tr>
<th>Registrar</th>
<th>Location</th>
<th>Access Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alibaba Cloud</td>
<td>China</td>
<td>Email registrar abuse contact</td>
</tr>
<tr>
<td>DENIC</td>
<td>Germany</td>
<td>Submit paper application form</td>
</tr>
<tr>
<td>eNom/Tucows</td>
<td>Canada</td>
<td>Tiered access based on legitimate interest</td>
</tr>
</tbody>
</table>

19 See Justin P. Webb and Sarah A. Sargent, An American Perspective on the GDPR One Year In, 11 LANDSLIDE 5, A.B.A. Sec. Intell. Prop. L. (May/June 2019), https://www.americanbar.org/groups/intelectual_property_law/publications/landslide/2018-19/may-june/an-american-perspective-the-gdpr-one-year-in/ (“Similar to the GDPR, U.S. companies will be forced to choose between providing the more robust privacy protections in the CCPA only to California residents or spending more money and time to provide those rights to all individuals”).
<table>
<thead>
<tr>
<th>EURid</th>
<th>Belgium</th>
<th>Submit email request</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy</td>
<td>U.S.</td>
<td>Available depending on location of registrant</td>
</tr>
<tr>
<td>Namecheap</td>
<td>U.S.</td>
<td>Subpoena/court order/UDRP</td>
</tr>
<tr>
<td>Namegear</td>
<td>Japan</td>
<td>Submit request to “Privacy Information Support Contact”</td>
</tr>
<tr>
<td>Network Solutions</td>
<td>U.S.</td>
<td>Submit “Report Abuse” web form</td>
</tr>
<tr>
<td>OVH</td>
<td>France</td>
<td>Anonymized auto-forwarding email address</td>
</tr>
<tr>
<td>Public Domain Registry</td>
<td>India</td>
<td>Subpoena/court order/UDRP</td>
</tr>
</tbody>
</table>

**Right of Access to WHOIS Information for Dispute Resolution**

Any new law on data privacy should grant an express right to intellectual property owners for access to domain registrant information in the WHOIS database for the limited purposes of enforcement against persons or entities engaged in violations of applicable law relating to intellectual property protections.

The Resolution does not suggest any specific information access model given that any form of access likely will need to be compliant in jurisdictions outside the U.S., and particularly in Europe under the GDPR. Regardless of the form of access model, access to registrant information in the WHOIS database should be restored for the effective enforcement of intellectual property rights online. The restoration of WHOIS access upon a showing of a legitimate intellectual property dispute would provide opportunities for amicable resolution that are not currently available. Parties could negotiate a transfer of the domain name at issue, allow the domain name to expire without renewal, alter or remove problematic content, or clarify a good faith basis for registering and using the domain name. Under current circumstances, there is little opportunity to initiate an amicable dispute resolution.

The current need to litigate, obtain a court order, or initiate a UDRP proceeding just to identify an infringing entity is overly expensive and burdensome to parties—justifiably seeking to enforce rights granted to them under law—while making it easier for infringers to hide from the parties they damage.

An access model allowing enforcers of intellectual property rights to view contact information for an allegedly infringing registrant for the limited purposes of intellectual property enforcement would respect individual privacy rights while also ensuring that intellectual property owners can reach entities that are violating applicable laws, such as the Lanham Act and the Copyright Act. Under U.S. data privacy laws, of which the CCPA is the most restrictive, such an access model would identify the enforcement of intellectual property rights as among the specific reasons an opt-out request can be refused. The
proposed Resolution does not intend to comment on European law, but in theory, such an access model would also help establish that a violation of applicable intellectual property rights is a legitimate interest which is not overridden by the interests or fundamental rights or freedoms of the registrant under the GDPR.²¹

Conclusion

The American Bar Association supports a public access system that would legally compel relevant entities to disclose contact information for persons or entities plausibly alleged to have engaged in violations of applicable law relating to intellectual property protections. Under such an access system, entities including, but not limited to, registrars and registry services should be legally required to disclose such contact information once the requesting party has established a legitimate interest in a legal right potentially violated by the domain registrant at issue.

Respectfully submitted,

George W. Jordan III
Chair, Section of Intellectual Property Law
February 2020

²¹ Council Regulation 2016/679, General Data Protection Regulation, art. 6, 2016 O.J. (EU) (“Processing shall be lawful only if and to the extent that … processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data…”).
GENERAL INFORMATION FORM

Submitting Entity: Section of Intellectual Property Law

Submitted by: George W. Jordan III, Section Chair

1. **Summary of the Resolution.**

   This Resolution supports a right that would legally compel the disclosure of domain registrant contact information by any U.S. entity that administers and maintains such contact information, upon receipt of a notice alleging a legitimate interest based on the registrant’s violations of applicable laws relating to intellectual property protections.

2. **Approval by Submitting Entity.**

   The Section of Intellectual Property Law Council approved the resolution on November 5, 2019.

3. **Has this or a similar resolution been submitted to the House or Board previously?**

   No.

4. **What existing Association policies are relevant to this Resolution and how would they be affected by its adoption?**

   At the 2002 Midyear Meeting, the House of Delegates adopted Resolution 111a, which favors in principle a requirement by the Internet Corporation of Assigned Names and Numbers ("ICANN") that all accredited domain name registrars provide continued, free access to WHOIS information, consisting of basic contact information obtained from domain name registrants. The resolution is consistent with that policy.

5. **If this is a late report, what urgency exists which requires action at this meeting of the House?**

   Not applicable.

6. **Status of Legislation.**

   No federal legislation yet. The California Consumer Privacy Act (CCPA) becomes effective in 2020, and is subject to amendment.

7. **Brief explanation regarding plans for implementation of the policy, if adopted by the House of Delegates.**

   This Resolution will provide Association support for any forthcoming federal or state
legislation or regulations regarding data privacy, including regulations or amendments to the California Consumer Privacy Act.


Adoption of the recommendations will not result in additional direct or indirect costs to the Association.


There are no known conflicts of interest regarding this recommendation.

10. Referrals.

The Resolution and Report will be distributed to each of the other Sections, Divisions, Forums, and Standing Committees of the Association in the version accepted and numbered for the agenda by the Rules and Calendar Committee.

11. Name and Contact Information

(Prior to the Meeting. Please include name, telephone number and e-mail address). Be aware that this information will be available to anyone who views the House of Delegates agenda online.)

George W. Jordan III
Section Chair, Section of Intellectual Property Law
Norton Rose Fulbright US LLP
Houston, TX
Ph: 713-651-5423
George.jordan@nortonrosefulbright.com

Lisa A. Dunner
Section of Intellectual Property Law Delegate to the House of Delegates
Dunner Law PLLC
Washington, DC
Ph: 202-298-6002
ldunner@dunnerlaw.com

12. Name and Contact Information.

(Who will present the Resolution with Report to the House?) Please include best contact information to use when on-site at the meeting. Be aware that this information will be available to anyone who views the House of Delegates agenda online.

Lisa A. Dunner
Section of Intellectual Property Law Delegate to the House of Delegates
Dunner Law PLLC
Washington, DC
Ph: 202-298-6002
ldunner@dunnerlaw.com
EXECUTIVE SUMMARY

1. **Summary of the Resolution.**

   The Resolution supports a right that would legally compel the disclosure of domain registrant contact information by any U.S. entity administering and maintaining such contact information, upon receipt of a notice alleging a legitimate interest based on the registrant’s violations of applicable laws relating to intellectual property protections.

2. **Summary of the issue that the resolution addresses.**

   The Resolution proposes that intellectual property owners challenging violations of applicable law relating to intellectual property protections should have a right to access the contact information of a domain registrant based upon plausible allegations of an intellectual property violation by such registrant. In this way, the parties would have an opportunity to address the dispute directly without costly litigation or a costly proceeding under the Uniform Domain Name Dispute Resolution Policy.

3. **Please explain how the proposed policy position will address the issue.**

   The Resolution would allow the ABA to provide comments to support the consideration of intellectual property rights in any federal or state legislation or regulations regarding data privacy, including regulations or amendments to the California Consumer Privacy Act.

4. **Summary of any minority views or opposition internal and/or external to the ABA which have been identified.**

   The Section of Intellectual Property Law is unaware of any ABA or non-ABA minority views or opposition.