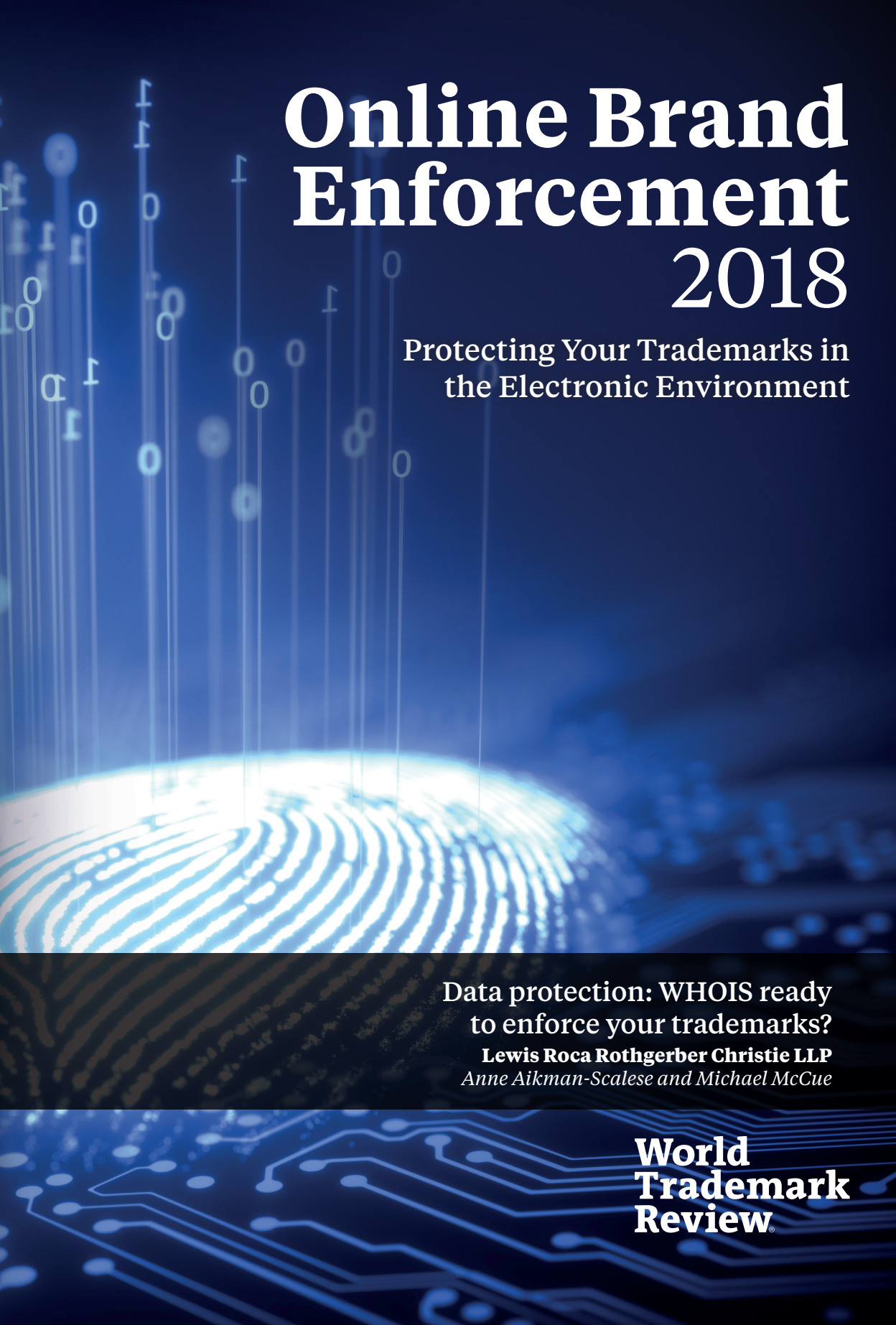

Online Brand Enforcement 2018

Protecting Your Trademarks in the Electronic Environment

Data protection: WHOIS ready to enforce your trademarks?

Lewis Roca Rothgerber Christie LLP
Anne Aikman-Scalese and Michael McCue

World Trademark Review®

Fortune 500 companies turn to us!

Lewis Roca Rothgerber Christie is trusted to protect and enforce the intellectual property of some of the world's most recognizable companies.

Nationally ranked for Trademark Law in the 2017 U.S. News – Best Lawyers® Best Law Firms rankings.

Anne Aikman-Scalese
aaikman@lrrc.com
520 629 4428 direct

Michael McCue
mmccue@lrrc.com
702 949 8224 direct

Lewis Roca
ROTHGERBER CHRISTIE

Lewis Roca Rothgerber Christie LLP lrrc.com

Albuquerque Colorado Springs Denver Irvine Las Vegas
Los Angeles Phoenix Reno Silicon Valley Tucson

Data protection: WHOIS ready to enforce your trademarks?

Authors
Anne Aikman-Scalese and **Michael McCue**

Both global and US-based businesses have been advised by their EU counsel that as of May 25 2018, the EU General Data Protection Regulation (679/2016) will apply to all online offers of goods or services to EU-based natural persons. The law will make the collection of data and tracking of online activity illegal, except where express consent is obtained and where such consent is not "tied" to the receipt of goods or services (ie, a 'check the box' form of consent is not expected to be usable).

While offers to corporate persons are exempt from this privacy regulation, businesses can expect would-be counterfeiters and trademark infringers to take advantage of the new regulation in order to avoid detection in the purchase and sale of counterfeit goods online. How will the established WHOIS system and domain name dispute resolution procedures such as the Uniform Domain Name Dispute Resolution Policy (UDRP) and the new Uniform Rapid Suspension (URS) mechanism deal with these changes?

Privacy advocates hail the new General Data Protection Regulation as a big step forward in the protection of personal data against misuse and abuse by commercial interests. The regulation confirms, they assert, that each natural person interacting on the worldwide web has "the right to be forgotten". But how does our increasingly global internet-based society deal with bad actors, including criminals, in the face of these new privacy protections?

Present WHOIS system

Under the present Domain Name System (DNS), registries (ie, operators of top-level domains such as '.com', '.net', and '.biz') and registrars (ie, sellers of domain name registrations) are obliged by their contracts with the Internet Corporation for Assigned Names and Numbers (ICANN) to maintain WHOIS information on every person or entity registering a domain name. This information includes the name and contact information of the owner, as well as the technical and administrative contacts. The logic behind WHOIS is similar to the reasoning behind statutes that require business entities to designate an agent for service of process – that is, consumers and others should be able to know how to find the entities with which they are doing business.

Because of the WHOIS system, trademark owners with complaints against infringing activity occurring at a particular website have been able to contact the responsible party directly and file a UDRP or URS action, which can ultimately result in disclosure of the registrant and the transfer of an infringing domain, even if the registration itself is privacy protected. While the maintenance of accurate WHOIS information was a requirement of ICANN's Affirmation of Commitments to the US government, that requirement was dropped when US control of the Internet Assigned Numbers Authority (IANA) contract (governing the addition of new names to the root server of the worldwide web) was turned over to

an independent entity in 2016. The 'IANA transition' was made in accordance with new accountability mechanisms established by the ICANN community via the multi-stakeholder, bottom-up policymaking process.

Evolution to a new system: registration directory services

Although relied on by trademark owners both large and small, the WHOIS system has long been considered by registries and registrars to be anachronistic. Even proponents of the system have acknowledged that WHOIS information is easily forged and that as much as 40% of WHOIS data may be fraudulent or inaccurate, despite the fact that certain verification procedures by registrars are required. Years ago, ICANN established an expert working group to conduct a mandated review of the WHOIS system. The group studied possible remedies to protect privacy interests and preserve freedom of speech on the Internet, balancing the need for consumer protection and the public interest in promoting trust, confidence and competition. Their recommendations pointed towards a 'need to know' system, designed to replace the general public availability of WHOIS information. These recommendations were then fed into the ICANN policymaking process for further discussion and refinement.

ICANN's registration directory services (RDS) policy development process working group set about the task of developing consensus policy for the collection and management of domain name registration information going forward. Enter the new General Data Protection Regulation, which appears to trump the bulk of RDS policymaking efforts thus far. Some registrars have even claimed that once the regulation goes into effect in May 2018, it will be illegal for them to collect registrant information when registering domain names, and thus illegal to perform a specific obligation set forth in their contracts with ICANN.

Effect on WHOIS: legal opinion

The RDS working group commissioned a legal opinion on the effect of the General Data Protection Regulation on its work. ICANN corporate management also sought outside legal counsel as to the effect of the regulation on its operations and contracts with registries and registrars. These opinions are consistent in advising that ICANN, as well as the registries and registrars, are at least 'joint data controllers' or 'data processors' under the new regulation. Thus, these entities are currently working through various models which will permit them to comply with the regulation by May 2018. Some have opined that these efforts have come too late to avoid a crisis in the security and stability of the Internet. Others maintain that interim solutions are available, as long as all the players cooperate now to work towards a resolution that satisfies the competing interests.

In the interim, ICANN's compliance department has announced the following suspension of enforcement of the contractual obligation:

> *During this period of uncertainty… ICANN Contractual Compliance will defer taking action against any registry or registrar for noncompliance with contractual obligations related to the handling of registration data.*

Both the ICANN business constituency and the ICANN IP constituency wrote letters to ICANN management in December 2017, objecting to the broad scope of the compliance statement and the modification of WHOIS policy without involving the ICANN community. Both letters underlined the fact that ICANN already has a policy regarding the procedure for handling WHOIS conflicts with privacy law.

Government advisory committee advice

There is general agreement that the present WHOIS system does not comply with the privacy law of certain EU member states and certainly will not comply regarding natural persons when the General Data Protection Regulation comes into effect. Indeed, most registries and registrars maintain that it will be illegal for them to collect or disclose registrant data for domain name registrations as of May 25 2018. However, the ICANN government advisory committee (GAC) formally advised the ICANN board at the Autumn 2017 meeting in Abu Dhabi that the maintenance of an information system which enables the enforcement of IP rights and consumer protection mechanisms is critical

> **There is general agreement that the present WHOIS system does not comply with the privacy law of certain EU member states and certainly will not comply regarding natural persons when the General Data Protection Regulation comes into effect**

to the stable and secure operation of the DNS. The GAC advised the board to take immediate and transparent steps with the European Commission in order to come into compliance with the regulation while meeting the public policy goals of consumer protection and IP enforcement. Under ICANN's amended bylaws, GAC consensus advice may be overturned only by a 60% vote of the ICANN board of directors; such an outcome is viewed as unlikely, given the nature of the advice.

Article 40 code of conduct: a possible way forward

As a possible solution, various trade associations are working with the European Commission to develop data models and codes of conduct pursuant to Article 40 of the General Data Protection Regulation. ICANN, as a California non-profit corporation, has been criticised for failing to develop such a code of conduct when the approach was first suggested to management, many months ago. However, some have pointed out that it was previously unclear whether ICANN itself would be considered a 'data controller' or a 'joint data controller' under the regulation.

ICANN received further legal advice regarding the WHOIS system and the new General Data Protection Regulation in December 2017 in the form of two memoranda affirming the notion that the enforcement of IP rights may be a "legitimate interest" for collecting data under the General Data Protection Regulation, but that the EU Article 29 Data Protection Working Party appeared to express the opinion that fundamental privacy interests may outweigh this legitimate interest. Correspondence from the Article 29 Working Party to ICANN dated December 11 2017 can be viewed at: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48839.

Accordingly, ICANN's outside counsel recommended the collection of WHOIS data for administrative, technical and law enforcement purposes, but recommended further dialogue with the Article 29 Working Party and the individual country data protection authorities as to possible collection and disclosure of data for the purposes of the private enforcement of IP rights. At the time of writing, the three models under consideration by ICANN for interim measures as of May 2018 were available at: www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf.

It is clear that if no resolution to the issues is found in time for the effective date, the entire WHOIS system – as well as rights-enforcement mechanisms such as the UDRP and URS – could enter a dark period. In that event, what can US-based rights holders do to enforce against infringers and counterfeiters when these remedies are no longer available in their present form?

Enforcement mechanisms against unknown registrants

The potential loss of the ability to identify domain name registrants is not new. Since registrars began offering privacy services, trademark owners have had difficulty identifying the owners of domain names. However, there was at least a mechanism by which trademark owners could unmask the identity of the registrants. If registrars were to be prohibited from requiring registrants to provide their names and contact information, enforcement would become exceptionally

Anne Aikman-Scalese
Of counsel
aaikman@lrrc.com

Anne Aikman-Scalese is of counsel with the firm's IP practice, assisting clients with worldwide trademark registration, copyright protection, IP due diligence and licensing transactions. She handles global trademark portfolio management, enforcement and dispute resolution for the missile systems division of Raytheon Company, the Pascua Yaqui Indian Tribe and Casino del Sol Resort. Ms Aikman-Scalese also handles copyright matters for artists, authors and Native American communities. She currently serves on the International Trademark Association Harmonisation of Trademark Law and Practice Committee and has been a member of the Internet Corporation for Assigned Names and Numbers' IP Constituency since 2010. She has been a panellist for the American IP Law Association, the Publishing Law Institute and the World Intellectual Property Organisation.

Michael McCue
Partner
mmccue@lrrc.com

Michael McCue is a partner in the firm's IP practice. He concentrates his litigation practice on trademarks, copyright, trade secrets, patents and rights of publicity, and has litigated hundreds of cases in federal courts throughout the United States and before the Trademark Trial and Appeal Board of the US Patent and Trademark Office. Mr McCue oversees a domestic and international trademark portfolio of more than 5,000 trademarks and has litigated cases for MGM Resorts, Nike, Visa, NBCUniversal, Restoration Hardware and Electronic Arts. In addition to litigation, he provides trademark and copyright prosecution, counselling, clearance, transactional and enforcement services.

difficult. However, there are potential options for enforcement even under such circumstances.

UDRP and URS

The UDRP has been in place since 1999 to enable trademark owners to recover domain names that are identical or confusingly similar to the brand owners' marks and are used in bad faith. In 2013 ICANN added the URS system, which is a faster and more cost-effective process than a UDRP proceeding, but results in the freezing (rather than transfer) of the domain name at issue during the remainder of the registration period.

Both the UDRP and the URS require that the domain name registrant be given notice of the complaint and have the opportunity to respond. If the requirement to disclose one's name when registering a domain name were to be dropped, the UDRP and URS procedures would need to be amended to provide that notice will only be sent to the email address provided – if any – during the transaction to acquire the domain name at issue. If no contact information is provided, then some sort of

notice by publication would be appropriate.

Indeed, as a matter of public policy and consistent with the GAC consensus advice, a registrant should not be able to refuse to provide contact information on the one hand, while also expecting notice and the opportunity to respond in the event of a complaint regarding the domain name. However, the difficulty in modifying this policy is the fact that ICANN is just beginning the process of reviewing the UDRP for possible revisions. This policymaking process is lengthy and is highly unlikely to result in such a significant change in time to meet the May 2018 deadline.

Anti-cybersquatting Consumer Protection Act and other civil actions

The other common procedure for recovering an infringing domain name in the United States is through a civil action under the Anti-cybersquatting Consumer Protection Act (15 USC Section 1125(d)). The act prohibits the registration, use or trafficking in a domain name that infringes or dilutes another's mark with the bad-faith intent to profit therefrom. The act enables a trademark owner to sue either the registrant or the domain name itself through an *in rem* action. If the registrant is unknown, the trademark owner can sue the unnamed registrant and then conduct discovery to try to identify the registrant and some means of serving the complaint on the registrant, such as an email address.

In cases in which the court cannot exercise personal jurisdiction over the registrant or cannot find the registrant through the due diligence of the trademark owner, the trademark owner can potentially pursue *in rem* jurisdiction over the domain name. The act provides for *in rem* jurisdiction only where the domain name registrar, domain name registry or other domain name authority that registered or assigned the domain name is located (ie, *in rem* actions in the United States would not be available for domain name registries located elsewhere).

In addition, the trademark owner must provide notice of the lawsuit to the registrant via the physical mail and email address provided by the registrant to the registrar and by publishing notice of the action, as the court may direct. If registrants are not required to provide consent to disclosure of physical or email addresses to registrars when they register domain names, it may be the case that only notice by publication would be required.

Indeed, the Anti-cybersquatting Consumer Protection Act provides that the *in rem* jurisdiction provided under the act is in addition to personal and *in rem* jurisdiction that otherwise exists. Thus, if a US court determines that a domain name is located in the judicial district (because the domain registry or registrar is located there), a court may decide that it can exercise jurisdiction over the domain name and that notice of the suit through publication is sufficient. Notice by publication is commonly recognised as a sufficient basis for providing notice of a dispute over property when the owners of the property cannot be identified or notified.

Conclusion

While the General Data Protection Regulation will make it more difficult for trademark owners to identify the registrants of infringing domain names, trademark owners are unlikely be left without a remedy. The UDRP and URS procedures as well as the Anti-cybersquatting Consumer Protection Act may need to be amended to provide for notice by publication where the domain name registrant has elected to provide no contact information when registering a domain name. In the interim, reliance on *in rem* jurisdiction may suffice, at least for recovering domain names when the domain registry or registrar is located in the United States. **WTR**

Lewis Roca
ROTHGERBER CHRISTIE

Lewis Roca Rothgerber Christie LLP
One S Church Avenue
Suite 700
Tucson AZ 85701
United States
Tel +1 520 622 2090
Fax +1 520 622 3088
Web www.lrrc.com