Trademark protection in the new gTLD environment: a policy and enforcement deep dive

Trademark and domain experts from the United States discuss the evolving landscape of generic top-level domains, exploring the challenges faced by the Internet Corporation for Assigned Names and Numbers and best practice in enforcement efforts

The generic top-level domain (gTLD) environment is constantly evolving, with new TLDs going live, reviews of the current rights protection mechanisms underway and the Internet Corporation for Assigned Names and Numbers (ICANN) grappling with how the EU General Data Protection Regulation (GDPR) will affect WHOIS in both the immediate and longer term. For trademark counsel, the need for effective policing and enforcement efforts, coupled with close monitoring of related policy issues, continues unabated.

In this exclusive roundtable, four trademark and domain experts – Corsearch's Stephen Stolfi, Virginia L Carron and Jonathan Uffelman of Finnegan, Henderson, Farabow, Garrett & Dunner, and Anne Aikman-Scalese of Lewis Roca Rothgerber Christie – provide insight into the challenges emanating from the ICANN world and explore best practice in enforcement efforts – including an exploration of Uniform Rapid Suspension system (URS) and Uniform Domain Name Dispute Resolution Policy (UDRP) decisions, policing efforts in a GDPR world and how to prioritise defensive registrations.

A review of new gTLD rights protection mechanisms (RPMs) is underway – what is your assessment of the protection mechanisms made available to rights holders? Are there improvements you would like to see?

Stephen Stolfi (SS): The protection mechanisms in place are sensible, but they need improvement to be practical and effective tools for rights holders in the long term. The Trademark Clearinghouse (TMCH) was a step in the right direction for trademark owners of new gTLDS and is working as a conduit mechanism to aid practitioners in their journey through the gTLD maze. However, it is only effective if it is used as it was intended – as a platform to keep rights known and protected. While it works well as a notification system for exact trademark names, what about for similar trademark names and typos? The TMCH is not as effective as it could have been because cybersquatters are still registering domain names that are similar to protected trademark names. A more valid proof-of-use requirement would help to weed out true non-users.

Meanwhile, the trademark claims process needs improvement. There should be an option for blocking registration of registered marks, in addition to notifying brand owners of the mark. While some blocking mechanisms are available, there is no reason that they should not be connected with and accessible through the TMCH. Finally, the URS is a mechanism that nicely complements the UDRP process, but it is underused because the burden of proof is high, so it is not that fast or simple; second, it provides only a suspension mechanism; and third, it has procedural limitations. So it does not provide a fully adequate solution. For the URS to do what it was meant to do, it has to be totally overhauled and simplified.

Virginia L Carron (VLC): One potential improvement to URS procedures would be to provide for more effective remedies for successful complainants. Currently the only remedy is the temporary suspension of a domain name for the remainder of the registration period. As a result, at the end of the registration period, a third party can register the domain name in question, cutting off the complainant a second time. It would be helpful for trademark owners – and the URS would be a more attractive protection mechanism – if remedies included cancelling the registration or transferring the domain to the complainant, like in the UDRP.

Anne Aikman-Scalese (AAS): In general, I agree that these mechanisms have worked well together as a suite of remedies for rights holders. Trademark owners are not one size fits all so approaches to the use of the RPMs will vary depending on the size of the portfolio and the nature of the client's business model and distribution channels. The TMCH has been an effective tool for many of our clients, especially those who do not conduct regular watches on domain names. However, there is definitely room for improvement. The new TREx blocking service offered by the TMCH will be a helpful addition when GDPR goes into effect. At present, it covers only 40 domains, but the service is affordable.

The following changes would be helpful to the trademark community. First, expand the TMCH notice to rights holders beyond "exact match". Second, add new policies in the next new gTLD round to curb the practice of offering so-called 'premium names' that are actually a direct match for TMCH-validated marks at exorbitant prices. Some of these names have been priced at tens of thousands of dollars, a practice which actually dampens trademark owners' enthusiasm for registering these domains at all. Why pay $25,000 for a domain (plus renewal

> **The protection mechanisms in place are sensible, but they need improvement to be practical and effective tools for rights holders in the long term**

fees year after year) when the owner can employ an inexpensive watch and later pay between $5,000 and $7,500 to recover the URL in a UDRP action if needed?

Let us look at the UDRP as that is also set for review. Are there changes you would make to the policy and is there a danger that its effectiveness could be negatively affected post-review?

Jonathan Uffelman (JU): The UDRP requires a complainant to establish that a disputed domain has been both registered and used in bad faith. This allows a registrant whose domain registration pre-dates the use of a brand owner's trademark to capitalise on the latter's consumer recognition by posting directly infringing content. In such cases where bad-faith use might be undisputed, but the domain name was not registered in bad faith, the UDRP will be unavailable, and substantially more expensive litigation may be a brand owner's only recourse. By contrast, some national domain dispute resolution procedures are written in the disjunctive, so a complainant may succeed by establishing that the respondent either registered or subsequently used the domain name in bad faith. Revising the UDRP to be written in the disjunctive would allow brand owners greater freedom to target the sorts of activity that the UDRP was intended to address.

Inconsistent results also remain a problem. Although the weight of UDRP decisions may point clearly to one result under certain circumstances, a level of uncertainty must always be factored in to any evaluation of likely success because the outcome might depend as much on the particular panellist deciding the case as it does on precedent. Unfortunately, where a UDRP party believes that a case has been wrongly decided, its only recourse is to file a court action. By contrast, Nominet's dispute resolution service allows complainants and registrants to file an appeal directly through Nominet. Like the UDRP and DRS procedure, the scope of this appeal is more limited than filing an infringement action in district court. Each party may file one substantive brief of no more than 1,000 words each and Nominet's fees are comparable to those incurred for filing the original complaint. The UDRP should provide for an appeals process so as to help create more uniform and predictable results.

AAS: I would say: "if it ain't broke, don't fix it." Many in the trademark community would also like to see a loser-pays provision added to the UDRP, even where the respondent does not ask for a three-judge panel. This would be a highly effective way to prevent bad-faith registrations. However, opening up the UDRP to big changes represents a veritable Pandora's box. The biggest vulnerability at present is, of course, the reality of ICANN's current GDPR compliance model, which would appear to make serving a UDRP complaint impossible given that the World Intellectual Property Organisation (WIPO) and other dispute resolution providers are third parties with no "accredited access" to WHOIS information under the GDPR. Assuming this problem can be fixed through an accredited access model, the biggest post-review danger is likely the insistence by certain passionate voices within ICANN that a decision for the complainant where the respondent has not filed a response somehow violates human rights of privacy and due process. If this principle gains traction, why would any respondent ever reply to the allegation of bad-faith infringement?

SS: We also would not recommend any changes to the UDRP. The UDRP has been a successful and effective mechanism for rights holders to protect their marks and the review by the Policy Development Process Working Group appears to be a drain on resources and a process that will bear limited added benefits for rights holders.

Inevitably the GDPR has been mentioned. At the time of talking, ICANN has requested that European data protection authorities (DPAs) provide specific guidance on its proposed interim compliance model. However, uncertainty remains as to what the situation will be in both the immediate and longer term with respect to rights holders' access to WHOIS. What do you think of the current approach taken by ICANN?

VLC: It is important to stress that searchable WHOIS information is a crucial component of online brand enforcement. If WHOIS information is hidden completely, even learning where and to whom to send a demand letter threatens to become a more involved and costly process. Online brand enforcement has often been referred to as the Wild West; if WHOIS information becomes substantially more difficult to access, this state of affairs will only get worse. As much of the current publicly available WHOIS content should be retained as possible, and at a minimum, a registrant's name and email address should be available.

The information must also remain accessible to brand owners and potential complainants for URS or UDRP proceedings and law enforcement officials and security researchers following private requests to investigate possible crimes and to mitigate

Corsearch

Stephen Stolfi
Chief commercial officer
steve.stolfi@corsearch.com

Stephen Stolfi is a member of the senior management team at Corsearch and oversees its digital brand services business. He has worked in the brand establishment and protection industry for over 25 years and has been with Corsearch for 18 years. Throughout his career, Mr Stolfi has helped to guide numerous Fortune 500 corporations and law firms on effective trademark clearance and brand protection strategies. He has also guest lectured at various colleges and universities throughout the United States, as well as local and global IP associations. He was most recently responsible for the successful registration of his former parent company's new .brand generic top-level domain and was one of the first members of the Brand Registry Group.

devastating malware attacks. Brand owners and law enforcement officials should not have to resort to subpoenas and court orders to acquire this basic information. Additionally, because registrars and the companies they serve operate across country and continent borders, a single solution would be preferable.

SS: At Corsearch we support open access of WHOIS information which is allowed by law. We are spending a significant amount of time and effort to try to understand the ramifications of the GDPR. Our general counsel and data protection officer, Diane Plaut, who is a certified privacy professional and authority on GDPR, is advising our commercial efforts to ensure that we are in compliance and also ensure that our clients are aware of what is happening. While the ICANN model does support the creation of an accreditation process for entities such as law enforcement, cybersecurity professionals and IP attorneys that require access to full WHOIS records for legitimate purposes, it could be a year before any such programme is fully operational. So, our concern is what will happen in the interim, particularly from May 25 onward (when the GDPR becomes enforceable). The bottom line is that this will make it harder to investigate and police against cybercrime and IP infringement, leaving rights holders with nowhere to turn to protect their valued rights. A great deal of work remains to be done and it appears to be non-sensible and unacceptable that there are no answers or working outlets at this time, with the date of GDPR implementation so close. There needs to be a temporary solution and rights holders have the right to demand it. At a minimum, the accreditation process should be put into effect immediately even if it is not perfect from the start and rights holders should have access to a registrant's name and email address.

AAS: I do think that ICANN's current GDPR compliance model (as of April 15 2018) is both overly broad and certainly late in coming. The issue of balancing public safety and IP rights on the one hand, with privacy rights on the other, was carefully addressed by the tiered access approach proposed by the Expert Working Group on WHOIS years ago. Those recommendations could have been moved forward in a timely manner under the banner of compliance with the law, which ICANN is now flying. Instead, the ball was kicked to the Generic Names Supporting Organisation policymaking process and that process stalled even with seasoned leadership doing its best in the Registration Directory Services Working Group.

Some of the delay is no doubt due to the natural conflict between the ICANN board's fiduciary duty to protect the corporation itself from the risk associated with being held to be a joint data controller under the GDPR and its duty to advance trust and confidence in the Internet. But why did it take until Autumn 2017 to request a formal legal opinion on the effect of GDPR? The bottom line is that the board and the community need to work together with the Article 29 Working Party and the DPAs to find a way to make UDRP service effective even while an accreditation system for WHOIS access is being developed. Otherwise, ICANN will once again open itself up to accusations of mismanagement of the Web and renewed calls for transfer of authority to the International Telecommunications Union. It is unfortunate that formal Governmental Advisory Committee advice was required before serious approaches to resolution of the compliance issue were undertaken.

The current ICANN GDPR cookbook is a bit of a boiling caldron, especially in light comments within the ICANN community and from the Article 29 Working Party which will become the EU enforcement board for GDPR on May 25 2018. These conflicting comments make it clear that an agreed access system for IP attorneys and rights holders will take a long time to achieve. Accordingly, the ICANN board would be wise to adopt an emergency policy under the Registry Agreement that requires registrars to obtain an email address from registrants that contains no personal information. This would at least permit the UDRP and URS mechanisms to continue to function. Specification 2 of the Registry Agreement would permit such an emergency policy to continue for up to one year while an accredited access program is being designed. There are signs that the board is making progress on this front. Hopefully ICANN will adopt a new model by May 25 that permits the UDRP to continue to function.

As far as can be discerned at this time, then, how should brand owners adapt their enforcement strategies in light of GDPR?

AAS: Unfortunately, brand owners will be forced into increased costs by a combination of more defensive registrations, more purchasing of blocking services and increased litigation, including against relatively innocent internet service providers (ISPs). Hopefully the ISPs will be able to bring some pressure to bear on the issue of continuing availability of the UDRP remedy pending development of an agreed accredited access system for registrant information. Given the increased costs associated with enforcement and the perceived lower importance that consumers place on domain names (as opposed to social media), we have seen clients selling at retail elect to skip some domain name enforcement options which they engaged in during previous years. Brand owners need to decide whether the costs of blocking services and other enforcement mechanisms are worth the potential risk of infringing domains, given the characteristics and actions of their customers and the possibility for post-infringement enforcement.

SS: Without full WHOIS records to investigate potential infringement, practitioners will need to seek alternate methods and data sources to help them identify patterns of abuse. First, brand owners are going to need to expend greater internal and external resources to investigate potential abusers and they are going to need to submit abuse complaints to registrars much more frequently in order to justify access to WHOIS records. Further, the need for domain name watch services, as well as services which identify the public (or previously public) contact details for cybersquatters, is going to be even more important.

JU: For now, enforcement strategies in the wake of the GDPR are evolving as

information sharing evolves. Until a new solution is proposed, brand owners should continue to monitor misuse of their brands as before, possibly being more proactive in the event that enforcement becomes more difficult in the future.

In terms of wider enforcement, reflecting on round one, to what degree did the new gTLD expansion practically affect policing efforts?

AAS: Both defensive registrations and trademark enforcement against infringing domains are now much more expensive. Although the URS was intended as a less costly and quicker remedy than UDRP, decisions have been inconsistent and the so-called 'freeze' remedy less satisfying to rights holders. In addition, the necessity of a finding on the merits based on clear and convincing evidence when a registrant does not answer the URS complaint may be the root cause of most inconsistent decision making.

VLC: Naturally, expanding the universe of gTLDs greatly affects the potential for cybersquatting and domain misuse and thus the need for policing by brand owners. The potential confusion for consumers and the need for effective brand policing are limited only by a cybersquatter's creativity. Early efforts to protect consumers have provided brand owners with some opportunities to protect their rights but they almost all come at a cost, burdening brand owners with additional expenses to proactively defend their brand or fight squatters. Expansion of the sunrise period and notices to brand owners for use of their mark could aid in the timely policing of bad actors.

SS: We have clearly seen growth in UDRP cases filed against new gTLDs, primarily driven by TLDs with low-cost acquisition models, and that has required broader policing efforts across the board. Of course, this will be much more difficult after the May 25 GDPR enforcement date. While the expansion has increased policing needs, it has also widened the whole landscape, so that rights holders do not have to chase small players but can instead create and protect a more targeted exact population of registrants. On the whole, policing is becoming more sophisticated as the expansion allows for more defined policing programmes.

Are there particular URS and/or UDRP decisions that you feel have been particularly noteworthy over the past 18 months?

SS: *Yves Saint Laurent* was noteworthy because they effectively used the URS platform and the UDRP together against the same registrant – first getting the domains in issue suspended (*Yves Saint Laurent v Khita Kongsansatien*, NAF Claim 1565626), followed by the decision order to transfer the domains through the UDPR (*Yves Saint Laurent v Khits Kongsansatien*, WIPO Case D2016-0496). While this case is older than 18 months, it is a good example of the way that the process should work. It proves that we can achieve holistic results without the need for two independent platforms – that should be the goal.

AAS: The transfer of 'virginpvcpipe.com' (D2017-0934) in July 2017 was also noteworthy in that the panellist found for Virgin Enterprises where the respondent failed to reply. The ruling found no legitimate interest on the part of the respondent and concluded that the disputed domain name had been registered "in an attempt to attract Internet users to its website for commercial gain, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation or endorsement of the website or of the products presented on the website". Oddly, the panellist stated that

Finnegan, Henderson, Farabow, Garrett & Dunner

Virginia L Carron
Partner
virginia.carron@finnegan.com

Virginia Carron, managing partner of Finnegan, Henderson, Farabow, Garrett & Dunner, LLP's Atlanta office, practises patent and trademark litigation, counselling and prosecution. Her client base is broad and includes computer software and hardware companies, members of the telecommunications industry, the world's largest manufacturer of hand-made cigars, a large international chemical and minerals corporation and numerous international clients in various technology fields. Ms Carron counsels clients on IP licensing and related transactional matters in both trademarks and patents for several Fortune 500 companies. She has served as first chair for several different plaintiffs in counterfeiting and trademark infringement litigation, which resulted in the recovery and destruction of millions of dollars' worth of counterfeit goods, and in two cases the incarceration of counterfeiters of computer memory products.

Finnegan, Henderson, Farabow, Garrett & Dunner

Jonathan Uffelman
Domain name specialist
jonathan.uffelman@finnegan.com

Jonathan Uffelman is an attorney and domain name specialist in Finnegan, Henderson, Farabow, Garrett & Dunner, LLP's Washington, DC office. He practises trademark, domain name and Internet law. In particular, he works on a broad range of internet and cyber law issues, including online brand enforcement and the Uniform Domain Name Dispute Resolution Policy (UDRP) proceedings. Mr Uffelman handles a variety of online brand enforcement issues including grey-market goods, trademark and copyright infringement, and cybersquatting. He has successfully handled numerous UDRP cases on both the complainant and respondent side, and his practice spans a wide spectrum of industries.

the fact that there was no further mention of the term 'virgin' in content posted on the site reinforced this conclusion. No mention was made in the ruling of the fact that 'virgin pvc' is an industry term for a type of PVC pipe that is distinguished from 'recycled pvc'. So now when you go to 'www.virginpvcpipe.com', you are redirected to Richard Branson's companies. Should we be asking complainants to specify to panellists whether any known industry terms appear in the alleged infringing domain?

VLC: I would highlight two UDRP decisions. *Paul DiCocco v Curtis Lee Mickunas* (D2017-1982, January 15 2018) is noteworthy for its interpretation of Paragraph 4(c)(iii) with respect to fair use. The panel determined that the central question to the fair-use analysis is whether the purpose is illegitimate and not "the specific nature and extent of the criticism". There are notable challenges for brand owners enforcing trademarks against so-called parody sites or free speech sites, particularly in the United States. However, this case shows that where the brand owner can show that the purpose of the site is illegitimate, then analysis of the quality of fair use may be avoided.

The second is *Air Serbia ad Beograd Jurija v Domains By Proxy, LLC* (D2017-1986, December 18 2017), which noted that if "subsequent evidence come[s] to light which would demonstrate a bad faith intent on the respondent's part, it is possible that a future panel may entertain a refiling of this complaint". This serves as an important reminder that filing a UDRP action does not preclude a future case. Thus, in the event that a complainant loses a particular action, under certain circumstances it may be able to bring a subsequent, successful action.

What is your assessment of the value of voluntary (non-mandated) blocking mechanisms adopted by some new gTLD registries?

SS: Those registries were first movers and should be commended for their efforts. It should be easier for brand owners to block registrations across all new gTLDs. Some type of universal blocking mechanism should have been an integral feature of the new gTLD programme from the very beginning, thus eliminating the need to evaluate and manage blocks on a piecemeal basis through different registries or mechanisms. This could have been done in such a way as to allow the registry operators to keep most of the revenue from the blocking subscriptions without multiple processes needing to be maintained.

AAS: Blocking mechanisms would certainly be much more effective if they ran across all TLDs. At present, not enough TLDs are covered to establish an effective remedy for trademark owners. In addition, for smaller brand owners, the cost of Donuts' DPML blocking service at a minimum expenditure of almost $6,000 per mark over 238 domains may be prohibitive.

JU: Voluntary blocking mechanisms can provide an important defensive tool for trademark owners. However, most are not free and the additional cost associated with using these mechanisms is yet another burden on trademark owners in protecting both their brand and consumers. The value added to a company is based on balancing the cost of blocking each gTLD associated with a trademark with the risk of a third party squatting on its rights and the costs associated with fighting that third party. While all trademark owners want to protect their rights, not all are benefited by the additional cost of defensive blocking mechanisms. Moreover, in most cases, the cost of blocking is relatively close to the cost of registering the additional domain. For certain domains, it may be worthwhile to register (rather than block) the extra domain name and have the wrong domain redirected to the correct one. Redirecting services have proven to be extremely helpful for several clients.

Outside multi-TLD blocks, what is your advice to brands with respect to defensive registration strategies?

AAS: No brand can afford to chase defensive registrations or blocks in every TLD. Effective enforcement strategies involve a careful analysis of domains which are likely to be problematic and cause confusion, actual customer complaints and fact situations which require strict enforcement. The strategy itself has not changed but the volume of analysis and action required has multiplied dramatically. This is so burdensome that it is actually an argument in favour of a '.brand' TLD and/or significant advertising and promotional efforts to tell customers that no site other than a brand's authorised site can be trusted. We have found that in the past few years the explosion of TLDs and the likelihood that a new company's brand has already been reserved by the registry as a premium second-level name means that brand owners are increasingly using a non-premium URL, or some other creative workaround, as their primary internet address. As a result, consumers are less likely to assume that a domain name containing a brand name is associated with the particular brand, and therefore the risk from not owning a domain name containing a brand name may become lower as marketing practices adapt.

JU: One of the most effective defensive strategies is to develop strong consumer recognition in a trademark. An important way to do this is to consistently use the same mark, or marks, across all platforms. The clearer a specific mark is to consumers, or the less diluted a mark is even within the same brand, then the better the protection available to the brand owner when enforcing its rights. For example, the activity a UDRP panellist is likely to find constitutes bad-faith use

> **Budgets are increasing to account for the need for more enforcement**

may expand or contract depending on how strong the asserted trademark is. Similarly, UDRP panellists may be more willing to infer bad-faith registration based on the strength or fame of the mark alone. Additionally, clients may consider investing in improving search engine rankings so that consumers looking for the client are more likely to find them. In developing a defensive registration strategy, clients should be forward thinking with regard to business growth, defending where the business may develop and not only where it is today. For example, a brand that markets only products today may be connected to a non-profit in the future.

SS: The best course of action will vary widely based on the client's business, trademark portfolio, history of infringement, appetite for risk and budget. That being said, brand owners are now less focused on defensively registering their marks in every TLD because of the vastly increased costs; instead they are focusing on watching and enforcement strategies to protect their core portfolio. For most brand owners, a complete strategy should combine trademark portfolio alignment, defensive registration, offensive registrations in key industry TLDS, geographic coverage, blocking mechanisms and watching services as appropriate for a brand owner's needs.

What arguments could counsel make for increased budget to meet the challenges created in the expanding online environment?

VLC: Every day more and more markets are moving online. Whether economic, social or informational, the ability of a business or organisation to capture its corner of the Internet is a fundamental building block in any growth strategy. As with most intellectual property, it pays to stake a claim early rather than to add significantly more expense later in fighting others who have encroached on a business's market. Accordingly, money budgeted early likely will aid in productive development strategies for the business and may even defray costs later. Additionally, as discussed above, the potential impact of the GDPR on rights holders' access to accurate and reliable WHOIS data may make online brand enforcement a more costly endeavour.

SS: There are numerous arguments for increased budgets because as the traditional brand marketplace vanishes and there are ever more outlets for infringement and more information and resources to sift through, follow and police, the world of brand protection has become more challenging and more time consuming. Counsel need to work with service providers who have sophisticated tools to aid them in the journey of brand protection. As the technological complexities grow, the cost of creating better and more effective tools will increase also. Counsel should invest in tools and resources that specifically address the nature of their respective business.

AAS: This is actually not a problem. Clients are coming to us as their representatives with more customer complaints and complaints of infringement. We are also bringing more issues to their attention via TMCH notices and the traditional watch process. Accordingly, budgets are increasing to account for the need for more enforcement. As a side effect, there is not much enthusiasm among the business community outside ICANN for a next gTLD round and ICANN does not even have one in its budget projections for the next few years.

Any other issues you would like to raise?

AAS: It is incumbent on the ICANN community to acknowledge once and for all that in contentious situations (eg, GDPR right now and certain RPM implementation issues in the 2012 round), it is really the ICANN board that has the final say on policy. The fundamental structure of stakeholder groups and advisory committees means that the ICANN board must, on occasion, step up proactively to move the community forward. Too often, forward progress is impeded and the organisation is ineffective due to the perpetuation of the myth that the board does not make policy. The reality for those of us who represent trademark owners (and their corresponding interests in consumer protection) is that we are very much indebted to the Governmental Advisory Committee for the protections that currently exist, as well as those that will be developed going forward under the legitimate interests provision of the GDPR. For the registries and registrars, these legitimate IP and consumer protection interests merely represent added costs in the conduct of their businesses. So why would they be interested in a rapid resolution of the GDPR issues? **WTR**

Lewis Roca Rothgerber Christie

Anne Aikman-Scalese
Of counsel
aaikman@lrrc.com

Anne Aikman-Scalese is of counsel with Lewis Roca, assisting clients with worldwide trademark prosecution strategy, due diligence, dispute resolution and licensing transactions. She currently manages global trademark portfolios for the largest division of a Fortune 150, an online retailer doing business worldwide and a Southwestern resort and casino with entertainment venues. In addition, Ms Aikman-Scalese handles copyright matters for artists, authors and Native American communities. She has been in leadership at the International Trademark Association for over 15 years and has been a speaker for the American Intellectual Property Law Association, the Practising Law Institute and the World Intellectual Property Organisation. A member of the Internet Corporation for Assigned Names and Numbers (ICANN) IP Constituency since 2010, Ms Aikman-Scalese is knowledgeable with regard to enforcement issues raised by the proliferation of unlimited top-level domains and the effect of the General Data Protection Regulation on changes in ICANN's approach to compliance with WHOIS.