Harms of Intellectual Property Protections in Internet Namespaces

Curtis M. Kularski

8 May 2018

The linguistic territory of the Internet, the domain name system, has recently undergone a large-scale expansion and you can claim a piece of it for yourself in the form of a domain name. This is exciting news for bloggers, photographers, artists, writers and anyone else who has or wants an online presence that previously struggled to find the perfect name in dot-COM! There is one catch however, you may be blocked from getting the perfect name in one of the new domains if it is similar to someone else's trademark or you may be able to register your new domain name but have it taken away later because a corporation demonstrated they had a prior legal claim to it, even if you were not aware of their trademark.

Domain names compose the lexical and semantic core of what most Internet users perceive as being the Internet. Domains function as an address, a way of locating resources, but also as an extension of the identity of the resource being accessed. The identity may be a corporation, a non-profit organization, an individual or any other configuration of personal or organizational identity. In generic top-level domain names (TLD), such as dot-COM, there are no restrictions on who can register a domain name, but the present arrangement of policies does advantage trademark holders and commercial organizations over other entities, including individuals, that would register a domain name.

Domain names are hierarchical, with the various levels being denoted by a dot between named spaces. The right-most portion is the top-level domain. The top-level domains are

registered in an invisible root zone[1]. The portion one dot from the right-most portion is the second-level domain, or simply 'domain name'. Internet Corporation for Assigned Names and Numbers (ICANN) is the governing organization that sets policy for the root zone and as a result exercises control over all top-level domains and the general principles of Internet naming inside the top-level domains.

Intellectual property protections of domain name registrations such as the Uniform Domain-Name Dispute Resolution Policy (UDRP) and the Trademark Clearinghouse (TMCH) are designed to protect intellectual property holders from malicious registrations that intentionally infringe upon their trademarks. UDRP protections were created during a time when there was domain scarcity due to finite technically and socially valid domain names. ICANN's recent expansion of the number of top-level domain names changes the underlying assumptions that existed at the time of the creation of the UDRP.

The addition of new generic top-level domain names (gTLDs) was accompanied by more elaborate protections and defenses for trademark holders. The new protections grant trademark holders the universal capability to defend their trademark without regard for legitimate cases of name duplication. A trademark holder has the capability to monopolize their string across all generic top-level domains. It is also possible for rights holders to force a domain owned by non-rights holders to be suspended before any arbitration or other due process can occur. This harms organizations that have not registered their names as a trademark, informal organizations and individuals by depriving them of their preferred domain name artificially.

[1] The root zone is invisible in the human-facing interactions with the DNS system, but is denoted by a trailing period (.) in the DNS protocol (Berners-Lee, 1994).

The policies and their impact to non-trademark holding entities translate systems of privilege from the physical world to replicate it on the Internet. Large organizations can easily block access to or take away domains from entities with fewer resources, reinforcing their control over language, space and even identity. To protect the future of the Internet as an open community of ideas and diverse perspectives, non-corporate entities must be seen as having value under the policies governing domain name registration because domain names are the essence of an online identity. Domain names are the only unchanging method for locating content, and by extension content creators, reliably. Other methods of establishing an identity online, such as social media profiles, rely on the longevity of the platform and a degree of unambiguity to be reliably located.

To eliminate unequal protections for different classes of Internet users, the existing policy structures must be altered to accommodate new idea for how an entity establishes a legitimate claim to a name. Further, policies that permit early access to domain registration in new gTLD for some groups are inconsistent with the principles established by the founders of the domain name system.

Intellectual Property Law & the Internet

When the first domain names were registered in 1985 it was not anticipated that the Internet would become a hub of commercial activity (Alramahi, 2008). There were initially no policies governing who could register a domain[2]. The accepted policy as of 1994 was that "the same rules are applied to all requests, all requests must be processed in a non-discriminatory

[2] MIL, GOV and ARPA were and remain restricted top-level domains that require special permission for registration

fashion, and academic and commercial (and other) users are treated on an equal basis" (Postel, 1994). While the policy of non-discrimination in accepting requests for domain names is consistent with the type of open system that the founders of the Internet hoped to create, it clashed with ideas of trademark claim and branding practice (Leiner, et al., 1997).

As the Internet grew between 1985 and the mid-1990s, some individuals became abusive of the open nature of the domain registration process in the absence of policies regarding the relationship between existing names and domains (Leiner, et al., 1997). Bad faith registrations began to occur, intentionally blocking legitimate registrants from gaining domain names related to their trademark, in a practice known as cybersquatting. Some of these cyber squatters extorted money from corporations in exchange for the domain name matching their brand or trademark. Other cyber squatters attempt to present themselves as if they were the entity typically associated with the name (Wright, 2012). Commercially this type of abuse is harmful because it can be used to deceive consumers and create a marketplace for counterfeited goods. Cybersquatting is typically considered an issue of concern to commercial entities, but the dilution or intentional misleading use of a name can be just as harmful to non-commercial entities, a fact that is often overlooked in discussions of intellectual property on the Internet. For example, if a cyber squatter were to register a domain in the name of a well-known scholar, it would deprive the scholar access to use the domain for their own purposes. If a website were established on the domain in the name of the scholar, but hosted material that was not academically rigorous or were contradictory to the scholar's personal beliefs, it would impede the identity of the scholar.

In the original policies of the domain name system, for situations where a domain name was disputed between two (or more) parties, it was left to the parties to seek a resolution, whether legal or otherwise. In September 1995, some parties who could not otherwise reach a

resolution began suing Network Solutions (NSI), the predecessor to ICANN, to gain access to domains that were in dispute (Weston, 2000). By July 1996 NSI had created a basic dispute resolution policy that would permit trademark holders to transmit a copy of their United States trademark registration to certify their claim to a domain name that was an exact match to the mark registered. If the domain holder could not produce a mark registration of their own within 30 days of a dispute being raised, then the domain was transferred to the trademark holder. This very simplistic process was efficient at catching and resolving cases of cyber-squatting, but unfortunately, it did not allow for any form of common-law use of a name (Weston, 2000). Recognition of common-law trademarks would enable those without formal registered trademarks to establish a de facto claim to a domain name based upon their prior use of that domain for productive activities.

There are three reasons for this bias in the early DNS system. First, the recognition of only registered trademarks was a convenience to NSI due to being simple to verify. Verification of a registered mark required no additional resources beyond those already required to operate the registry[3]. Second, registered trademarks would have been the only class of intellectual property that NSI (and eventually ICANN) was obligated to recognize due their status as a contractor for the United States Department of Commerce. Finally, in the beginning registered trademark holders were the primary targets of cyber-squatters, therefore the group that needed protection at the time.

[3] Until the transition to ICANN and the shared registry model, most changes to domain name registrations were conducted with notarized letters and forms, therefore trademark claims were handled as a routine administrative process.

The assumptions that were established as a reaction to early cyber-squatting complaints were carried forward into the fabric of modern intellectual property protections, embedding trademark holders as a privileged class of domain registrants.

Changing Landscape of Internet Names

The initial top-level domain names (COM, NET, ORG, EDU, MIL, and GOV) were based on broad categories with the intention on being generic classifications for organizations. At the time the categories were sufficient and representative of the composition of the Internet. There were just over 1,000 computers attached to the network and they were owned by entities in those categories (Postel & Reynolds, 1984). The original specification that created the initial set of top-level domains, RFC 920, specified ORG as the only top-level domain that would be appropriate for entities that were not governmental entities, educational institutions, commercial companies or network operators (Postel & Reynolds, Domain Requirements, 1984).

Due to organizational isomorphism and other social factors, the COM top-level domain became the accepted standard for brand identity representation on the Internet. In the early 1990s, established companies began expanding into the online space and registered in the appropriate namespace, COM for commercial entities. Due to the popularity of the Internet occurring during and because of the success of commercial entities on the Internet, COM took on a broader generic meaning than was initially intended. As COM quickly became the most visible of the top-level domains, it gained a sense of standardization and was a symbol for the Internet itself to many early Internet users (Goodnight & Green, 2010). The number of semantically

meaningful domain names available to register in COM waned, resulting in pressure to ICANN from the Internet community to expand the number of available top-level domains.

After the Internet grew in popularity and population ICANN still resisted adding new top-level domain names due to concerns about the technical stability of the root zone (Internet Corportation for Assigned Names and Numbers, 2010). In June 2008 ICANN issued a policy which initiated a process for adding new generic top-level domain names on an unlimited scale. The new generic top-level domain names are not restricted to being broad categories and do not necessarily describe the type of entities that register within them.

As of 2018 there were over 1,300 new top-level domains delegated in numerous categories, such as political affiliation (.REPUBLICAN, .DEMOCRAT), location (.NYC, .LONDON), culture (.SOY, .CAT), social designators (.MOM, .MEN) and "super-generics" (.XYZ, .OOO) (Internet Corporation for Assigned Names and Numbers, 2018). The distinction between what used to be and what now exists is important because it is an area where the prior theories of intellectual property related to the Internet begin to break down.

Until this point only what existed to the left of the dot mattered for trademark purposes, primarily because most of the quarreling entities were registered in the COM gTLD and in most cases only commercial entities possessed a defensible trademark. The increase in the diversity of the top-level domains means that it is possible for trademarks to be considered in context of the full registered string. Lisa Sharrock (2001) states, "there can only be one 'united.com'". This is as much true as it was when she wrote the line, but now entities sharing the same trademark (or other identity marker) have the option of locating themselves inside a space that more closely matches their industry, service area or other identity category rather than fighting for a single domain that only identifies the identity marker inside a large organizational classification.

The expected result of this expansion based upon ICANN's reasons for the expansion and even the nature of trademark law should be that there are fewer domain disputes and less scarcity in domain name selection.

Objections of IP Advocates to new gTLDs

Intellectual property advocates expressed concerns about how the addition of new gTLDs would impact trademark holders and brand owners (Stein & Horowitz, 2015; Joseph, 2012). Common objections include the cost of registering brands in all new gTLDs to protect their brand identity, cost and labor associated with monitoring gTLDs for intellectual property violations and the potential of confusing consumers (Joseph, 2012). ICANN, which at the time was still under the guidance of the United States government, responded to the concerns by implementing new intellectual property protections. These protections aimed to calm concerns of trademark owners while still allowing the domain expansion to go forward (Stein & Horowitz, 2015).

"Domains have become an integral part of corporate branding" claims Joseph (2012). While this is true, it does not in itself constitute a reason to limit the number of top-level domains or to create wide-reaching trademark protections. Joseph (2012) uses the example of Coca-Cola's Sprite brand to defend her claim that consumers would be confused by additional top-level domain names. While a TLD like DRINK or BEVERAGE[4] could permit a registration that

[4] As of the time of this writing, neither DRINK nor BEVERAGE had been approved or delegated and function only as an example

would violate the Sprite brand, a group of fantasy or Shakespeare enthusiasts could register <sprite.club> without violating the Sprite trademark or brand identity.

The efforts and objections of brand owners focus on the protection of commercial interests on the Internet and particularly of preventing any disruption in the process of connecting consumers with brands (Joseph, 2012). When the domain name system was first established in 1984, commercial entities were only one of the types of entities that were anticipated to be part of the Internet (Postel & Reynolds, 1984). Educational institutions, governmental agencies and non-profit organizations were expected to be the other classes of entity that would need a named space on the Internet. Two of those, education and government, have spaces that are specified to be exclusively for their use (EDU and GOV).

Commercial entities are not the only entities utilizing the Internet as a platform and therefore the use of trademarks, which are inherently linked to commerce, are an inadequate and inappropriate way to determine domain rights.

Uniform Domain-Name Dispute Resolution Policy

The Uniform Domain-Name Dispute Resolution Policy (UDRP) was created by ICANN in cooperation with World Intellectual Property Organization (WIPO) in its original form in 1999, several years prior to planning for new gTLDs (Weston, 2000). UDRP is an extension of the previous NSI dispute resolution policy. A key change is that UDRP removes all of the burden for managing disputes from the registry or name system owner and instead places the responsibility of arbitrating the dispute with independent arbitration panels at the expense of the rights-holders (Internet Corporation for Assigned Names and Numbers, 2012). While placing the

financial burden for arbitration on the rights holder may seem like a method for balancing the power relations, it does not in reality because the burden for proving legitimate ownership of the domain still rests with the domain owner. There are also occasions where multiple trademark holders of different sizes and industries have disputed the same name, maintaining a power imbalance (Sharrock, 2001).

UDRP offers some additional protections over the previous policies in that there is a requirement that some form of bad faith be demonstrated. The significant change to the policy is that three conditions must be met before a domain name can be transferred to a rights holder:

> "(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
>
> (ii) you have no rights or legitimate interests in respect of the domain name; and
>
> (iii) your domain name has been registered and is being used in bad faith."

Condition (i) is an extension of the authority of the previous dispute process that required the marks to be identical, in UDRP even a similar mark may be protected. The remaining two conditions are subjective and are at the discretion of the arbitration panel to determine. In many previous cases, the "bad faith" condition was met only by the demonstration that consumers arrived somewhere other than they expected (Sharrock, 2001).

The UDRP requirements for a domain owner to enter into arbitration with a disputing party is made enforceable by the legal agreement that must be accepted by every domain registrant before they can purchase a domain name (Internet Corporation for Assigned Names and Numbers, 2013).

New Intellectual Property Policies Effecting New gTLD Registrants

When creating the new gTLD program, ICANN was under pressure from intellectual property rights advocates, such as the World Intellectual Property Organization and various private companies, to increase protections for trademark holders (Brown, 2012). As a result, ICANN wrote additional protections into the standard registry operator contracts that must be executed before a new TLD could be delegated in the root zone. Whereas the existing UDRP protections are designed to protect trademarks after a domain name has been registered the new policies are designed to protect trademarks before a TLD is open for general registration (Internet Corporation for Assigned Names and Numbers, 2015).

The Trademark Clearinghouse (TMCH) authenticates trademarks and allows rights holders to centrally register their trademark in a single system for use in either defensive registration or in mark restriction in multiple top-level domains. Trademark rights holders also have the option to utilize their registration in the TMCH to begin later arbitration or dispute processes (Internet Corporation for Assigned Names and Numbers, 2015).

New gTLDs are opened in phases. The first phase is called Sunrise. During Sunrise registrations are limited to entities that have successfully registered their trademarks with TMCH. Registrations placed during this time are ‘defensive registrations’, as their purpose is to allow trademark holders to simultaneously protect their trademark and establish their claim in the new gTLD (Internet Corporation for Assigned Names and Numbers, 2015).

Trademark Claims Service allows for various types of trademark protection. Rights holders can file restrictions for the use of their marks in specific top-level domains or across

multiple top-level domains at once. Some options produce a notification to would-be domain registrants that warns of their potential infringement, whereas other options block specific strings from being registerable in the gTLD at all (Trademark Clearinghouse, 2018).

The Trademark Clearinghouse and the services it offers, including Trademark Claims Service, permit trademark holders the ability to select how they wish to handle the registration of similar marks. One option functions to prohibit the general availability of domains matching a mark registered with the Trademark Clearinghouse before the top-level domain opens for general registration. Prohibiting the availability of certain strings reduces the number of viable domains for registration under the top-level domain, which is contrary to the public good of the Internet and is contrary to the mission of ICANN when they began the new gTLD program. Another option open to rights holders is the ability to permit registrations but be notified of the identity of the entity that registered an offending domain name. A potential registrant is notified that the string they are attempting to register is listed with the Trademark Clearinghouse but is permitted to continue with the registration. While this may seem to be a progressive alternative to blocking registrations completely, it is more appropriate for other trademark holders with the same or similar mark. Only another rights holder with legitimate claim to the domain could register the domain without the risk of the domain being suspended or otherwise taken by the rights holder in the future.

Uniform Rapid Suspension (URS) supplements the existing UDRP dispute protections to allow trademark holders to quickly and inexpensively initiate a process to suspend domain names that use names that are similar to registered trademarks. An independent organization validates that the claim filed matches or is confusingly similar to the domain disputed. If the URS objection is passed then the domain name is immediately suspended. One of the harmful

problems with the URS process is that it is based only on the documentation from the complainant and often the registrant of the offending domain name will not be notified of the domain suspension until after it has occurred (Internet Corporation for Assigned Names and Numbers, 2015).

Some registry operators[5] that manage large numbers of top-level domains, such as Donuts Inc., have taken further actions to protect mark holders in the TLDs they operate. Whereas the Trademarks Claims service and Sunrise process require the trademark holder to specify each TLD individually and pay the cost for each TLD separately, the registries collect an annual fee to protect the mark in the TLDs they manage. Donuts calls this a "Domains Protected Marks List". Any mark on the list is prohibited from registration for as long as the protection is renewed (Donuts Inc, 2018). This fee-based "mark list" creates a source of revenue for the registry operator but denies any entity the ability to register a domain matching one of the protected marks.

Abuse of Trademark Protections

Trademarks are a part of the legal tradition in the United States and other countries that are foundational to the concept of intellectual property, but they do not grant ownership or monopoly rights to a particular mark. The difficulty with the new policies that allow trademark holders to block registrations in any (or all) new gTLDs and have priority registration access across all new gTLDs is that it grants trademark holders universal rights based on an intellectual

[5] A registry operator is the entity to which a top-level domain has been delegated. A registry operator is responsible for the technical operation of the domain and is under contract with ICANN for the execution of that role.

property construction that was designed to be restricted to a specific category of goods or services. Applying trademark rights to the COM TLD was somewhat less complicated because it was defined to encompass any type of commercial entity and as such, there was more risk in losing a de-facto equivalent to the mark online. Culturally, the COM portion of the name became an invisible technical inconvenience rather than a bearer of meaning.

In the new gTLDs the top-level string is included in the overall meaning of the full domain name, which for many trademark and TLD combinations makes little semantic sense. As an example, Apple Inc. produces various electronic devices and computers and holds trademarks for the wordmark ‘Apple’ in the relevant good and service categories. This would enable Apple to defensively register or block registration of ‘apple’ in any top-level domain. Apple Inc. would have rights to block a registration for <apple.pub>, which does not represent a class of product for which Apple Inc. holds trademark. Apple’s block could prevent other parties with a bona-fide purpose for the domain from being able to register it. Any challenge to Apple Inc.’s block would also require registration with the TMCH to be recognized as an entity with a valid legal interest in the domain.

The requirement to register with the TMCH is not in the best interest of the Internet community as it legitimizes a specific type of intellectual property structure and disregards less formal uses of marks. Uses of marks or identifiers that are not registered are not protected and cannot be defended. If Justin Bieber’s fans wished to register BELIEBERS.CLUB (in reference to their self-ascribed collective name) they would only be able to do so during the general registration window (after the Sunrise defensive period) and only then if Bieber’s record label had not filed a trademark block or performed a defensive registration prior to that point. By

recognizing only specific types of identifiers as having legitimacy the scope of protection is very narrow.

The expansion of the top-level domains to include narrower categories necessitates re-evaluating the way in which trademark rules are applied to domain names. Domain names are not examined holistically under the current UDRP guidance. Current UDRP rules actually specify the opposite, that the top-level domain name is not to be considered in any evaluation of dispute claims (Internet Corporation for Assigned Names and Numbers, 2012). In a namespace which has only three viable options under which a name could be registered such a broad interpretation of trademark and ignorance of the top-level is logical, but with several hundred possible extensions there is meaning to be found in the top-level.

The current use of trademark protections could be used by a trademark holder to create a monopoly of their mark across all top-levels, regardless of the applicability of the top-level to the mark, either in common use or as formally declared by the registry. While it is unlikely that many organizations would do this, it is a flaw in policy that this act is permitted without viable recourse for those adversely affected. Further, examined as an ethical case, if many organizations were to act on this flaw the expanded number of TLDs would fail to alleviate domain scarcity and would be unsuccessful at promoting a more diverse utilization of domain names.

Multiplicity of Names

The lexicon in any given language is limited and as such so are short, memorable names and brands. This results in the duplication of names across industries and sometimes in the same

industry. This is an important factor as it demonstrates that there is a need for permitting conflicting names in different TLDs.

Many organizations with long names abbreviate their names when selecting a domain name to make the domain more memorable and easier to input. As an example, consider three distinct academic associations: American Psychological Association (<apa.org>), American Psychiatric Association (<psychiatry.org>) and American Philosophical Association (<apaonline.org>). Only one of the three 'APA' organizations can own the obvious domain name, apa.org. There are presently 53 active registrations for the term 'APA' in the United States Patent and Trademark Office (United States Patent and Trademark Office, n.d.). This search did not include pending applications or registered trademarks in other countries. Any one of the 53 holders of the 'APA' trademark could register the mark with the TMCH to have authority over the mark. Other holders of 'APA' would then have to file their own registrations to have the same access to related domains as the first.

There is no inherent problem with the duplication of names or even the duplication of trademarks, especially with the expanded TLD space where there is a much larger realm of domains in which names may be established. Assume that there exists two people who identify themselves with the name 'Judith Butler'. One is a gender studies scholar and the other is a chef. Trademarks are not a regular occurrence in academia and therefore the scholar 'Judith Butler' does not have a registered mark, but her chef counterpart who recently opened a self-named restaurant does. The names are the same, but their areas of claim to the name and legal standing, are different. Despite these differences there is space for both names in the expanded namespace, one may have <JudithButler.PhD> and the other may have <JudithButler.Resturant> without interference or detectable harm to either entity.

Harms to Non-Corporate Entities

Trademark registrations in the United States are not free and often require a lot of research, legal experience and other resources to perform. In addition, trademarks are primarily created for the purpose of protecting intellectual property rights related to activities involving commerce. The Lanham Act, the primary trademark legislation in the United States, is designed to protect against unfair competition in commerce. Further, trademarks are expected to gain "distinctiveness" through commercial activities (Joseph, 2012). Trademarks are therefore not appropriate for use by other formal or informal entities that are not conducting commerce on behalf of the mark.

Returning to my example of the scholar, lets consider the legal status of a doctoral candidate who has not yet established themselves as a well-known scholar in their field and perhaps does not have commercial ambitions for their degree. The emerging scholar would have no need for a registered trademark and even if a trademark were registered there would be no recognized commercial use to satisfy the requirement to demonstrate a history of use in defending the trademark.

The use of trademark as the cornerstone of all dispute-resolution and intellectual property protection guidance for the domain name system disadvantages entire classifications of Internet uses and content creators. Postel's (1994) statement of policies[6] for domain names establishes an expectation of fairness and equal access to domain registrations while also reiterating that

[6] In RFC 1591 Postel is writing in his capacity as the appointed Internet Assigned Numbers Authority (IANA), rather than as an individual engineer.

commercial entities (those who were expected to register in COM) were only one of several groups of Internet users. The number and types of users have changed significantly since Postel's original document and even since the beginning of formal intellectual property protection on the Internet. Individuals not involved in commercial activities, groups (formal or informal) that do not hold trademarks and small businesses are held to the same requirement as trademark holding corporations to protect their domain names from entities with more resources. Further, if one of the non-trademark holding entities were the victim of cybersquatting there would be no basis for reclaiming a domain name registered in bad faith. There is a denial of rights to non-trademark holders on both the complainant and respondent sides of the UDRP.

This is the area where the discrepancy between the two Judith Butlers becomes more concrete. If someone had registered <JudithButler.PhD> prior to the scholarly Butler deciding to register it, then scholarly Butler would have no standing for recourse under UDRP if the registrant attempted to extract a large sum of money from the scholarly Butler in exchange for the domain name. If the same situation were to arise for chef Butler, who does hold a trademark, the requirements for a UDRP complaint would be met and chef Butler could utilize that method to gain control of the ransomed domain. From the perspective of each of the Butlers as a respondent to a UDRP claim there is a similar discrepancy. Because chef Butler holds the Judith Butler trademark, the UDRP process would not move beyond verification of the trademark, whereas scholar Butler would be required to demonstrate that there was no bad faith or intention of deception in registering the domain name.

UDRP does not replace or supersede the ability to pursue legal resolutions to a domain dispute and in the United States a UDRP decision can be challenged in federal court. Legal challenges are granted the full range of rights as specified in the Lanham Act, but is a costlier

option than a UDRP arbitration (Internet Corporation for Assigned Names and Numbers, 2012). While individuals have more protections under that option, it is not viable for most due to its cost and the amount of required legal knowledge to begin such a process.

Disputes are not the only area where non-trademark holders are harmed. As noted previously, each new TLD launches with a sunrise period. During the sunrise period only trademark holders are permitted to register. While in concept this is a proactive protection of intellectual property rights, it is also an additional constraint for other entities that may also have a valid claim to the domain. The previously mentioned lack of trademark category specificity and absence of an alternative method for asserting rights to a mark complicate this particular protection. Chef Butler could register her trademark with TMCH to gain access to sunrise registrations. This would enable chef Butler to prevent others from registering her trademark in any TLDs if she wished, so if she were to decide to register <JudithButler.PhD> prior to the PHD TLD becoming generally available, she could. This would of course prevent scholar Butler from registering that domain. Without the sunrise period both Butlers would have equal opportunity to register <JudithButler.PhD>. I am not arguing for the elimination of the sunrise period entirely, as it does serve a purpose to permit established identities to register their domain ahead of the general availability period in competition with others. Instead I propose that some sort of applicability criteria be applied to sunrise registrations to prevent the abuse of the process toward unfair monopolization of the trademark phrase. As with the UDRP problems, limiting eligibility to trademark holders unfairly disadvantages non-trademark holders who otherwise have a demonstrable claim to a name.

The functional difference between the two Butlers can be reduced to one has a commercial interest and therefore has a method of protecting and utilizing her identity in the

domain name system, whereas the other operates in an industry and profession that is not centered on the conducting of commerce or commodification of identity, therefore is not granted any protections or guaranteed utilization of identity.

Equal access to domain names matters because it is equal access to a stable identity in the online environment. Present rules permit trademark holders to not only defend their mark online, but also ensure a degree of stability in the assumption that domain names have the same permeance as real property and remain assigned to the registrant unless the registrant decides to either give up or reassign the domain. Domains that are not held by trademark holders are subject to challenge and can be forcibly transferred or deleted if it is determined that they are in conflict with a trademark claim. The artificial limiting of what domain can be selected and the ability to defend a domain based on trademark registration status is an unfair privileging of commercial entities over others. This bias grew out of the historical makeup of the Internet and does not reflect the current composition of Internet content creators.

Free Speech Objection

A related objection to the current ICANN policies on the defense of trademarks in domain names is that of the interference of intellectual property protections on free speech. Excessive control of domain name registrations, including blanket ability for trademark holders to defensively register (ahead of general availability) or block any domain name containing their registered mark or similar mark, prohibits the legitimate exercise of free speech on the Internet.

This is another situation in which the expansion of the number of top-level domains prevents existing policy from working as intended and instead unnecessarily restricts utilization

of domains. In this case however, the concern is not with multiple entities sharing a name or a trademark blocking a registration outside of its trade scope. The free speech objection to excessive trademark protections involves limitations on invoking a trademark for reasons of critique, satire or information. Such a use of domain names inside the new gTLD space was specifically provided for by the Generic Names Supporting Organization in their definition of "freedom of expression", prior to launching the new gTLD process (ICANN Generic Names Supporting Organisation, 2007).

The expectation of free expression being preserved can be seen in ICANN admitting the SUCKS TLD to the root zone. The mission of the TLD, which is described succinctly in the tag line of their registry website "tell us how you really feel", encourages consumers to voice their opinions and complaints in a public forum (Vox Populi Registry Ltd., 2016). The UDRP does not discourage registrations for purposes of critique or parody and therefore most uses of SUCKS would be protected, at least per the written criteria. However, because the top-level domain is not considered in UDRP cases this opportunity for critique could be easily challenged without consideration of the expression limitations imposed.

Due to the diversity of the categories of TLDs there are many possible domain names that suggest legitimate uses of existing trademarks. Take for example an existing website, NikonF6.net, which incorporates two trademarks owned by Nikon Corporation into its name. The website provides detailed information and reviews about a camera produced by Nikon but is clearly not operated by the trademark holder. Such a resource could be located in the new CLUB or INFO TLDs which would place more emphasis on the relationship with the trademark holder, further eliminating concerns of dilution while also providing a resource for interested parties.

The current culture of the Internet is brand-heavy and as such trademarks do flow into the normal discourse and function not only as identity for the trademark holder but also as reference for others. Sometimes the references are positive, as with the Nikon example above, but other times they are negative such as domains established for the purpose of critical review or for uniting frustrated consumers. In either case they are forms of expression and not attempts to confuse or mislead Internet users who access them. Rapid suspensions and blanket blocks of names including trademarks undermine free expression as a value of the Internet and severely limit the opportunities for critique.

Recommendations for Policy Change

The present intellectual property protections are inadequate and are discriminatory in favor of corporate entities, which was not the intention of the founders of the domain name system. Domain registration is to be a public resource available to any entity that has the capacity to operate one, without unnecessary bias. The current policies also permit and encourage rights holders to conduct their own exercise in domain squatting by way of preventing other legitimate claimants of a domain name from registering the name without beginning a potentially expensive legal process.

As an initial change I believe ICANN must take steps to give entities that have a reasonable claim to a domain name, but no trademark, the ability to defend their domain name against trademark holders and other registrants that may have registered a domain in bad faith[7]. This change would entail the establishment of a more thorough evidence collection procedure

[7] A different version of 'bad faith' than is written in the UDRP, where malice must be proven.

than is currently deployed in UDRP arbitration cases. Through allowing past instances of name use in a public medium, such as social media, to stand as evidence of a claim to the name the burden on individuals and small organizations will be reduced, allowing them a more reasonable way to demonstrate that they have a claim to the challenged domain.

The objective of the dispute process and any protection must be to protect from intentional infringement of a name in a malicious way, such as to extort money or to block a domain name for the purpose of preventing someone else from registering it.

Second, ICANN should re-evaluate the way that trademark protections are deployed. The present practice of allowing any trademark holder who is registered with the TMCH to block registrations of domains or have early access to domains in freshly launched gTLDs creates a de facto trademark with universal effect. The top-level domains are more robust than a simple matching of a trademark to an industry, therefore special considerations should be made for gTLDs that do not fit the normal category or industry focused model. For example, a trademark holder whose sole place of business is in California should not be permitted to exercise their trademark to register their brand in the NYC gTLD. I do not advocate for preventing them from registering in non-related gTLDs, but they should also not be afforded the normal protections.

Finally, a class of gTLD should be established that is exempt from the traditional trademark protections, for use by individuals and small groups. The existing NAME gTLD, which is designated for personal name registrations, could be the first member of this class. There are many nuances to the way this type of classification would be implemented and to avoid complications would require that the individual registries consent to joining the classification. While I would be supportive of a defense mechanism based on legal name, this should not be a requirement or an entitlement to block a name. Other scholars, such as danah

boyd (2012), have discussed the power and privacy politics of "real names" online in great detail and as such I will not revisit that topic here.

The most fundamental mistake made by ICANN in the creation of new TLDs was treating all new gTLDs as being the same as the original three. The new gTLDs span different types of scopes and serve different functions linguistically. Each registry that applied to create a new TLD had a different vision for how the domain would function and serve the Internet. Ignoring the distinctiveness of each TLD disregarded the range of possibilities for how the new gTLD program could have met the objectives of creating a more diverse namespace while also respecting intellectual property rights. Each TLD is different and different rules make sense. There is precedent in the country code TLD (ccTLD) namespace for not treating all TLDs the same and respecting individual local policies. A similar approach could have been taken with gTLDs that align to specific industries or subsets of users. For example, the dot-PHD TLD could have utilized documentation reflecting the earning of a doctoral degree as a verification of eligibility to participate in sunrise registration or for extending the protections of UDRP in a way consistent with social expectations of the TLD. Similar points were raises regarding the dot-HEALTH TLD based upon its position as a potentially dangerous TLD based on the perceived authority granted to domains under the TLD (Vezzani, 2014). Policies must evolve to match both the technological and social realities of the domain name system to afford all Internet content creators and users equal protection, or at a minimum protections that are fair and reasonable in the context of the specific TLD.

Conclusion

Since the 1990s the domain name system has presented a challenge for intellectual property rights holders. Cyber squatting is a legitimate concern of the Internet, not only for intellectual property rights holders, but other entities as well. The Uniform Domain-Name Dispute Resolution Policy (UDRP) was a conceptually necessary protection in an era of limited numbers of top-level domain names where carving out an identity in an emerging space was a challenge. After the first few new gTLDs were delegated to their registries and became operational the UDRP became obsolete due to its failure to recognize differentiation between industries. Further, new protections created specifically for the new gTLD process also fail to account for the industry-specific nature of trademarks.

The new gTLD program was supposed to create more options for domain names as well as inspire more consumer choice and competition between registries. While there are technically more options for domain names, some of the implications of a more open naming structure, such as being more hospitable to non-traditional (non-corporate) registrants have not been met. The overall addition of new gTLDs could probably be viewed as a success as there are new content providers being established [cite… and put paragraph in main paper], there is still a long way to go toward creating an environment that is nurturing to new ideas and new types of content creator and where those creators have some protections from ICANN to assure that their domain will not be claimed by another entity that can demonstrate they have a superior claim.

The challenges presented by the absence of industry boundaries to rights protections are a minor part of a greater problem with domain name protections. Trademark owners are privileged above all other entities in the domain name lifecycle. Individuals are not permitted to protect their own names from malicious registration, nor are there any affordances for allowing a private

citizen that has not registered their name as a trademark to challenge a registration. Due to requirements of using a mark in commercial use for it to be recognized, an entity who registers a trademark after a domain has already been established could then take the domain from the original owner if the name was not used in commercially recognized activities.

Elevating non-trademark holding entities to the same status as their rights-holding counterparts will require revision of ICANN's policies and a new architecture for validating claims to domain names. The preservation of the Internet as an open and democratic space will require the common blogger to have the same access to register and defend a domain name as a multi-national corporation.

Alramahi, M. (2008). New gTLDs – Pandora's Box is open. *International Review of Law, Computers & Technology*, 183-192.

boyd, d. (2012). The Politics of "Real Names". *Viewpoints*.

Brown, N. A. (2012). Six Degrees of Disputation: New DRPs for new gTLDs on the Internet. *Dispute Resolution Journal*.

Donuts Inc. (2018). *Enhanced Brand Protection*. Retrieved from donuts inc.: https://donuts.domains/what-we-do/brand-protection

Goodnight, G. T., & Green, S. (2010). Rhetoric, Risk, and Markets: The Dot-Com Bubble. *Quarterly Journal of Speech*, 1479-5779.

ICANN Generic Names Supporting Organisation. (2007, August 08). *Final Report - Introduction of New Generic Top-Level Domains.* Retrieved from ICANN Generic Names Supporting Organisation: https://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm

Internet Corporation for Assigned Names and Numbers. (2012, February 25). *Dispute Resolution Options.* Retrieved from Internet Corporation for Assigned Names and Numbers: https://www.icann.org/resources/pages/dispute-resolution-2012-02-25-en

Internet Corporation for Assigned Names and Numbers. (2012, February 25). *Uniform Domain Name Dispute-Resolution Polcy.* Retrieved from Internet Corporation for Assigned Names and Numbers: https://www.icann.org/resources/pages/policy-2012-02-25-en

Internet Corporation for Assigned Names and Numbers. (2013). *2013 Registrar Acreditation Agreement*. Retrieved from Internet Corporation for Assigned Names and Numbers: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

Internet Corporation for Assigned Names and Numbers. (2015, September 11). *The Revised Report: Rights Protection Mechanisms Review.* Retrieved from New Generic Top-Level Domains: https://newgtlds.icann.org/en/reviews/rpm/rpm-review-11sep15-en.pdf

Internet Corporation for Assigned Names and Numbers. (2015). *Trademark Clearinghouse.* Retrieved from New Generic Top Level Domains: https://newgtlds.icann.org/en/about/trademark-clearinghouse

Internet Corporation for Assigned Names and Numbers. (2015). *Uniform Rapid Suspension System.* Retrieved from New Generic Top-Level Domains: https://newgtlds.icann.org/en/applicants/urs

Internet Corporation for Assigned Names and Numbers. (2018). *Delegated Status.* Retrieved from New Generic Top-Level Domains: https://newgtlds.icann.org/en/program-status/delegated-strings

Internet Corportation for Assigned Names and Numbers. (2010, October). *Summary of the Impact of Root Zone Scaling.* Retrieved from ICANN Archives: https://archive.icann.org/en/topics/new-gtlds/summary-of-impact-root-zone-scaling-06oct10-en.pdf

Joseph, A. M. (2012). I Cann't Believe It's Not Better: Why New gTLDs are Bad for Brand Owners and Trademark Law. *Journal of Intellectual Property Law*.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). *A Brief History of the Internet.* Retrieved from Internet Society: https://www.internetsociety.org/internet/history-internet/brief-history-internet/

Postel, J. B. (1994, March). *Domain Name System Structure and Delegation.* Retrieved from Internet Request for Comments Series: https://tools.ietf.org/rfc/rfc1591.txt

Postel, J. B., & Reynolds, J. K. (1984, October). *Domain Requirements.* Retrieved from Internet Request for Comments Series: https://tools.ietf.org/rfc/rfc920.txt

Sharrock, L. M. (2001). The Future of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions from within the UDRP Framework. *Duke Law Review*.

Stein, M., & Horowitz, M. (2015). Generic Top-Level Domain Expansion Brings New Opportunities, Risks for Business Owners. *Florida Bar Journal*, 85-89.

Trademark Clearinghouse. (2018). *Trademark Claims Services*. Retrieved from Trademark Clearinghouse: http://www.trademark-clearinghouse.com/content/trademark-claims-services

United States Patent and Trademark Office. (n.d.). *Trademark Search*. Retrieved from United States Patent and Trademark Office: http://tmsearch.uspto.gov

Vezzani, S. (2014). ICANN's New Generic Top-Level Domain Names Dispite Resolution Procedure Viewed Against the Protection of the Public Interest of the Internet Community: Litigation Regarding Health-Related Strings. *The Law and Practice of International Courts and Tribunals*, 306-346.

Vox Populi Registry Ltd. (2016). *dotSucks Domain Names*. Retrieved from https://www.registry.sucks/

Weston, M. (2000). Domain Names: Disputes and Resolutions. *Computer Law & Security Report*, 223-231.

Wright, S. (2012). Cybersquatting at the Intersection of Internet Domain Names and Trademark Law. *IEEE Communications Surveys & Tutorials*, 193-206.