Brand Protection on the Internet: Domain Names, Social Media, and Beyond

By Brian J. Winterfeldt* and Diana Moltrup, with contributions from: Tish L. Berard, Larissa Best, Christopher Casavale, Tammi Collie, Michele Huntzinger, Karen Holme, Philip Karnofsky, Diane Lau, Phillip Marano, Alessandro Masetti, Emily Murray, Christopher M. Ott, Daniela Rojas, Elaine Steelman, Sabrina Sturion, Griffin Barnett, David Rome

I. Introduction

As the Internet has become an increasingly important business tool for brand promotion, the growth of the Internet has presented new challenges to brand owners concerning trademark infringement, policing, and brand enforcement. While in the past trademark owners policed primarily the brick-and-mortar world for unauthorized uses of their marks, since the mid-1990s they have also had to address increasing levels of infringement across the Internet.

This chapter provides an overview of the basics of the Internet, a survey of the various Internet platforms that support online content, and practical techniques for trademark administrators or paralegals (“Administrators”) who are responsible for prioritizing and managing various online matters and enforcement actions.

* Head of Winterfeldt IP Group, Washington, D.C.
II. The Domain Name System

A. Origins of the Internet

The Internet was not always a commercial enterprise. What started as a network system for university and government researchers to share information has evolved into the commercial enterprise and global social network that is today’s Internet. In 1968, the Advanced Research Projects Agency of the U.S. Department of Defense (DOD) requested quotations for a networking technique that would enable researchers in labs around the country to share files and send information to one another from remote locations. From this networking technology emerged the Advanced Research Projects Agency Network (ARPANET).

Eventually, ARPANET split into two separate elements: a military DOD network and a public, secondary entity funded by a civilian network agency, the National Science Foundation (NSF). The NSF’s standards required, however, that use of the network be limited to research and education. When funding of the network by the NSF eventually expired and its limitations on commercial use no longer applied, the Internet continued expanding, and so did ideas regarding its commercial potential. Demand for a presence on the Internet surged, and by the end of February 2017 approximately 329 million domain names had been registered globally.

B. Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit partnership of stakeholders from all over the world dedicated to developing policies to keep the Internet domain name system secure, stable, and interoperable, as well as to promote competition among domain name registration authorities.

The domain name system essentially works as a mnemonic device that translates the numerical addresses used by computers on the Internet to find one another.
into words and phrases that are capable of being easily remembered by users. ICANN’s primary role is to ensure that users receive the same predictable results navigating the Internet no matter where they are in the world. To achieve this end, ICANN develops policies through the “multi-stakeholder model,” bringing together diverse stakeholders from business, government, civil society, and academia, among other backgrounds, to reach consensus positions on particular issues related to domain names and numerical addresses.

C. Internet Domain Name System

The Internet Domain Name System (DNS) is the Internet’s hierarchical address system that helps users find targeted webpages. The DNS functions like a telephone directory for the Internet; a domain name is the user-friendly form of a webpage’s “phone number,” which is called the Internet Protocol (IP) address. The benefit of the DNS is that users are able to refer to and access websites using domain names (such as icann.org) rather than the all-numeric IP addresses (e.g., “192.0.32.7” for icann.org) assigned to each computer on the Internet. Also, much like a phone number, a domain name contains both shared and unique elements. The DNS forms a treelike hierarchy, where each top-level domain includes many second-level domains, each second-level domain can include a number of third-level domains, and so on. These various elements within a domain name are called labels; they are organized into different levels segmented by a “.”—called a “dot” in a domain name. A domain name that includes top-level, second-level, and third-level domains is shown below. (Note that the abbreviation “www” in a domain name refers to the World Wide Web, a system of linking documents accessed via the Internet.)

![Diagram of domain name hierarchy]

1. Top-Level Domains

The very end portion of a domain name—for example, .com, .org, or .biz—is the top-level domain (TLD). The TLD is like the area code in a phone number, which is common to all phone numbers in that region. TLDs composed of three or more letters are generic top-level domains (gTLDs). TLDs composed of two letters (e.g., .de, .mx, and .jp) represent a certain country or external territory; they are known as country-code top-level domains (ccTLDs). (See Section I.C.3, below.) Until late 2012, there were 22 operating gTLDs in existence and more than 250 ccTLDs, including many in non-Latin scripts. Starting in late 2013, however, several hundred new gTLDs were added to the DNS, resulting (by September 2017) in over 1,200 delegated new gTLDs on the Internet.

2. ICANN's New Generic Top-Level Domain Program

In 2012, ICANN invited organizations that could meet certain technical, operational, and financial requirements to apply to operate their own customized gTLD extensions. ICANN received 1,930 new gTLD applications (often referred to as strings) for generic words, such as “music,” “art,” and “home,” but trademark owners also applied for gTLDs containing their trademarks. For example, Honda applied for .honda, Google applied for .google, and Travelers Insurance applied for .travelers. The application landscape also included a number of geographic terms (e.g., .berlin for Berlin, .wien for Vienna, and .bcn for Barcelona) and more than 100 applications for strings in non-Latin scripts, called Internationalized Domain Names (IDNs) (e.g., .商店 which is Chinese for “store,” .برع which is Arabic for “Arab,” and .クラウド which is Japanese for “cloud”).

A number of new rights protection mechanisms were introduced for gTLDs delegated after 2012: the Trademark Clearinghouse (TMCH) (which incorporates trademark claims and sunrise services), the Uniform Rapid Suspension System (URS), and the Trademark Post-Delegation Dispute Resolution Procedure (PDDRP).
a. Trademark Clearinghouse

The TMCH is a centralized database of verified data of registered trademarks. It is intended to minimize the burden on bona fide trademark owners by allowing them to deposit, for a fee, their trademark data in one centralized repository, rather than individually with each new gTLD registry. New gTLD registries will then be able to retrieve such centralized data from the TMCH to validate sunrise registrations and issue trademark claims notices.

- **Sunrise Registrations:** Whenever a new gTLD opens, brand owners that have met certain requirements have a limited period of time, called a “sunrise period,” in which to register their marks as domain names prior to the general availability of domain name registrations in the TLD. All non-brand new gTLD registries are required to offer a sunrise period of a minimum of 30 days wherein eligible trademark owners will have a limited opportunity to defensively register second-level domain names matching their marks recorded in the TMCH. To be eligible for sunrise registrations, such marks must have been submitted along with proof of use.

- **Trademark Claims Service:** The Trademark Claims Service will notify potential domain name registrants that the domain names they are attempting to register may infringe a brand owner’s trademark rights—provided the domain names are an identical match to an entry in the TMCH. Should a registrant receive a trademark claims notice and proceed to registration anyway, the brand owner will receive notice of the registration. The duration of the trademark claims period for each new gTLD is 90 days upon launch of general availability of domain name registration in the TLD (immediately after the sunrise period; see above). After 90 days, no notifications will be made to potential domain name registrants or to brand owners unless the registry has voluntarily extended the trademark claims period or the brand owner has opted in to the TMCH’s “ongoing notification” service, which provides ongoing notices of registered names for the duration of the brand owner’s TMCH-validated record. (Note that this
service does not provide registrant-side pre-registration notices, only post-registration notices of registered names to the brand owner.)

For more information, visit the **Trademark Clearinghouse website**.

**b. Uniform Rapid Suspension System**

The URS is designed to offer faster and cheaper resolutions than the Uniform Domain-Name Dispute-Resolution Policy (UDRP) (see Section IV.A.2.c, below) to address “the most clear-cut cases of infringement” in the domain name system. However, there is a much higher standard of proof, and the only remedy under the URS is suspension of a domain name for a limited period of time.

For more information, see ICANN, “**Uniform Rapid Suspension System (URS)**.”

**c. Trademark Post-Delegation Dispute Resolution Procedure**

The PDDRP is supposed to provide brand owners with a means for redress against new gTLD registries’ acting in bad faith with the intent to profit from systematic cybersquatting in their TLD(s). However, the PDDRP is narrowly limited to instances where a registry has exhibited a pattern or practice of “actively and systematically encouraging registrants to register ... domain names [that] take unfair advantage of the trademark to the extent and degree that bad faith is apparent” or of “acting as the registrant or beneficial user of infringing registrations, to monetize and profit in bad faith.” This is a high burden to satisfy, and unsurprisingly, no PDDRP complaints have been filed as of September 2017.

**Practice Tip**

Enforcement in ccTLD spaces may be challenging for brand owners because of the variety of dispute resolution processes and the linguistic issues that arise; the assistance of local counsel may be required. Administrators whose responsibilities encompass management of international domain name matters in ccTLDs would be wise to develop a network of counsel in the relevant jurisdictions who can advise on and assist with these matters efficiently. (See **INTA Membership Directory**.) Given that there is no single rating guide that one can rely upon in hiring trademark counsel abroad, it is useful to obtain word-of-mouth information from other counsel with experience in countries of interest to determine which counsel might be best for a particular situation.
For more information, see ICANN, “About Trademark Post-Delegation Dispute Resolution Procedure (Trademark PDDRP).” On this process and the new gTLD program in general, see INTA, Policy and Advocacy, “New Generic Top Level Domains (gTLDs);” ICANN, “New Generic Top-Level Domains” microsite.

3. **Country-Code Top-Level Domains**

Country-code top-level domains have been established for more than 250 countries and external territories. They are delegated to designated individual country managers, whose country or territory is assigned a unique two-letter code from the International Standards Organization’s table (ISO-3166-1); the managers operate the ccTLDs according to local policies that are adapted to best meet the economic, cultural, linguistic, and legal circumstances of the country or territory involved. (For more details, see ICANN, Internet Assigned Numbers Authority (IANA), “Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation).”)

ICANN develops policies related to gTLDs, but policies regarding registration of domain names and dispute resolution in ccTLDs will vary according to the individual ccTLD sponsoring organization, which may be a local government or commercial group. For example, certain ccTLDs may restrict registration of domain names to entities with a documented local presence. Most ccTLDs have designated country-code managers (see above) to administer registration of their domain names.

As explained above, a ccTLD represents a certain country or territory. IDNs have historically been a subset of ccTLDs, representing country or territory names in non-Latin scripts, such as Arabic or Thai, to reflect local languages. However, the new gTLD program has facilitated the creation of IDNs outside of ccTLDs, including IDNs for other geographic terms, generic terms, and even IDN .Brand TLDs.
III. Establishing an Internet Presence

A. Websites

Most corporations begin their online presence by establishing a website that highlights the corporation and its products and/or services. This content is located on a second-level domain name that is purchased through one of the commercial service providers that facilitate the buying and selling of domain names. These providers are called registrars, and their customers—the entities (or companies) purchasing the domain name—are called registrants. There are thousands of registrars—for example, Network Solutions, GoDaddy, and MarkMonitor—that offer domain names for sale. The price for purchase of a domain name varies among the various providers; there may be certain registration requirements or criteria that a registrant must satisfy for some TLDs. Some registrars offer special pricing for longer registration periods or when a domain name is purchased along with other services, such as Web hosting. Web hosting services allow individuals and organizations to make their websites accessible through the World Wide Web by selling or renting space on a server, and also provide Internet connectivity to their websites.

1. Domain Name Portfolio Management: Benefits of a Domain Name Policy/Procedure

The protection and maintenance of domain names is a very different practice from the searching and clearance of trademarks. Trademark searching and clearance is very much controlled by members of the legal department or outside counsel, with launches of new product or service names or other branding elements being carefully coordinated among legal, marketing, and business teams. The situation is different with domain names. Any individual, regardless of his or her role in or outside the organization, can simply visit a registrar’s website and register any available domain name for a small fee, without any legal clearance required by the registrar. This type of action, usually by well-meaning employees, may be a common occurrence for organizations that do not have domain name registration policies in place. Problems can occur, for example, if an employee obtains a domain name registration in his or her own name—though
the domain name is related to the employer’s business—and then either refuses to transfer the domain name registration to the employer or simply leaves the organization without transferring the ownership of the domain name. Companies may also encounter difficulties with vendors, licensees, and other business affiliates registering domains without permission. Resolving these issues can be challenging and expensive. Thus, it is important to set expectations and to publicize the dangers of employees and other business affiliates taking these kinds of actions.

As a best practice, companies should develop written policies and/or procedures that outline how domain names should be purchased, maintained, and protected from infringement and abuse. For some companies, these various functions can reside within various business units, such as information technology, marketing, security/compliance, or legal. Elsewhere, the company may decide to form a cross-functional domain name management team composed of representatives of its business units, whose primary responsibility is to create, manage, and protect the company’s domain names. Often the Administrator is the legal department’s representative on such a team.

Because domain names are critical to the effective promotion and protection of a company’s brands online, the protection of key domain names can be as important as protection of a company’s trademarks. A decentralized or uncoordinated approach can lead to problems, such as (1) domains that expire and are dropped or “lost” to a third party; (2) registering too many or too few domain names; (3) paying too much to register domain names through the failure to explore preferential pricing based on volume; and (4) inconvenient and costly legal action to recover key domain names to support the business. It is a must for legal teams to assist the various business units in developing a coordinated approach to performing the various domain name activities.

A good domain name registration policy will aim to ensure that domain names are registered, monitored, and managed in an orderly, controlled, and accountable fashion for the benefit of the company, so that the company’s brands are properly promoted and protected, while driving additional online traffic to the company’s websites and improving customer experiences. The domain name
registration policy can easily be incorporated into and integrated with existing brand policing and enforcement policies.

The checklist below highlights key issues and concerns that should be taken into account when formulating a domain name registration policy.

<table>
<thead>
<tr>
<th><strong>Checklist: Domain Name Registration Policy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Purpose.</strong> Why is it important to have a policy/procedure about domain name registration?</td>
</tr>
<tr>
<td>2. <strong>Scope.</strong> To whom does the policy apply? (Certain business units, vendors, licensees, advertising and marketing agencies, and other key business partners, as well as locations and jurisdictions)</td>
</tr>
<tr>
<td>3. <strong>Key Brands/Terms.</strong> What trademarks (or terms) are core to the company’s strategy, and how are existing and new trademarks incorporated into the domain name registration strategy?</td>
</tr>
<tr>
<td>4. <strong>Key Registries.</strong> What are the most critical extensions (gTLDs and ccTLDs) to the company for registering domain names? How are registrations handled in new registries? Will the organization participate in sunrise programs, which may allow trademark holders the opportunity to reserve desired domain names before a registry opens for registrations by the general public?</td>
</tr>
<tr>
<td>5. <strong>Registration Request Process.</strong> What forms or processes are used to request a new domain name? What standard information should be included in routine registrations? Such information may include, for example, specific contact details to ensure consistency throughout the domain name portfolio, and whether the organization will use privacy or proxy services (which mask the identity of the registrant to the public).</td>
</tr>
</tbody>
</table>
### Checklist: Domain Name Registration Policy

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 6. | **Roles/Responsibilities**  
  - **Registration**: What teams/employees have the authority to purchase, renew, and acquire domain names? To avoid confusion, the policy should explicitly state that other employees do not have this authority.  
  - **Enforcement Strategy**: How are decisions made regarding online enforcement? How are domain names acquired via enforcement action incorporated within the portfolio?  
  - **Traffic Statistics**: What team is responsible for receiving and reviewing website traffic statistics? (These statistics could be helpful in determining renewal periods and search engine optimization efforts.)  
  - **Enforcement/Monitoring**: What teams are responsible for monitoring new third-party domain registrations to identify problematic domain names?  |
| 7. | **Effective Date**: When does the policy take effect? How should requests be handled during the transition period?  |
| 8. | **Resources/Appendix**: Include sample request forms, FAQs, contact numbers, and other resources.  |

### 2. Proactive Steps to Minimize the Impact of Domain Name Infringement

Traditional trademark infringement involves the use of a trademark in a manner that causes a likelihood of confusion with a different trademark owned by another party, usually in relation to identical or similar products or services. Domain name infringement, however, involves protecting a trademark outside the obvious context of its consumer market, because domain names are global and not necessarily limited by or tied to specific goods or services. Trademark owners can enforce their rights against domain names that are sufficiently similar or identical to their existing trademarks where those domain names create a likelihood of confusion, just as they could against infringers in the brick-and-mortar world.
While it is impossible to prevent domain name infringement, Administrators can assist attorneys and business teams in taking several proactive steps to minimize the impact of infringing activities and the abuse of their company’s brands online. These include the following:

- **Register key domain names.** It is impossible for any company to own all possible domain names with all registries that might incorporate its brands. Instead, a company should consider purchasing the exact matches and frequent misspellings of its primary brands within its key registries, especially those that are most commonly used and searched—for example, .com, .net, and .org. Companies that conduct business outside the United States, or that are likely to do so in the future, should consider registering domain names with the appropriate ccTLD, provided the country-specific requirements for such ownership can be met. (Note: It may be helpful to collaborate with experienced intellectual property counsel to obtain names and keywords in key international jurisdictions, as registration requirements may vary among ccTLDs.) The best offense can be defensive registration, especially as the cost of identifying, investigating, and disabling or recovering an infringing domain name can be far greater than the cost of obtaining and maintaining a domain name registration in the first place.

- **Register quickly.** Keeping in mind that domain name registration generally operates on a first-come, first-served basis, companies should register domain names of interest as soon as they learn that a desired domain name or new TLD has become available. In the changing Internet landscape brought about by new gTLDs, it is especially important to monitor when new gTLDs of interest will be launching in order to capitalize on mandatory Sunrise Periods wherein brand owners are granted registration priority in exchange for premium prices.

- **Monitor domain name registrations.** The company should employ a law firm or a reputable monitoring company to monitor the Internet for possible domain name infringement of key brands and
regularly review the results. After proper investigation (see Section IV.A.1, below), the Administrator may recommend timely action for problematic registrations.

- **Renew domain names in a timely fashion.** The Administrator should use a docketing system as a prompt to renew the domain names in a company’s portfolio. For core domain names (such as those supporting the corporate website or an active e-commerce website), the company should consider arranging for automatic renewal or purchasing these domain names for multiyear terms to minimize the burden of monitoring deadlines.

### B. Social Media

In addition to domain names, content appearing on websites can also be a concern for brand owners.

For many years, webpages and websites displayed only static content. A website operator would provide the framework and content for a site, and the Internet was more or less a passive experience, in which users could review the content but did not have an opportunity to interact with it directly. The transition to the modern Internet—described by the term Web 2.0—occurred when the user experience became more interactive and users started contributing to the content. Examples of the products of this transition are weblogs (blogs) and social media sites. The advent of Web 2.0 also signaled a shift in how brand owners would need to view online enforcement strategies. Although Web 2.0 introduced many exciting commercial opportunities for brand owners, it also meant new layers and levels of the Internet landscape for them to monitor and enforce.

The rise of social media websites, such as Facebook, Twitter, YouTube, and numerous other platforms, has added another dimension to the Internet enforcement landscape. Infringement on social media sites may take several forms, including the unauthorized registration of trademarks and brands as social media profile names, unauthorized use of logos or copyrighted content in social media postings, impersonation of company personnel, and more.
One way for companies to limit the impact of trademark infringement on social media platforms is to proactively build and maintain their own social media presence. This may mean, for example, setting up a Facebook page, maintaining a Twitter account, or building a YouTube channel. By offering its own official social media resources, a company can ensure that customers looking for information online not only will be able to find it from a direct source but also will be able to engage directly with the company. Official resources that are updated regularly can be an excellent draw for customers, who will no longer need to resort to third-party sites to obtain information.

While detailed social media policies are recommended for all organizations, they are an absolute must for companies that maintain a social media presence. Given that examples of a company’s use of social media can be sent around the globe in a matter of seconds, it is imperative that a company’s employees engage in the use of social media in a uniform manner. Social media policies may address a variety of topics, including guidelines for all employees (e.g., whether they are authorized to speak on behalf of the company), strategies for engaging with customers who offer feedback (e.g., how to personalize a response), and use of intellectual property (e.g., whether logos can be used in tweets). To protect the integrity of a company’s trademarks, the same branding guidelines that apply to other media should also apply to social media.

Administrators often are called upon to help their organizations and clients develop and maintain their social media resources. Just as Administrators often review marketing and other collateral materials, their job function may now include reviewing company websites and social media content to ensure both that the company’s proprietary rights are protected and that the company’s social media presence does not infringe upon the proprietary rights of others. As new product and service offerings may first be announced through social media, Administrators assist with all facets of reviewing materials before they go live.

When a company is using social media to build and promote its brand, it is important that it take the steps listed below. While not all of them will be an Administrator’s responsibility, the Administrator can be extremely helpful in working with the company to track the status of these items.
<table>
<thead>
<tr>
<th></th>
<th><strong>Checklist: Building Brand Presence Through Social Media</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Understand the demographic.</strong> Determine who the customers are and how they use social media.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Select optimal platforms.</strong> Determine which of the available social media platforms will best enable the company to interact with its target customers.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Follow relevant guidelines.</strong> Research the Terms of Use for the selected platforms. Pay attention to any special considerations that apply when using a platform for commercial/promotional purposes.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Develop terms and conditions and social media policy.</strong> Design guidelines for employees and customers to follow when using the social media resources or when discussing the company on social media. These should include guidelines for using trademarks and other intellectual property.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Develop privacy policy and data protection system.</strong> Determine how the company will protect personal information and other data for the users of its social media resources.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Provide internal and external training regarding resources and policies.</strong> Once the company has developed a social media policy and/or launched social media resources, all affected personnel (employees, licensees, vendors, etc.) should receive training on how to follow and implement that policy.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Ensure resources can be monitored, maintained, and updated regularly.</strong> Ensure that personnel are assigned to monitor the social media resources and to update them on a regular basis, and that the workload is manageable for the overall resources available to devote to social media.</td>
</tr>
</tbody>
</table>
Checklist: Building Brand Presence Through Social Media

8. **Review target demographic and new platforms and technologies regularly; adjust strategy as needed.** New platforms and technologies are constantly emerging, so staying current with these trends is important. Similarly, if the customer base expands or changes (e.g., if the company introduces new product lines that target a different demographic, or expands internationally into markets where different social media platforms are popular), be sure to consider how this may affect the optimal social media presence.

9. **Remain engaged with the user community.** Social media can be an excellent means of receiving constructive feedback from customers, and spending time interacting with them can build loyalty and assist with better targeting of the company’s offerings.

C. **Apps**

“Apps” are software applications that users download to their mobile devices or, less frequently, to laptops or desktops. These programs can retrieve information or perform tasks, such as playing games, finding places, getting the weather, making travel itineraries, making restaurant reservations, keeping in touch with friends (social networking), streaming videos, or taking and editing photographs; the possibilities are virtually endless.

Increasingly, many companies offer apps that provide additional opportunities for engagement with their consumers. For example, apps may offer mobile shopping experiences or allow customers to locate the nearest store and place an order for pickup. As an app may be a mobile user’s primary method of interacting with a brand, it is important that trademarks and other branding elements be used properly and consistently. An Administrator may be responsible for reviewing the content of an app before launch in order to identify and correct any improper uses of trademarks and other intellectual property. Because apps may be updated frequently in order to introduce technical refinements and improve the user experience, such review and clearance may be required on a regular basis to address new content.
IV. Enforcing Your Brand Online

Online infringement can take several forms, and each company should have a plan for detecting, investigating, and taking action against the forms most threatening to its business model and to its key brands. The most common types of online infringement are:

- **Cybersquatting**—bad faith registration and use of unauthorized domain name that incorporate a company’s trademarks or colorable imitations thereof.

- **Content infringement**—infringing or fraudulent use of a company’s trademarks or copyright-protected content on a website (rather than, or in addition to, just in the domain name itself) to create the illusion of an authorized or legitimate company website or some sort of affiliation with the company, or to otherwise divert attention from the company’s authorized website(s).

- **Social media and mobile app infringement**—abuse of a company’s trademarks on social media platforms, or unauthorized use of intellectual property in third-party mobile applications.

- **Hacking/malware/phishing**—unauthorized access to and control of a company’s website, domain name, or IP address to disrupt the website’s operation (hacking), inject harmful code (malware) or to send fraudulent email solicitations (phishing).

These are discussed below.
A. Cybersquatting

Cybersquatting occurs when a third party, without authorization, registers a domain name that incorporates another’s trademark, with the bad faith intent to illicitly benefit or profit from using or holding the domain name. Cybersquatters may register domain names that are exact matches, common misspellings, typos, transliterations, or variations of corporate names and brands, often coinciding with the launch of a company’s new service, product, promotion, or other event. (For example, www.inttel.com is a typo of www.intel.com.) Early trademark abuse on the Internet was perpetrated by cybersquatters who registered domain names incorporating well-known marks or typos of the marks for the purpose of using or reselling the domain name registrations for profit, often to the trademark owner. Although several rights protection mechanisms are now available to brand owners to recover domain names, abusive registrations remain a significant enforcement concern; brand owners may face hundreds or even thousands of potentially infringing domain name registrations.

Because it is easy and inexpensive to register a domain name, domain name infringement is particularly widespread. Infringing use of a trademark in a domain name can be discovered by:

- Using a professional watching service, which will provide notices when domain names containing identical or similar trademarks are registered.
- Performing simple Internet searches using one or more search engines.
- Requesting that customers or employees alert the company to infringing domain names.
- Periodically ordering full searches from a commercial vendor in order to obtain a broad view of the infringement landscape.
- Recording trademark registrations with the Trademark Clearinghouse, which can generate notices of newly registered domain names in new generic Top-Level Domains.

The task of reviewing reported infringing domain names for action often is delegated to Administrators, who are most familiar with a brand owner’s
portfolio of trademarks. As the Administrator is the individual responsible for sorting through perhaps hundreds of domain names, it may help to prioritize the domain names according to categories, for example: (1) domain names resolving to sites selling competitors’ goods and services; (2) domain names resolving to sites offering offensive content, such as pornography, malware, or scam sites; and (3) domain names resolving to pages with links to other commercial sites—that is, parked pages with pay-per-click advertising. A consistent domain name enforcement strategy that categorizes the types of infringement and assigns priorities to each can be very useful in ensuring that domain name enforcement resources are used consistently and efficiently.

The steps listed below outline a suggested strategy for addressing infringing domain names of concern in order to minimize ongoing harm from domain name abuse.

1. **Step One: Investigation**

After a potentially infringing domain name has been identified, a very important next step for the Administrator is collecting detailed evidence of the infringement. Collecting evidence is both imperative and time sensitive. A successful outcome may depend on the evidence the Administrator preserved from the initial investigation.

<table>
<thead>
<tr>
<th>Checklist: Collecting Evidence for an Infringing Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If the domain name resolves to a website, capture dated screen shots or printouts of the website. Consult with your company’s help desk/IT desk, or search online for the best strategies to take screen shots or generate printouts of websites, using the resources of the company’s IT network.</td>
</tr>
<tr>
<td>2. Take notes on the content and behavior of the domain name—for example, does it redirect to a different site? If the domain name does not resolve to a website, document that fact too.</td>
</tr>
</tbody>
</table>
### Checklist: Collecting Evidence for an Infringing Domain Name

3. Check Internet archives (using free services such as the Wayback Machine or subscription services such as DomainTools) for previous snapshots of the website offered at the domain name, to help determine the length of time a website has been active and what type of content has appeared on the site. Each resource used to find earlier versions of websites may provide different information from different dates.

4. Retain and date copies of the record containing information about who owns the domain, called the “Whois” record. Registrars and some third-party vendors offer searchable databases of Whois records. The Whois record for an individual domain name includes the name of the domain name owner and the registrant, as well as the following information:

- Name of the registrar that reserved the domain name for the registrant.
- Date the domain name was first registered (sometimes called the “domain creation date”).
- Current status of the domain name.
- Expiration date of the domain name.
- Contact information for the registrant, as well as any administrative or technical personnel associated with the domain.
- Nameservers, which relay information about the company hosting the domain. The domain host enables a website to occupy space on the Internet and is sometimes the same entity as the registrar.
If the registrant information is masked via privacy or proxy service, registrars or Web hosting companies generally are reluctant to reveal the name of the masked registrant; thus, initially, they usually provide information about their users only pursuant to a court order or when the authorities are investigating criminal or other unlawful activity. In other words, registrars and web hosting companies are not likely simply to divulge information about their clients to brand owners that approach them seeking to enforce their trademark rights. At least that is the status quo until a formal accreditation system for privacy and proxy service providers is put into place through ICANN. However, to the extent that any material is illegal (e.g., child pornography, malware, phishing, or other scams), that content should be immediately reported to the website host and local authorities. In addition, trademark abuse may violate a registrar’s or Web hosting company’s terms of use for registrants. If a review of the terms of use indicates that there may be a violation, arguments can be made to the registrar that the registrant’s identity should be revealed and that the registrant has forfeited the right to continue to have its identity shielded by the privacy/proxy service.

ICANN requires that each registrar for gTLDs such as .com, .net, and .org provide free public access to Whois data for domains it manages, but no registrar is required to provide Whois information for domains managed by other competing registrars. Third-party providers specializing in related domain information services include Whois reporting; they can be a good resource if registrar Whois data are not available. Requirements for Whois data vary among ccTLD registries; if information is not readily available, engaging counsel in the appropriate jurisdiction may be helpful or even necessary.

Whois records generally are plagued with inaccuracies because many registrars do not have consistent verification policies and are not generally held accountable for false information. Registrants generally bear the onus to maintain accurate
registration data for their domain names, and in the event that false or inaccurate data is reported to ICANN, the same registrants must correct any deficiencies or face suspension and deletion of their domain names. In addition, proxy services and privacy laws in some jurisdictions (e.g., the European Union) make it difficult to locate or contact the owner of a domain name. Nevertheless, the fact that the Whois record contains false or hidden information about a registrant serves as useful evidence of bad faith, and therefore it should be preserved.

The frequency with which evidence should be downloaded and saved depends on the circumstances of a particular domain name. Immediately before and shortly after taking any action against an infringing domain name (e.g., sending a cease and desist letter) are good times to check for changes to the website or the Whois record; in addition, periodic monitoring of both the website and the Whois record is advisable.

In general, pay particular attention to preserving evidence that demonstrates any of the following:

- The domain name was registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the trademark owner or to a competitor—for example, the registrant makes an unsolicited offer to sell the domain name to the trademark owner for a fee higher than the registration cost.

- The registrant routinely registers or traffics in domain names that are identical or confusingly similar to a trademark for the purpose of misdirecting Web traffic and misleading users—for example, the registrant owns numerous domain names that contain registered trademarks of third parties and/or has been forced by other trademark owners to surrender infringing domain names. Brand owners can view the entire portfolio of a domain name registrant by ordering a reverse Whois search from various vendors.

- The domain name was registered by a competitor primarily for the purpose of disrupting your business—for example, preventing you from registering the name of a new line of your goods or services.
1. The use of the domain name is an attempt to attract, for commercial gain, Internet users to a website or other online location by creating a likelihood of confusion with a trademark as to the source, sponsorship, affiliation, or endorsement of any feature of the website or online location.

In the event a dispute over a domain name escalates, evidence that the current domain name owner had or has no legitimate interest in the domain name will improve the trademark owner’s prospects in any legal action.

2. Step Two: Enforcement Options

The next step is to determine a course of action. In part the course of action will depend on the desired remedy in each case. The Administrator should work with the client or business team to determine whether the company wants to transfer the domain name to the company’s control or whether disabling the infringing domain name, along with any associated website content or other uses, is a sufficient remedy, and whether the company has suffered damages that it hopes to recover.

The following questions are also helpful to consider when determining the desired outcome and the actions to take to achieve it:

- Would the brand in question be considered strong or weak? How is it currently being used?
- Does the brand owner have broad or narrow protection through its trademark portfolio and use of the trademark?
- Has there been any lapse in use of the mark?

The answers to these are especially important in ccTLD cases, where a valid registration or bona fide use of the trademark may weigh heavily in proceedings to recover a domain name.

2.a. Domain Name Acquisition

One popular enforcement strategy is for the brand owner to try to recover a domain name that someone else has already registered because the domain name
contains a term the brand owner wants to use or the domain name consists of a trademark. However, just because someone has registered a domain name that contains a term or terms that are similar or identical to another party’s trademark does not necessarily mean that the domain name is legally objectionable. Absent evidence of bad faith and/or any likelihood of confusion, and where there are no other indications of infringement, purchasing the domain name may be the only strategic option available as both a practical and a legal matter.

Before reaching out to the registrant directly to purchase a domain name, it is a good idea to research means of resolving the issue effectively without an exorbitant cost. Registrars, law firms, and vendors are good resources for information about available options, including purchasing domain names anonymously, so that the company’s interest in the domain name remains private and the owner of the domain name won’t drive up the sale price. Buying and selling domain names is a business, and any agreement to buy or sell a domain name should be reviewed and considered, as it would be in any other business transaction.

b. Cease and Desist Letters

If investigation results suggest that the registrant is acting in bad faith or in a legally objectionable manner, circumstances may warrant a formal cease and desist letter to the registrant that demands transfer of the infringing domain name or identifies other remedies the sender is seeking. Either in-house or outside counsel should prepare and send this letter directly. The letter should outline the conflict and request a response by a particular date. (For additional information, see INTA, Practitioners’ Checklists, “Cease and Desist Letter for Trademark Infringement, Unfair Competition, or Claim of Dilution.”) The Administrator should keep track of when correspondence is sent and any responses or returned letters received.

Generally, try to avoid paying or offering to pay even nominal sums of money to settle with infringers, because this can encourage future infringing activity by third parties and expose an organization to further extortion attempts. Brands quickly develop a reputation in the domain name industry as either being
litigious through enforcement of their rights, or easy targets that roll over quickly with settlement offers.

Nevertheless, in a handful of cases—especially where the indicia of infringement, though present, are not very compelling—a very small payment to cover demonstrated out-of-pocket expenses relating to transfer of the domain name and registration of a new, non-infringing domain name may be acceptable. However, if a registrant responds to a cease and desist letter with an offer to sell the domain name to the owner, particularly for an amount that exceeds the cost to register a new domain name, this is generally considered evidence of bad faith and should be documented by the Administrator.

When drafting a cease and desist letter, keep in mind that the content of the letter may need to vary depending on the jurisdiction of the trademark owner or domain name registrant. In certain territories outside the United States, for example, cease and desist letters are viewed as extremely hostile and can actually cause bigger problems for the trademark owner than the infringing domain name registration. Thus, it may be helpful to consult with international counsel as to how to proceed when one or more parties are outside the United States, particularly if the domain name at issue is registered in a ccTLD.

c. Uniform Domain-Name Dispute-Resolution Policy

The Uniform Domain Name Dispute Resolution Policy (UDRP) provides for an arbitration proceeding whereby trademark owners can recover or cancel infringing domain name registrations. It is available in connection with all of the gTLDs (including new gTLDs and legacy gTLDs, such as .com, .net, .info, and .org), as well as some ccTLDs (including .me, .tv, and .md). Some ccTLD registries not following the UDRP may nevertheless offer other, similar dispute resolution procedures (e.g., Nominet, the registry for .uk domain names, offers its own Dispute Resolution Service).

The UDRP allows challenges to the registration of abusive gTLD domain names. Generally, it is much faster and less expensive than litigation, but the only remedy is recovery or cancellation of the infringing domain name; no other remedies are available.
Complaints under the UDRP are administered by dispute resolution service providers, including the World Intellectual Property Organization (WIPO) and the National Arbitration Forum (NAF). Filing fees as of 2017 for a complaint regarding a single domain name considered by a single arbitrator range from $1,300 to $1,500. An Administrator’s responsibilities in connection with a UDRP proceeding may include gathering evidence of infringement (including copies of the infringing website and Whois record); compiling information regarding an organization’s or client’s trademark rights, such as copies of trademark registrations; communicating with the dispute resolution provider during the proceeding; and coordinating transfer of the domain name following a favorable decision.

For additional information, see INTA, Fact Sheet, “The UDRP: Alternative Dispute Resolution for Domain Name Disputes.”

d. Uniform Rapid Suspension System

For instances where a company does not wish to recover a domain name, but needs to quickly prevent it from being abused, arbitration using the Uniform Rapid Suspension System (URS) can provide a faster and less expensive alternative to the UDRP.

The URS is only intended to address clear-cut cases of infringement and requires a complainant to prove its case by clear and convincing evidence in five hundred words or fewer. Remedies are even more limited than the UDRP and are limited to suspension of the offending domain name. A suspended domain will once again be available to the public, including the original registrant, once the term of the registration expires and the domain name is deleted. Complainants can also opt to extend the term of suspension for another year following expiration.

The URS is only available with regard to domain names in new gTLDs and a few sponsored TLDs, but does not currently apply to the major legacy gTLDs such as .com and .net. As a result of these shortcomings, the URS is a far less attractive mechanism compared to the UDRP in all but a handful of scenarios, such as phishing and malware.
e. Litigation

Litigation is a strategic option that should be considered when other avenues have been exhausted or if the domain name at issue is not eligible for dispute resolution under the UDRP or an equivalent. Litigation may become necessary for effective relief if (1) significant damages have been caused by the infringement; (2) transfer, suspension, or cancellation of the domain name is an inadequate remedy; and (3) the infringer, despite having sufficient resources, is unwilling to pay an adequate settlement sum. Generally, litigation is much more expensive and time-consuming than other options, and a cost-benefit analysis should be performed before it is initiated. However, because litigation may ultimately be a possibility in any domain name dispute, keeping detailed records of the investigation (see Section IV.A.1, above) and preserving any evidence of infringement are essential practices for the Administrator.

For additional information, see INTA, Presentation, “Use of Trademarks in Domain Names & Domain Name Disputes.” The presentation reviews domain name basics and domain name dispute resolution through the UDRP and the Anticybersquatting Consumer Protection Act of 1999 (ACPA).

**Enforcement Options—Administrator Action**

If a client company is seeking to register a domain name that is valuable to its business and the Administrator learns that the domain name has already been registered by a third party but is not necessarily infringing, several strategies should be considered:

- **Making an anonymous offer to the registrant to buy the domain name** (through a law firm, an investigator, or another third party that can protect the client’s privacy). Concealing the company’s identity could improve the likelihood that the registrant will agree to sell for a reasonable amount. In sum, in order to avoid price gouging, any offer should be made through appropriate subterfuge, rather than directly by the brand owner, or other readily recognizable parties, such as corporate domain name registrars or consultants.
**Enforcement Options—Administrator Action**

- **Placing a backorder to purchase the domain name**, whereby the client can get in line to offer to purchase it. Backorder is a service that attempts to register an expired domain name on the client’s behalf before another party is able to rush in and register it. Not all expired domain names can be backordered, however, as the registrant might renew them before they are deleted by the registrar or they might be on “hold” status pending a trademark dispute. Typically, backordering services charge a fee when the backorder is successful and these fees tend to be relatively small. A backorder may be an option if the client would like to acquire the domain name at the next opportunity but it is not essential that it be acquired immediately.

- **Sending a cease and desist letter** (“demand letter”). Assuming that there is legal justification to do so, sending a cease and desist letter is a common, simple, and cost-effective method of acquiring a domain name. Many infringers, on receiving a cease and desist letter, will quickly agree to transfer the domain name at issue.

- **Filing an administrative complaint when there is evidence of bad faith by the registrant**. A procedure governed by the UDRP allows for the filing of an administrative complaint to request that a domain name be transferred. This procedure is available in many instances of cybersquatting and, depending on the client company’s goals, can be more cost-effective than litigation. The most popular service providers for this procedure are WIPO and the NAF. *(Note: Some ccTLDs have their own administrative procedures, which are similar to the UDRP. In such cases, working with international counsel to manage the proceeding is recommended.)* In clear-cut cases of infringement, where time is of the essence and the client company’s priority is not to recover the domain name, an expedited procedure under the URS can result in suspension of the infringing domain name.
Enforcement Options—Administrator Action

- **Filing a lawsuit.** In some instances, the facts might warrant proceeding with litigation. For example, a California court preliminarily enjoined a company from registering any domain names confusingly similar to Verizon’s trademarks, after the court reviewed the defendant’s domain name tasting, kiting, and other cybersquatting activities. *Verizon California Inc. v. Ultra RPM, Inc.*, No. 2:07-cv-02587-PA-CW (C.D. Cal. Sept. 10, 2007). It should also be noted that, under certain laws, significant monetary damages may be awarded. For instance, under the ACPA, a company could be entitled not only to transfer of the domain names at issue but also to treble damages, attorney’s fees, and statutory damages of up to $100,000 per domain name. 15 U.S.C. § 1125(d).

The following checklist may be useful in keeping track of tasks associated with the investigation and management of a domain name enforcement matter.
## Checklist: Domain Name Enforcement Matter

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
<th>✔</th>
<th>Initials</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the matter is docketed or otherwise tracked in an enforcement chart</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search, print and file potentially infringing website content</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search, print and file hidden text and metatag content (may require the use of tools available through investigators or watching service vendors)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search, print and file results of archived or cached versions of the website</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Date</td>
<td>✓</td>
<td>Initials</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
<td>---</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Search, print and file Whois information for registrant</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search, print and file reverse Whois results (may require the use of vendor tools)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search, print and file reverse telephone/address/other registrant information results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Checklist: Domain Name Enforcement Matter

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
<th>Initials</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure all actions and information are recorded in the docket or other</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>internal management charts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B. Online Content Infringement

1. IP Infringement on Websites and Social Media Platforms

Separately from domain names, trademarks often are infringed on websites and social media platforms, both in posts, in user names and in user profiles. For instance, either directly on websites or indirectly in meta tags, infringers may use other parties’ word marks to increase the likelihood of appearing in search engine results and thus driving Internet traffic to the infringing sites. Similarly, infringers may use third-party word marks or logos on websites or social media platforms to create ostensibly authentic websites or profiles in attempts to sell counterfeit goods, spread malware, or provide services of lower quality than those provided by the mark owners. Some infringers are sophisticated enough to very nearly replicate official websites and trick users into providing personally identifying information or financial information.

Online platforms, and social media sites in particular, have become common infringement fronts, because the costs of entry are very low and there is a virtually limitless ability to reach a large audience. Registering a new username takes only a few minutes, and, as with domain names, with infinitely many permutations of their names, brand owners can never preemptively defend the entire space and thus always face some exposure. In addition, unlike domain names, which do bear modest registration costs, registration of profiles on social media platforms is
usually free and requires only minimum, if any, identifying information. Major platforms such as Twitter or Facebook have hundreds of millions of users; infringers can cause serious damage to a brand with only a few keystrokes.

As with traditional enforcement efforts, generally it is far easier to protect strong, distinctive trademarks.

Websites and social media profiles and posts are easy to modify or even take down completely, so it is especially important to capture dated evidence of the infringement. Enforcing rights usually mandates that brand owners maintain records showing the date and time when potentially infringing material was made available online, as well as the specific Uniform Resource Locator (URL) through which the content was made available. In the case of infringing content on a webpage, also capture the Whois information for the domain name and archival screen shots if available. (See Section IV.A.1, above.)

Online and social media enforcement is complicated by the publicity that can surround enforcement efforts. The examples of companies’ overreaching by sending overly aggressive demand letters only to have the targets post those letters for ridicule are too many to list. Therefore, generally it is appropriate to have a tiered approach to enforcement which, depending on the circumstances, begins with a polite, direct request to the infringer to remove or change the offending content, followed by use of the social media platforms’ established dispute resolution procedures, a formal cease and desist letter, and, finally, a lawsuit.

For more information on the subject of social media, see Jomarie Fredericks, “Social Media Issues Facing In-House Practitioners,” INTA Bulletin, Vol. 67 No. 15 (September 1, 2012).

2. IP Infringement in Mobile Applications

The degree to which people around the world are using smart phones, personal digital assistants, tablets, and electronic book readers in lieu of desktop computers indicates the importance of these electronic devices and modes of communication. The number of mobile app downloads continues to rise through the last decade, catching the interest and attention of lawyers and others in the legal field.
As with all instances of trademark infringement, whether the infringing content has a direct negative impact on a business plays a big factor in the determination of whether to take immediate action against infringing mobile applications. The top priority would be third-party mobile applications offered by or in connection with a competitor’s goods or services, making unauthorized use of your trademark or a confusingly similar trademark. Generally, a competitor’s unauthorized use of a brand to promote its own goods or services, including its own mobile application(s), should not be tolerated. However, be aware of fair use issues, such as nominative fair use of a brand in comparative advertising, which is generally allowed in the United States. In addition, a company should not tolerate any unauthorized third-party sale or distribution of its branded mobile applications—especially where the company already offers its own branded mobile application for free download.

Infringing content in mobile applications can be found by understanding how the apps work and monitoring proactively across several marketplaces (also called platforms). The major platform operators in this arena (called mobile marketplaces) are Apple’s App Store, Google Play (including the Android Market), Amazon Appstore, Palm’s App Catalog, Blackberry World, Samsung Galaxy Apps, and Microsoft’s Windows Store. Regardless of whether a company’s brand currently has its own mobile application(s), a quick search on these platforms may allow trademark owners to identify unauthorized third-party use of their marks. The need to police this space has given rise to various third-party mobile app monitoring and abuse detection services, such as App Detex. There are often additional infringing applications or content in the profile of the particular application developer or developers.

Infringing apps can prove highly problematic for both the users and the companies that are infringed. At a minimum, unauthorized apps may function poorly, resulting in a subpar user experience that can generate dissatisfaction among users. Such apps may also direct users to links with undesirable content, thereby creating an undesirable association with the brand. Finally, infringing apps that appear to be genuine may capture users’ financial or other personal details and use them in a malicious manner, and they may also contain viruses or malware that can infect users’ devices. Thus, the potential for infringing apps to
cause damage to a company’s brands and goodwill is quite high, and they can have a significant impact on a company’s ability to connect with customers.

As with evidence of an infringing domain name, when a potentially infringing app has been identified, it is important to collect and preserve evidence of the infringing application. The Administrator should document any evidence of infringement. It may be helpful to keep a schedule of a company’s registered trademarks on hand for comparison purposes—especially where logos or design marks are in question.

**Checklist: Collecting Evidence for an Infringing App**

1. Take date-stamped screen shots of the infringing content.

2. Make note of the following information:
   - The name of the app.
   - The purported developer.
   - Where the app is available, and, if it is offered for sale, the price.
   - The mobile platforms or operating systems for which the app is available.
   - Any comments about the app, noting any actual confusion with your brand.

3. Before pursuing any enforcement action, investigate in-house to see whether the developer was contracted to develop the app. Sometimes, different departments within a company may not communicate such an arrangement to the legal department or outside counsel.

Major social media platforms have in place unique notice and takedown policies and procedures. When available, these are often the most efficient and cost-effective means of having problematic content removed. Trademark owners typically enjoy a higher success rate in removal of infringing content through the mobile marketplace, as opposed to taking action directly against an infringer. Mobile marketplaces outline their notice and takedown policies and procedures on their websites and provide links to online takedown or complaint forms for reporting suspected infringement of intellectual property rights, including instances of trademark infringement. Often, the Administrator is responsible for
completing takedown requests and for tracking the status of requested takedowns. (See INTA, Industry Perspectives, “Using Third-Party Logos in Downloadable Applications.”)

In the enforcement realm, Administrators most often are requested to contact the website or social media platform to ask that infringing content be removed. Website hosting providers usually have broadly worded policies for reporting abuses, which are available on their websites. Sending a letter to the host and citing specific clauses in the provider’s acceptable use policy or terms of service is a quick and cost-effective method of handling trademark infringements.

A survey of takedown policies and procedures for the most popular social media and mobile application providers is provided in Appendix 1.

3. “Phishing” and Fraudulent Emails

a. Definition

Phishing generally is defined as the criminally fraudulent process of attempting to obtain information or money by masquerading as a trusted person or entity in an electronic communication. Some thieves operate by sending out emails to divert people to websites that appear very similar to an organization’s authentic site but in reality are fraudulent and used solely to obtain personal and financial information. Other thieves hack into the email accounts,

Practice Tip

An Administrator may be able to help the company’s IT and/or security business unit(s) trace fake emails by examining the message’s “long header,” which provides certain technical information. This is viewed in different ways in different email systems, but it is possible to locate it in any system and from that to track the path the message has taken from its origination to the recipient computer. Although headers will not always produce reliable answers, it is possible for a skilled infringer to “fake” this information as well; in many cases, this type of tracking works. Therefore, when an Administrator receives notice of a potentially phished email, he or she should contact the recipient of the email and request that it copy and paste the original email header received for analysis by IT professionals.

1 Google provides a simple description of how to find the headers in the most common email systems. See http://mail.google.com/support/bin/answer.py?hl=en&answer=22454.
steal their email address books, and send messages that purport to come from those hacked persons. Also, every year hackers appropriate numerous corporate email addresses and then use phishing to elicit information from would-be customers, supporters, and/or employees, which often results in the threat of contamination of IT systems and infrastructure.

b. Strategies for Addressing and Preventing Phishing

A “best security practice” is to require that all company personnel conduct business from email addresses established within their institution’s domain name, because it allows the company’s IT and security staff easily to monitor and prevent phishing schemes and other forms of Internet fraud. The company should establish a domain name such as www.company.com rather than using email addresses from free email providers, in order to improve system security. An organization possessing its own domain name normally is able to launch an email system from that domain name.

It is also very important that users change their password whenever there is evidence of phishing; the first step that users should take is to change their password. Choose a password that is difficult to crack, such as a word that does not have an obvious association with the user. It need not necessarily contain a combination of letters, numbers, and symbols, but should nevertheless be difficult for a third party to guess. Finally, companies should require screening of new passwords against lists of commonly used or compromised passwords.

Companies should work with law enforcement and registries to prosecute thieves that use phishing to harm their infrastructure and damage their reputation.

---

2 http://www.millersmiles.co.uk/submit.php, a website dedicated to the provision of anti-phishing services, contains practical steps that a company should take if phishing occurs.

V. Conclusion

The Internet presents brand owners with amazing opportunities for growth, as well as unique challenges related to potential infringement. By developing best practices for conducting business on the Web and understanding available mechanisms to enforce rights, brand owners can minimize the negative aspects of the Internet and reap the benefits that it has to offer. Here are some tips for Administrators whose responsibilities have been expanded to include oversight of domain name portfolios and/or policing and enforcement on the Internet:

- First, understand that, in many ways, these responsibilities are no different from the typical policing and enforcement activities. Although the specific mechanisms may be different, ultimately the daily activities will become as comfortable to you as reviewing other watching materials.

- Immerse yourself in the material as much as possible, including your organization’s or client’s website(s), other aspects of its online presence, and, if relevant to brand promotion and enforcement efforts, social media platforms. Take advantage of the many free webinars on domain name topics and Internet enforcement strategies offered by law firms, corporate registrars, and other service providers.

- Make sure to work with your organization’s corporate registrar if that role is not handled by the legal group. Become familiar with your organization’s domain name portfolio and domain name registration policies.

- Generate customized plans and checklists that reflect your organization’s or client’s priorities in connection with the Internet and brand enforcement online.

- Refresh and enhance your knowledge as much as possible. Remain apprised of key ICANN developments, new social media platforms that appear to be gaining traction, and technical trends regarding infringement and other problematic online behaviors you may need to police.
• As responsibility for your organization’s Internet presence and enforcement may seem to be a daunting task, take the time to enlist a skilled support network. This may include the organization’s IT and security personnel; marketing personnel, who can keep you informed regarding digital marketing efforts and priorities; vendors, such as registrars; outside counsel; and international counsel, who can ensure that you are ready to handle any matter, regardless of jurisdiction.
Appendix 1

Survey of Social Media Takedown Policies and Procedures

Procedures may vary from one provider to another, but generally the provider asks for information regarding the infringing content (location, how the infringement affects you, and other documentation of the infringement) and information about your business (including address and other contact information, and registration details, if applicable).

Following is information regarding the takedown policies and procedures for some of the most popular content providers and social media platforms at the time of publication.

Twitter

- [https://support.twitter.com/articles/18367](https://support.twitter.com/articles/18367)
- **Twitter Trademark Complaint Form:** [https://support.twitter.com/forms/trademark](https://support.twitter.com/forms/trademark)
- Once you have submitted the form, Twitter will send an email acknowledgment, which will have the ticket number for this matter. If you submit a report with incomplete information, Twitter will follow up with you to request that information. Please note that this will result in a delay in processing your report. Average response time is generally 10-15 business days. Following up on the acknowledgment email generally will not expedite matters.

Facebook

- Community Standards: [https://www.facebook.com/communitystandards](https://www.facebook.com/communitystandards)
• Report trademark infringement by completing the Facebook Trademark Violation/Infringement Form (http://www.facebook.com/help/contact/?id=208282075858952).

• Once you have submitted the form, Facebook will send an email acknowledgment. Facebook usually will take action or follow up with additional questions within 5 business days.

Google Properties

• Trademark infringement reports apply to the various Google properties through the Removing Content from Google Tool. https://support.google.com/legal/troubleshooter/1114905

• Once you have identified the method for a complaint and submitted an appropriate form, Google will send an email acknowledgment, which will have the ticket number for this matter. Google usually will take action or follow up with additional questions within 5 business days. If you have not heard anything after 5 business days, you can follow up by responding to the acknowledgment email.

• Be aware that Google may send a copy of your complaint to Chilling Effects, which in turn may publish it on the Chilling Effects website, though your contact information will be redacted.

YouTube

• As noted on the YouTube Support Website, “YouTube is not in a position to mediate trademark disputes between users and trademark owners. As a result, we strongly encourage owners to resolve their disputes directly with the user who posted the content in question.”

• To begin the YouTube trademark dispute resolution process, go to https://www.youtube.com/reportingtool/trademark?rd=2.
iTunes App Store

- Once you have submitted the form or sent your email, Apple usually will take action or follow up with additional questions within 5 business days.

CafePress

- Report trademark infringement by contacting CafePress.com’s Intellectual Property Rights Agent, Lindsay Moore, by mail, email, or telephone, as follows:
  
  **Mail:** CafePress.com  
  Attn: Lindsay Moore  
  Intellectual Property Rights Agent  
  11909 Shelbyville Road  
  Suite 300  
  Louisville, KY 40233  
  
  **Email:** trademark@cafepress.com  
  **Telephone:** (502) 822-7501  

- Information you will need to include in the notice to report trademark infringement to CafePress.com:
  
  - A physical or electronic signature of a person authorized to act on behalf of the owner of the copyright or other rights that have been allegedly infringed.
  - Identification of the trademark that has been allegedly infringed.
  - The URL or product number(s) used in connection with the sale of the allegedly infringing merchandise. (Note: A storeid URL is www.cafepress.com/storeid. Simply including www.cafepress.com
is not sufficient to identify what you are objecting to; use the “storeid” part of the URL to identify the user.)

- Your name, address, telephone number, and email address.
- A statement that you have a good-faith belief that use of the material in the manner complained of is not authorized by the rights owner, its agent, or the law.
- A statement that the information in the notification is accurate and, under penalty of perjury, that you are authorized to act on behalf of the owner of the copyright or other right that is allegedly infringed.