

**American Bar Association
41st Annual Forum on Franchising**

DOMAIN NAME MANAGEMENT AND ENFORCEMENT

**Carol Anne Been
Dentons US LLP
Chicago, Illinois**

and

**Susan Meyer
Greensfelder, Hemker & Gale, P.C.
Chicago, Illinois**

**October 10 - 12, 2018
Nashville, Tennessee**

Table of Contents

I.	INTRODUCTION.....	1
II.	REGISTRATION AND MAINTENANCE OF DOMAIN NAMES - BASICS.....	1
	A. Very Brief History and Background of the Internet.....	1
	B. Basic Terms and Concepts	2
	1. What's in a Name? IP Addresses, Domain Names, URLs	2
	2. ICANN	4
	3. TLDs.....	5
	4. gTLDs and ccTLDs	6
	5. UDRP and ACPA.....	7
	C. Selecting a Domain Name Registrar.....	7
III.	PORTFOLIO MANAGEMENT	7
	A. Which Domain Names to Register.....	7
	1. Business Needs / Budget.....	8
	2. Blocking Cybersquatting, Infringement and Other Misuse of Trademarks in Third Party Domain Names.....	9
	3. Public Registries	9
	4. Scam Emails Using Domain Name Information.....	10
	B. How Long to Maintain Registrations	10
IV.	OWNERSHIP / CONTROL ISSUES WITH EMPLOYEES AND VENDORS	11
V.	FRANCHISE SPECIFIC CONCERNS	12
VI.	HOW TO OBTAIN DESIRED DOMAIN NAMES	12
	A. Offers / Negotiations.....	12
	B. Sales of Domain Name Portfolios.....	14

VII.	POLICING OF DOMAIN NAMES	19
A.	Trademark Evaluation	19
B.	Problems with WHOIS Registries	19
1.	Privacy Shields	19
2.	WHOIS Blackout.....	20
C.	Cybersquatting Proceedings	21
1.	UDRP	22
2.	Dispute Resolution for ccTLDs.....	26
3.	ACPA.....	27
4.	Trademark Owners Vote by Their Choice of Jurisdiction.....	29
VIII.	FUTURE OF DOMAIN NAMES	30
A.	What is on the Horizon?	30
B.	Checklist for Best Practices.....	32
1.	Treat Domain Names Like Trademarks	32
2.	Treat Domain Name Registrations Like Copyright Registrations.....	32
3.	Register Domain Names Containing Main Trademarks, (i.e. house marks)	32
4.	Choose Domain Registrar Carefully.....	32
5.	Establish Appropriate Protocols for Records Retention	32
6.	Manage Domain Name Portfolio and Enforcement	32
7.	Avoid Scam Artists.....	33
8.	Be Pro-active	33
IX.	CONCLUSION	33
	EXHIBIT A, SUPPLEMENTAL MATERIALS	34

DOMAIN NAME MANAGEMENT AND ENFORCEMENT

I. INTRODUCTION

Are domain names disappearing? Are they like mobile telephone numbers – programmed into a telephone once and never dialed again? Or are they valuable intellectual property assets on par with trademarks – worthy of time, attention, and budget? Although consumers' use of domain names will change as the public continues to adapt to advancing technology and legal developments, for now domain names remain an important element of any business' strategy.

This paper addresses fundamental issues concerning domain names to help franchise systems, clients, and law practices. After providing some background, with a brief history and key terms, this paper discusses the ownership and management of domain names. The paper focuses on key questions facing the franchise relationship and offers practical considerations for obtaining, selling, and policing domain names. Finally, the paper takes a glimpse into the future and presents a checklist suggesting some best practices.

II. REGISTRATION AND MAINTENANCE OF DOMAIN NAMES – BASICS

A. Very Brief History and Background of the Internet

Simply put, the Internet is a global network of computers. In the 1950's, local area networks (LANs) interlinking computers within a single building expanded into wide area networks (WANs).¹ Starting in the 1960's, interested technologists began to propose the idea of a global network following the same principle.² While there were many projects and networks that helped pushed the boundaries of the technology, the United States Department of Defense's ARPANET (Advanced Research Project Agency Network) is perhaps the most famous.³ ARPANET was begun in 1969 as a packet switching network and was the first to interconnect multiple networks as well as the first to begin using the Internet protocol suite (TCP/IP) in 1982.⁴ The World Wide Web which uses Uniform Resource Locators (URLs) interlinked by hyperlinked text was invented by Tim Berners-Lee⁵ (who was influenced by computer scientist Jon Postel, sometimes called one of the "fathers" of the Internet).⁶ The World Wide Web first became accessible via the Internet in 1989, and available to the public in 1991.⁷

¹ <http://www2.law.columbia.edu/donnelly/lda/ih/techprof3.html>.

² <http://www2.law.columbia.edu/donnelly/lda/ih/techprof4.html>.

³The United States Department of Defense Advanced Research Project Agency is also referred to as DARPA; <https://www.darpa.mil/about-us/about-darpa>; <https://www.darpa.mil/Timeline/index.html>.

⁴ <http://www2.law.columbia.edu/donnelly/lda/ih/techprof2.html>.

⁵ <http://www2.law.columbia.edu/donnelly/lda/ih/techprof5.html>.

⁶See, e.g., <https://www.independent.co.uk/arts-entertainment/obituary-jon-postel-1179966.html>; <https://www.internetsociety.org/grants-and-awards/postel-service-award/ten-year-tribute-jon-postel/>.

⁷ https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

Just three years ago, Google's then-executive chairman, Eric Schmidt, predicted "that the Internet will disappear." He explained to confused audiences in several presentations⁸ that it will soon become like telephone lines and electricity – part of the fabric of our existence - we just know it is there – we take for granted that it works.

Domain names serve as a recognizable gateway to the Internet by providing a user-friendly address system to locate the computers hosting the websites sought by the public in a vast sea of data. Domain names are actually a string of letters that are used for networking and routing purposes by the computers that make up the Internet.⁹ Domain names serve a similar function for a host computer's numerical IP address, but people recognize words more than a string of numbers. Other than DARPA, the first domain name *created* was nordu.net.¹⁰ A Scandinavian research collaboration created nordu.net on January 1, 1985.¹¹ The first domain name registrar was Network Solutions Inc. ("NSI") in 1993.¹² The first domain name *registered* was symbolics.com (March 15, 1985) to a computer systems company in Cambridge, Massachusetts.¹³ Both of these domains remain active today, though symbolics.com is now owned by another company.¹⁴

Since the creation and registration of the first domain names, the very way that humans interact, collect information, and conduct business has evolved dramatically. As this paper discusses how best to manage domain names, it is useful to understand some basic terms.

B. Basic Terms and Concepts

1. What's in a Name? IP Addresses, Domain Names, URLs ...

a. IP Address

Each computer that connects to the Internet needs a unique identifying number, which serves as its individual address. This is its Internet Protocol address (IP address).¹⁵ An IP address provides information about the host (or network interface identification) and location.¹⁶ For example, the IP address for the Forum on Franchising's home page is: 45.60.122.186.¹⁷ It is located in or around Redwood City, California.

⁸ <https://www.businessinsider.com/google-chief-eric-schmidt-the-Internet-will-disappear-2015-1>.

⁹ <https://www.icann.org/resources/pages/glossary-2014-02-04-en#d>.

¹⁰ https://www.verisign.com/en_US/domain-names/net-domain-names/first-domain-name-registered/index.xhtml.

¹¹ <https://www.whois.com/whois/nordu.net>; <http://nordu.net/>.

¹² <https://www.networksolutions.com/why-choose-netsol/company-history.jsp>.

¹³ <http://symbolics.com/about.php>.

¹⁴ *Id.*

¹⁵ <https://www.icann.org/resources/pages/glossary-2014-02-04-en#d>

¹⁶ *Id.*

¹⁷ <https://www.iplocation.net/>.

b. Web Server/Web Host

A web server is typically an individual machine that runs websites.¹⁸ If the web server is connected only to designated machines within an organization, then it is part of an *Intranet* and is not available to the public.¹⁹ If a web server is connected to the Internet, then its IP address will be used to communicate between different servers.²⁰ A web host computer is typically a computer controlling other terminals or computers. (A web host may also refer to an organization that provides a service.) Whether on an Intranet or the Internet, each host has an identifier known as a hostname, to help identify each machine as well as the network.²¹ When connected to the Internet, the local hostname becomes part of the overall domain name.²² The most famous local hostname on the Internet is for the World Wide Web, that is, www._____.²³

c. DNS; Domain Name

People remember names and words more easily than they do strings of numbers. Because the Internet functions by connecting IP addresses – strings of numbers – every web server must be able to translate domain names into IP addresses.²⁴ This happens via the Domain Name System (DNS), a decentralized system made of many DNS servers.²⁵ Essentially, the DNS is the phone book of the Internet that maintains a directory of domain names and converts them to IP addresses, while a DNS server is a part of the whole system and stores DNS records for a domain.²⁶ The Forum on Franchising is located through the domain name www.americanbar.org.

d. URL

“URL” stands for “Uniform Resource Locator.”²⁷ This is the unique address for a file on the Internet.²⁸ A URL has two main components: the protocol identifier and a resource name.²⁹ For the URL http://example.com/ex.html, the protocol identifier is “http” and the resource name

¹⁸ <https://pc.net/glossary/definition/server>.

¹⁹ <http://www.businessdictionary.com/definition/intranet.html>.

²⁰ <https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm>.

²¹ *Id.*

²² *Id.*

²³ <https://cyber.harvard.edu/readinessguide/glossary.html#l>.

²⁴ <https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm>;
<https://www.icann.org/resources/pages/what-2012-02-25-en>.

²⁵ *Id.*

²⁶ <http://www.networksolutions.com/support/what-is-a-domain-name-server-dns-and-how-does-it-work/>.

²⁷ <https://cyber.harvard.edu/readinessguide/glossary.html#l>.

²⁸ *Id.*

²⁹ <https://pc.net/glossary/definition/url>.

is "example.com/ex.html".³⁰ HTTP stands for Hyper Text Transfer Protocol and it is the protocol over which data is sent between a browser and the website that a consumer is connected to.³¹ "HTTPS" means Hyper Text Transfer Protocol Secure (HTTPS) and is the secure version of HTTP.³² This protocol encrypts all communications between a browser and the website.³³ HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

The resource name is divided by the slash into the domain name, here, the domain name, example.com, and the file name, ex.html. The Forum on Franchising's home page URL is: <https://www.americanbar.org/groups/franchising.html>. Thus, https is the protocol, and www.americanbar.org/groups/franchising.html is the resource name, breaking down further into the domain name www.americanbar.org, with www. as the local hostname, and the filename being groups/franchising.html.

2. ICANN

Originally an informal group formed out of the ARPANET project known as IANA (Internet Assigned Numbers Authority) administered the registries of Internet protocol identifiers, including distributing top-level domain names and IP addresses.³⁴ As the Internet expanded, some objected to this role being handled by the United States government. Therefore, in 1998 key parties created a formal, non-governmental organization, the Internet Corporation for Assigned Names and Numbers ("ICANN").³⁵ ICANN is a US nonprofit public benefit corporation.³⁶ Its "role is to oversee the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another."³⁷ ICANN has responsibility for IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions.³⁸

ICANN is made up of eight groups that represent the various interests on the Internet and contribute to ICANN's final decisions.

ICANN Groups	
"Supporting organizations" that represent:	1. Organizations that deal with IP addresses
	2. Organizations that deal with domain names

³⁰ <https://www.iana.org/domains/reserved>.

³¹ <https://pc.net/glossary/definition/http>.

³² <https://pc.net/glossary/definition/https>.

³³ *Id.*

³⁴ <https://www.icann.org/history>.

³⁵ *Id.*

³⁶ *Id.*; <https://www.icann.org/resources/pages/governance/articles-en>.

³⁷ <https://www.icann.org/resources/pages/what-2012-02-25-en>.

³⁸ *Id.*

	3. Managers of country-code top-level domains ("ccTLD") (an exception explained below)
"Advisory committees" that provide ICANN with advice and recommendations, and represent:	4. Governments and international treaty organizations
	5. Root server operators
	6. Those concerned with the Internet's security
	7. The "at large" community, meaning average Internet users.
"Technical Liaison Group"	8. Works with the organizations behind the basic protocols of Internet technologies. ³⁹

ICANN's final decisions are made by its Board of Directors. The Board is made up of fifteen voting members and six non-voting liaisons from around the world. An independent Nominating Committee chooses eight of the voting members, while the remaining members are nominated from the supporting organizations.⁴⁰

ICANN operates on consensus to formulate coordination policies implemented by the agreement of the operators of the core elements, including generic top level domain ("gTLD") registry operators and sponsors, ccTLD managers, as well as regional Internet (IP address) registries, and root-name server operators.⁴¹ Perhaps the most important decision by ICANN was the creation of the Uniform Domain Name Dispute Resolution Policy ("UDRP"), which is used to resolve issues between competing interests in domain names.⁴² One recent example of ICANN action is the 2010 decision to loosen some of the restrictions on gTLDs, to allow non-Latin characters in what are called internationalized country code TLDs or IDN ccTLDs) and eventually pave the way for hundreds of new generic (as opposed to country-specific) TLDs (gTLDs).⁴³

3. TLDs

Domain names are divided into levels by the "dot."⁴⁴ To the furthest right is the top-level domain ("TLD") and to the left are collectively "lower level domains" with each level being referred to by its ordinal rank, e.g., second-level domain, third level domain and so forth.⁴⁵ In www.example.com, ".com" is the TLD and "example" is the second level domain name. Other well-known TLDs are .net, .org, and .edu.⁴⁶

³⁹ *Id.*

⁴⁰ *Id.*; The current ICANN Board of Directors is shown at <https://www.icann.org/news/announcement-2-2017-09-01-en>.

⁴¹ <https://www.icann.org/resources/pages/what-2012-02-25-en>.

⁴² <https://www.icann.org/resources/pages/help/dndr/udrp-en>.

⁴³ <https://www.icann.org/en/system/files/press-materials/release-06may10-en.pdf>.

⁴⁴ <https://archive.icann.org/en/tlds/>.

⁴⁵ *Id.*

⁴⁶ *Id.*

A registry is a company that is in charge of all domain names with a particular TLD.⁴⁷ The registry holds a full list of domain names under that TLD and the associated IP addresses. Second level domain names are registered with the registries and are used to provide online systems such as websites, email servers, and such.⁴⁸ There are a large number of “registrars” that sell these domain names to users at prices set by the registrar, with the registrars paying a per-domain name fee to the registry of the applicable top level domain.⁴⁹

One of ICANN's activities is to work with the organizations involved in the Internet's technical coordination to formally document their participation within the ICANN process and their commitments to implement the resulting policies.⁵⁰ These include entering into agreements with over 150 ICANN-accredited registrars, the regional Internet registries (for number allocation), and the Internet Engineering Task Force.⁵¹

4. gTLDs and ccTLDs

There are currently three main groups of top level domains (TLDs): (i) generic top level domains (gTLDs) mentioned above, which encompass sponsored and unsponsored gTLDs, (ii) country-code TLDs (ccTLDs), and (iii) infrastructure TLDs.⁵²

Currently there are only six “unsponsored” gTLDs (.com, .org, .net, .biz, .info and .name). These are the least restrictive gTLDs. Domain names using these gTLDs may be purchased and used for most purposes, subject only to the policies of ICANN.⁵³

“Sponsored” gTLDs are sponsored by various companies, organizations, and agencies, which are free to put restrictions on their use.⁵⁴ For example, .mil is sponsored by the United States Department of Defense and is restricted to US military use, while .museum is sponsored by the Museum Domain Management Association, which restricts its use to museums. There are currently approximately 1,300 sponsored gTLDs. This number grew dramatically when ICANN invited applications for new gTLDs in 2012.⁵⁵ ICANN is not currently accepting applications for any additional gTLDs.⁵⁶

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ <https://www.icann.org/resources/pages/listing-2012-02-25-en>.

⁵⁰ <https://www.icann.org/resources/pages/groups-2012-02-06-en>.

⁵¹ <https://www.icann.org/resources/pages/ietf-2012-02-25-en>; <https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en>.

⁵² <https://archive.icann.org/en/tlds/>.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ <https://newgtlds.icann.org/en/about/program>.

⁵⁶ <https://newgtlds.icann.org/en/>.

An individual or legal entity wishing to register a domain name under a generic top-level domain in any registry⁵⁷ may do so through an ICANN-accredited registrar.⁵⁸ There are several hundred accredited registrars located throughout the world that provide support in local languages. The relationship between a domain name registrant and the ICANN-accredited registrar is governed by a registration agreement.⁵⁹

Country-code top-level domains are two-letter domains (.au, .ca, .jp, .uk, etc.) that are controlled by the respective country and usually restricted to use by their government. There are currently approximately 250 ccTLDs.⁶⁰

The single infrastructure TLD is the .arpa domain which is reserved solely for Internet infrastructure use by ICANN.⁶¹

5. UDRP and ACPA

Domain name disputes typically arise when a brand owner objects to a third party including its trademark in a domain name without authorization. The two main systems to resolve such disputes used by US brand owners are ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP")⁶² and the federal Anti-Cybersquatting Consumer Protection Act (ACPA).

C. Selecting a Domain Name Registrar

In addition to the ICANN accredited registrars for the gTLDs, there are thousands of ICANN accredited registrars for domain names under the gTLDs. Many registrars promote themselves with flashy commercials advertising low rates for domain name registration. Because the relationship between the domain name registrant and the registrar is governed by an agreement and terms of use, it is important to review the agreement and terms before choosing a registrar. Key factors to consider include price; the ease of transferring a domain name to another registrant, or a portfolio of domain names to another registrar; how failure to renew a domain name is handled; customer service; additional services; and the policy addressing disputes between the registrant and registrar. Godaddy, name.com and networksolutions.com are probably the most widely known registrars based in the US.

III. PORTFOLIO MANAGEMENT

A. Which Domain Names to Register

A domain name registration program should be aligned with an overall trademark portfolio strategy. Domain name registrations can help protect the owner's existing trademark

⁵⁷ See, <http://www.icann.org/en/resources/registries/listing> for a list of registries.

⁵⁸ See, <http://www.internic.net/regist.html> for a list of registrars.

⁵⁹ <https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en>.

⁶⁰ <https://www.icann.org/resources/pages/cctlds-21-2012-02-25-en>.

⁶¹ <https://www.iana.org/domains/arpa>.

⁶² <https://www.icann.org/resources/pages/help/dndr/udrp-en>.

rights, are part of the owner mapping new source identification rights on the Internet, and may be useful to keep competitors and cybersquatters away from the owner's trademark rights. Registration of domain names for blocking purposes is particularly important as many domain names are available on a first-come, first-served basis with no scrutiny of brand ownership at the time of registration, and many registrants ignore contractual restrictions in taking domain names using another's mark for commercial purposes.

In general, a brand owner needs to balance the additional trademark usage and goodwill created by including a trademark in a domain name and the blocking benefits of preventing unauthorized uses against the expenses of training the market to recognize a new domain name and of maintaining a portfolio of domain names that can be ever-expanding. The pros and cons are discussed further below.

1. Business Needs / Budget

Of course, the trademark owner should obtain domain names using its main trademarks, typically its house brands. Slogans, mascots, and non-traditional trademarks may also be worth registering if the owner's market would expect to find the company's website using those signals. Sub-brands and temporary or seasonal marks might be worthy of domain name registration as well, such as for a site that is available only periodically or for special purposes (such as for a sweepstakes or special promotion). Frequently, companies adopting a new brand or trademark conduct a domain name availability search together with -- or before -- a trademark clearance search. This remains a prudent approach, as a web presence under key trademarks remains an important part of a company's identity. The business' needs and budget will impact the decisions concerning which and how many domain names to register.

The budget for domain names must be balanced against the owner's business needs. While each domain name registration and renewal may be relatively inexpensive, when a portfolio gets into the hundreds or thousands of domain names, the carrying costs can be high. Even after deciding which marks to include in domain names, selecting the specific domain names to register may be more difficult. If the mark is "example," the brand owner must consider whether to register example.com alone, or also example with other TLDs such as .org, .net, .biz, .info and .name, and perhaps with some sponsored TLDs. The brand owner also must consider which country code domain names may be valuable.

For example, if the owner's main market outside the United States is the European Union, the owner must consider whether to register example.eu and "example" with the country code of each of the 28 EU member states. With the United Kingdom exiting from the European Union effective March 29, 2019, the .eu country code will no longer apply to the United Kingdom. A .eu domain name registrant based in the United Kingdom will no longer fulfill the eligibility requirement that registrants with .eu domain names must have their registered office or principal place of business in the European Union. The Registry for .eu domain names may revoke domain names for United Kingdom registrants on its own initiative.⁶³

In addition, the brand owner must consider whether to choose second level domains that include words, numbers or symbols in addition to the brand itself. If the house mark is "example kitchen", the owner might consider examplekitchen, examplekitchenrestaurant,

⁶³ See, *Notice to Stakeholders, Withdrawal of the United Kingdom and EU rules on .eu Domain Names*, European Commission Directorate-General for Communications Networks, Content and Technology (Mar. 28, 2018), https://ec.europa.eu/info/sites/info/files/notice_to_stakeholders_brexit_eu_domain_names.pdf.

examplerestaurant, examplekitchencoffee, etc. as second level domains. Although this may result in a large number of variations, that number would be multiplied by the number of TLDs chosen. Many companies also acquire additional domain names in business transactions and in domain name policing, which can further increase the size of a portfolio and the cost to maintain it.

Yet another consideration is whether the brand owner should consider obtaining internationalized domain names ("IDNs") which use other language characters (e.g., Chinese, Arabic, Hebrew). If the mark is promoted in China, for example, it may be important to have a domain name in Chinese characters. The brand owner should consult with local Chinese speakers who are familiar with brand issues in China, to work on the choice of characters and their meaning (and possible misunderstanding of the meaning). Some brands choose a Chinese name that is not a transliteration of their English name, but that has meaning that is attractive to the local market, perhaps signifying honesty or good luck in a Chinese dialect.

2. Blocking Cybersquatting, Infringement and Other Misuse of Trademarks in Third Party Domain Names

Brand owners may want to block others who wish to cybersquat, infringe or otherwise misuse the brand owner's rights (such as by incorporating the mark in a domain name for a website to misdirect traffic, or an email server to conduct phishing attacks and fraud). Brand owners also may want to block scammers that register mistyped or misspelled domain names in order to misdirect unaware consumers to their websites. This practice, known as typosquatting or brandjacking, may directly benefit the scammer or cause harm to the competitor. While one could potentially win a claim against these misuses under the UDRP or ACPA, the cost of proceedings and the potential harm pending resolution may not be worth it. Some brand owners will register misspelled variations of their own domain names in order to block others from getting domain names with the misspelled domains. Brand owners often will redirect their domain names under various gTLDs and misspellings to one main website. Other brand owners may just hold the domain names without activating them, to keep the domain names out of use.

3. Public Registries

It is important to remember that domain name registries, like the United States Patent and Trademark Office registries, are public records with registrant information available to third parties. ICANN manages a central database with domain name registrant (and registrar) information for all TLDs, called the WHOIS directory. The WHOIS database is a free, publicly available directory of domain name registrants and the domain names they own, maintained by the entity that governs domain names, ICANN.⁶⁴ The WHOIS database contains information provided by domain name registrants to registrars, and is publicly accessible through the registrars, intended to provide transparency. Availability of domain name ownership information is critical to learning who is behind a domain name or website, and to assessing whether the domain name registrant may be engaging in cybersquatting or trademark infringement due to the website posted at the domain name. Many registrars and other entities provide access to WHOIS records from ICANN.

For the most part the WHOIS records are "self service," meaning that domain name registrants can identify themselves as they choose, sometimes with pseudonyms, assumed

⁶⁴ <https://www.whois.com/>.

names or false contact information, with no checking by a registrar or other authority of the accuracy of the name and contact information of the listed registrant -- even if this violates the agreements to which the registrants are bound.

Some domain name registrants choose to register through a company that provides a privacy shield, to conceal the identity of the domain name owner. The use of a privacy shield is permissible. A brand owner may choose a privacy shield to remain discrete, such as in the situation where an individual owns the domain name and does not want to make public his or her personal contact information, or a brand owner has not yet announced the launch of a new brand and does not want the brand connected to the brand owner via the domain name registration until the announcement is made.

However, privacy shields have had an impact on handling of domain name disputes. In addition, in response to the new European privacy directive European Global Data Privacy Regulation ("GDPR"), ICANN has suspended the availability of registrant information due to privacy concerns while interested parties work toward a solution to balance privacy concerns and the needs of others to learn who owns a domain name.

4. Scam Emails Using Domain Name Information

Domain name registrants are also targets for scam artists that direct various schemes to extract unnecessary payments from unsuspecting registrants. The most common scam is to contact domain name owners claiming alleged registration of their mark in a country code TLD by an unauthorized party and seek to engage the domain owner in paying for the scammer to "prevent" the alleged third party from obtaining the country code TLDs. The general advice for brand owners is to evaluate their domain name registration portfolio and plans, engage a domain name watching service for domains that may interfere with their portfolio or plans (see discussion below), and have the confidence to ignore unsolicited requests to allegedly police the mark in other domains that are not a business concern for the brand owner. Many attorneys use language such as the following in their transmittal letters to clients when they file a new trademark application or make other public registrations:

Please be aware that there are unscrupulous third parties who retrieve the data off of the USPTO website and send trademark registrants statements, urgent requests, monitoring services, and foreign trademark information. Many of these mailings (via the post, fax, or email) look official and/or extremely important. They are almost always scams. Please forward any of these to us for review.

We are your official correspondent for this mark. The US Patent & Trademark Office and other "Official" Trademark Offices throughout the world will NOT correspond directly with you.

B. How Long to Maintain Registrations

As companies evolve, they adopt new trademarks, slogans, and marketing symbols while letting others lapse. A company may want to review its domain name portfolio and determine what are still active and valuable. Periodic culling of the portfolio may help keep maintenance expenses in check. But companies should resist the urge to jettison domain names too quickly even if they are not in the company's current advertising plans. Maintaining domain name registrations that may still be identified with the company or block third party adopters should be part of a company's overall strategy. Like trademarks, the maintenance of

any single domain name registration is relatively inexpensive. Decisions about maintenance of domain names should be aligned with protection of the associated trademark.

One thing that many companies do to maintain rights in both their domain name registrations and their trademarks is to build history pages on their websites. These history pages help to show continued use in commerce of their legacy marks. Continued use may help to prevent others from claiming that the older marks are abandoned, provide long continuous use priority, and add value to a trademark portfolio. A legacy domain name can direct traffic to a current site.

It is also important to keep a record of the original launch date and advertising examples for each trademark and domain name. This is particularly useful in policing infringements or if a company prepares for a sale or participates in due diligence such as for a financing.

The brand owner should docket dates for renewal of the domain name renewals in its portfolio, and provide timely renewal instructions to the registrar or service provider who deals with the registrar. Then-current account access credentials will be needed at the time of renewal, so the brand owner should have obtained any access credentials from service providers or employees by the time of renewal. Some companies choose to avoid the administration costs and risks of what could be annual or bi-annual renewals of domain names by selecting and paying for longer term registration at the outset (e.g., 10 years) or setting up auto-renewals that will take place unless the company provides contrary instructions.

IV. OWNERSHIP / CONTROL ISSUES WITH EMPLOYEES AND VENDORS

Many companies include domain name registration among the services that they outsource to advertising agencies, brand developers, and webhosting providers. Others have an employee in the marketing department keep track as they roll out new domain names for new initiatives. It is crucial that the company direct that all domain name registrations be made in the brand owner's name, and check periodically to ensure that those instructions are being followed. Further, the brand owner should request and obtain the access credentials to control all domain registrations and accounts, such as the user name and password.

If a dispute arises with the service provider or employee that obtained the registration and retained control of the domain name, the brand owner that failed to enforce such policies can be left at a serious disadvantage. The typical example occurs when an employee of the service provider or of the company registered the domain name in their personal name and leaves the company. Disputes may arise about who was really intended to own the domain name, and the evidence does not always point conclusively to the owner of the brand. Where questions are raised about who the parties intended as the owner of the domain names, it can be a difficult and expensive process to untangle that intention and for the company to win ownership of what it believes always were its domain names.

Remember also that there may be copyright protection associated with a domain name, such as copyright in the website content or in advertising materials that reference the domain name. Trademark rights spring upon use and are used to identify the source of a good or service. However, copyright belongs to the author of the work and exists upon creation. It is important that the brand owner obtain assignments of copyright in any ancillary materials that include the domain name. Copyright assignments generally must be in writing, and must be

obtained from any author that is not an employee working within the scope of their employment responsibilities.⁶⁵

V. FRANCHISE SPECIFIC CONCERNS

Between a franchisor and a franchisee, who should register and own the domain name? It may seem obvious that because franchisors own their brands, they should therefore own and control their brands' online presence through domain names. However, when franchisors seek to control the domain name and brand, tension can arise with franchisees. Franchisees often want to be able to add their own personal touch, by running location-specific sites and events, and sharing local news and highlights. This can be problematic in the context of both franchisee-run websites as well as social media names and pages. Regardless, a franchisor should always own the domain registration, but it is possible to allow franchisees some creative control.

However, a franchisor that decides to allow franchisees to control their own webpages or create local-specific content has several issues to manage. First, the franchisor must provide proper training and oversight to be sure that the franchisees are adhering to brand guidelines, following legal requirements for advertising, avoiding unauthorized uses of images or photos of customers, and otherwise acting consistent with the franchise system requirements. In addition, franchisors must ensure that they have current credentials and access to the website, webpage and domain name registrations used by franchisees in the event of a dispute with the franchisee, receipt of a takedown notice, or other controversy. The exact amount of control a franchisor should permit a franchisee in regard to their online presence depends on balancing these issues with the potential disgruntlement of franchisees that feel they cannot properly advertise their locations.

VI. HOW TO OBTAIN DESIRED DOMAIN NAMES

A. Offers / Negotiations

Typically when a company starts to develop a new brand, it checks whether a preferred gTLD, such as .com, is available for use with their mark as a second level domain. Many companies decide that if they cannot acquire the desired domain name without too much difficulty (as discussed below), then they will select another name for the brand.

Let's assume that Company B, has selected EXAMPLE as its new brand, and therefore seeks ownership of example.com. However, that domain name is already taken and is owned by someone else. Company B may wish it had the means to force the existing owner to transfer rights in the example.com domain name to it. However, the definitions of cybersquatting and the causes of action against cybersquatters under the UDRP and ACPA do not include a scenario where the domain name existed prior to the company's selection of the brand (except under narrow circumstances). This is the case even if the prior domain name registrant is not actively using the domain name for a website or business. Generally domain names are allocated on a first-come, first-served basis. Further, under these facts the registrant did not register or use the domain name in a manner to profit from Company B's brand, as the brand only came into existence after the registrant obtained the domain name.

⁶⁵ *Community for Creative Non-Violence v. Reid*, 490 U.S. 730 (1989).

If Company B still wanted to use EXAMPLE as its mark, then it could try to purchase the domain name from the registrant. Domain names may be bought and sold between parties, so Company B may be able to acquire the domain name from the registrant. Company B could consider any of the following strategies.

a. Many domain names may already be offered for sale if they were acquired for speculation (which arises when a registrant does not use or plan to use the domain name for its own business, but hopes to receive a payment for sale of the domain name that is larger than the registration and maintenance fees paid). The WHOIS record or any webpage related to the domain name may post a notice stating that the domain name is for sale, and may even give the asking price. Such an offer to sell surmounts what is usually the first hurdle, which is persuading the registrant to be interested in negotiating a sale. Some registrants that intend to use and maintain the domain name will just say "no" to an initial approach requesting a sale.

b. If there is no rush, or the domain name is due to expire shortly, Company B could place a "backorder" to try and pick up the domain name if the current registrant fails to renew it. When domain name registrations are not renewed, after a grace period they are returned to the general status of domain name availability on a first-come, first-served basis. An interested party may use a backorder service to request the opportunity to register the domain name as soon as it becomes available. However, since several companies may also place a backorder on the same domain name, Company B might not be first in line to acquire the domain name if and when it expires. If the domain name does become available and Company B's backorder is the first in line, Company B will receive a notification and an opportunity to register the domain name. From the other perspective, if the current domain name registrant is concerned about losing its domain name through failure to timely renew may choose to put the domain name on "autorenew" so each renewal automatically takes place with no need for the registrant or its representative to intervene.

c. Many companies do not want to wait for a domain name to become available, and prefer to make an offer to purchase the domain name from the registrant, for domain names that are not offered for sale publicly. Companies often prefer making an anonymous offer to avoid the risk that the registrant increases the asking price based on the offeror's identity. For the cheapest and fastest approach, several vendors offer online services to make anonymous offers to acquire a domain name. These services tend to be electronic only, whereby the offeror completes a webform with the domain name and the offer amount. The anonymous offer is then sent to the owner indicated in the WHOIS record. The registrant may reply to accept, reject, or make a counter offer. The registrant of course could just ignore the offer, which due to the limited form of communication available using these services, leaves the interested party high and dry. Company B might, for example, make a low-ball offer through an anonymous offering service as a first step. The service enables counter-offers to be exchanged. If the parties reach an agreement, the service facilitates the transfer process (and collects a fee).

d. Another course of action, if anonymity is important, is to have Company B's attorney (without disclosing the client) or a designated employee (using a private account or number) reach out to the registrant and make an offer by any available method of correspondence. This communication creates the opportunity for more communication than an anonymous offering service. However, if the attorney or employee is closely associated with the client (e.g., counsel of record on filings for the trademark involved or other prominent trademarks), then they may not provide the anonymity desired.

e. Another approach for Company B to conceal its identity when making an offer to purchase a domain name is to use an investigator or other vendor with experience negotiating domain name acquisitions. A sophisticated broker service may set up a temporary shell company to acquire the domain so the seller would not know the real party in interest until the transaction is completed. After transfer of the domain name to the shell company, the investigator or vendor would have the shell company further transfer the domain name to Company B. This is the most sophisticated (and often the most expensive) method.

These activities can get more interesting when the domain name registrant holds the domain name in high value. If the registrant demands a steep price, or perhaps Company B finds itself in a bidding war for the domain name, then Company B may want to consider obtaining a valuation of the domain name. Expert appraisals are available, based on comparables, business plans and the like, often for a substantial price. Online appraisal services also are available, many offering a free service based on comparables. Because each domain name is unique and may have special value to the registrant or offeror, the only true valuation may be the number that results from the parties' negotiation. Rule of thumb: .com domain names with second level domains that are short, easy to spell and easy to remember, garner the highest prices.

The mechanics of transferring a domain name depend on the registrar's terms. Frequently the transfer follows these steps:

- ▶ Registrant places the domain name to be transferred into a separate account with the registrar.
- ▶ Registrant gives Buyer access credentials to that account.
- ▶ Buyer accesses the account and changes the access credentials, thus taking control over the domain name in the account.
- ▶ Buyer then can update the WHOIS record to reflect Buyer as the owner of the domain name.
- ▶ Often Buyer will move the domain name to a different registrar handling the remainder of Buyer's domain name portfolio.

B. Sales of Domain Name Portfolios

In addition to stand-alone transactions involving a single domain name, large numbers of domain names maybe be acquired at one time, perhaps as a stand-alone portfolio of domain names or included with other assets in larger transactions such as mergers and acquisitions or financings. When domain names are a stand-alone portfolio, buyers typically consider the viability of using or reselling domain names, taking into account whether claims of cybersquatting may be made against use of the domain names.

When a domain portfolio is part of a body of assets in a transaction, the domain names often are overlooked or under-reviewed during due diligence. Yet they might represent a valuable asset, either from objective value or due to their use and recognition in connection with the target's business. In short, when reviewing a portfolio of intellectual property, the acquiring company should be sure to check that domain names are included, and that the record owner of the domain names is a seller in the transactions. While social media names are outside the

scope of this paper, note that social media names also may be transferred (depending on the terms posted by the platform), and should be subject to similar due diligence and contractual provisions.

A due diligence checklist might include the following with respect to domain names:

<u>Due Diligence Topic</u>	<u>Description</u>	<u>Notes</u>
List of domain names involved in the transaction	Identify registrar, date of registration, expiration or renewal date, status, owner and administrative contact for each domain name	Check the WHOIS record for each domain name individually to confirm or correct the information to the extent it is publicly available. Require the assignor to correct the WHOIS records or transaction documents to align ownership of the domain names with the seller in the transaction.
Check for similar domain names	Ask target to confirm that the assignor does not own a closely similar domain name that is not on the list of domains to be assigned; consider possible similar or related domains and check them in the WHOIS records	No resource is generally available to the public where a domain name buyer or other third party can look up all domain names owned by a registrant. "Bulk searching" of domain names is possible, but complicated. A vendor would need to be granted access to the WHOIS database at the root zone level, and then develop software to connect to the database and navigate the different formats, throttling and parsing. For this reason, most buyers must due diligence production and contractual language to ensure that all relevant domain names are included in the transfer.
Trademark registrations	Check to see if the target (or others) own trademark registrations for the second level domains, and evaluate potential impact of those trademark rights on the domain names. Check ownership of the trademark registrations to compare to	

	seller in the domain name transaction	
Access credentials	Location and availability of keys to each registrar account, all usernames and passwords needed to transfer	
Opinions and valuations	Evaluating availability of domain name and possible cybersquatting, trademark infringement, or other exposure for use of any domain name	
Chain of title	Any transfers, bankruptcy outcomes, chain of title opinion letters, joint ownership agreements, agreements to sell	
Licenses	Any licenses, authorizations, permissions, use agreements, royalty agreements, agreements to license,	
Encumbrances	Any security interest, collateral assignment, lien or other encumbrance on any domain name; any UCC-1 filings; any security interest or collateral assignment recorded against any trademark registration for the second level domain	There is no provision for recordation of security interests in domain names through the WHOIS database. Domain names probably fall within general intangibles under the UCC.
Threats and Disputes	Any objections, demands, threats or actions alleging cybersquatting, trademark infringement, unfair competition, false advertising, breach of contract, or any other proceedings (including alternative dispute resolution) concerning any domain name in any jurisdiction or tribunal; any consent agreements or settlement agreements	
Sunrise / Blocking	Any domain names for which there is a sunrise (early filing rights) or blocking request (blocking others from registering) filed with any registrar	

Below are a few sample contractual provisions of the type used in formal domain name assignment agreements (depending on the facts):

Title	Clause
Grant	Assignor hereby sells, assigns and transfers to Assignee all right, title and interest in, to and under the Domain Name and the registration thereof through any registrar; any trademark rights owned by Assignor in connection with the Domain Name anywhere in the world, and any goodwill symbolized by and associated therewith; and any other rights relating to the foregoing, for Assignee's own use and behalf, and for the use and behalf of its successors, assigns or other legal representatives, as fully and entirely as the same would have been held and enjoyed by Assignor if this assignment and sale had not been made; together with all income, royalties, fees and payments now or hereafter due or payable in respect of the foregoing, and the right to file any action and recover damages by reason of infringement, misappropriation or other unauthorized use of the foregoing, with the right to sue for, and collect same for its own use and behalf, and for the use and behalf of its successors, assigns, or other legal representatives.
Steps to Transfer	Within five (5) days following the execution of this Assignment, Assignor shall follow the requirements of the applicable registrar for the Domain Name to carry out transfer of the Domain Name to Assignee, and/or shall instruct the registrar to transfer the Domain Name to Assignee, and/or shall cooperate with Assignee to accomplish assignment of the Domain Name to Assignee such as by providing the usernames, passwords or codes for Assignee to access and control the account for the domain name, and/or otherwise shall cooperate with Assignee to accomplish ownership by Assignee of the domain names. Assignor and Assignee shall execute such further documents and take such further steps as may be required to carry out the transfer of the Domain Name to Assignee as registrant in the registration records maintained by the applicable registrar.
Consideration	In full consideration of the assignment to Assignee of Assignor's rights in the Domain Name and any related trademark rights and goodwill or other rights relating to the foregoing, Assignor shall pay Assignee the sum of _____ Dollars (\$____.00), payable as follows. Promptly following receipt by Assignee of control of the Domain Name, including the capacity to change the ownership details in the registrar's WHOIS database, Assignee shall forward to Assignor a check payable _____ in the amount of _____ Dollars (\$____.00) by wire transfer of immediately available funds pursuant to instructions provided by Assignee.
Representations and Warranties	Assignor represents and warrants that: - it has the full legal power and authority to grant this Assignment and to fully perform all of its obligations hereunder, without any limitations or restrictions whatsoever; - it is the owner of all rights in the Domain Name being conveyed hereunder; - it has the right to assign the Domain Name and any related trademark rights and goodwill or other rights relating to the

	foregoing, free and clear of any conflicting agreements, security interests, liens, charges or encumbrances; - it does not hold any domain names, trademarks or trademark applications other than the Domain Name that incorporate the term "_____" any variation thereof; - there is no claim or threatened claim or basis for any claim that the Domain Name infringes or misappropriates any third party rights, or that Assignor has engaged or is engaged in any cybersquatting or bad faith in acquiring, using or transferring the Domain Names; - the execution and delivery of this Assignment Agreement, the consummation of the transactions as herein contemplated and the carrying out by Assignor of its obligations hereunder will not contravene or constitute a default under any provision of applicable law or regulation, or violate or constitute a default under any material agreement, commitment, judgment, order or other instrument binding upon or relating to Assignor; - no consent, approval or other authorization of or filing with any individual, corporation, partnership, trust or unincorporated organization or any government or an agency or political subdivision thereof, or any other person or entity is required for the valid execution, delivery and performance of this Assignment Agreement by Assignor and the consummation by Assignor of the transactions contemplated hereby; - upon such transfer, Assignee shall be the owner of the Domain Name, and any related trademark rights and goodwill or other rights relating to the foregoing, free and clear of all security interests, liens, claims and encumbrances.
Further conduct of Assignor	Upon execution of this Assignment, and except as required under this Assignment to enable Assignor to transfer its rights in the Domain Name and any related trademark rights and goodwill or other rights relating to the foregoing, to Assignee as provided herein, Assignor shall not retain any right to use or register the Domain Name, or any variation thereof, or any other rights transferred as provided hereunder, and shall not use or register, nor authorize others to use or register, the Domain Name, the term "_____" or any variation thereof, in any manner, including without limitation as a metatag, marketing keyword or adword, social media name or handle, or any other reference thereto.
Further Assurances	Assignor hereby agrees that it will, at any time upon request, without further compensation, execute, acknowledge and deliver any and all documents, instruments and agreements that in the reasonable opinion of Assignee may be necessary or appropriate to secure to Assignee the full right, title and interest in, to and under the Domain Name and any related trademark rights and goodwill or other rights relating to the foregoing, and the rights, privileges, benefits and goodwill associated therewith.
Wind-down Period	For and during the Wind Down Period only, Assignee grants to Assignor the non-exclusive, non-transferable, royalty-free right and license (without the right to grant sublicenses) to use the

	Domain Name only resolve to the website known as _____ [add limitations]. At the conclusion of the Wind Down Period, it shall be a violation of this Assignment Agreement for Assignor to use any corporate name, trademark, trade name, fictitious business name, tag line, domain name, social media name or other name that is confusingly similar to the Domain Name or any related trademark rights.
--	---

VII. POLICING OF DOMAIN NAMES

A. Trademark Evaluation

It may be helpful to think of domain names as an extension of any trademark rights in the second level, and to treat domain names similarly to how trademarks are handled for policing purposes. Domain name registrants are advised to keep an eye on new domain names as they become registered or used, so the registrant can protect its trademark rights by seeking to prevent confusingly similar uses.

Trademark services vendors that provide "watch services" for trademarks also provide such services for domain names. A watch service can alert a trademark or domain name owner about new registrations or uses of domain names that may be of concern. Company employees and service providers also should be asked to bring any confusing or questionable domain names or websites to the attention of a designated person (often the trademark or intellectual property counsel) at the company.

Once learning of a problematic domain name, the trademark or domain name owner should evaluate the domain name and any related website for evidence of cybersquatting, trademark infringement, copyright infringement (spoofing sites), false advertising, phishing, or other torts or objectionable activity, as well as possible bases for legitimate use of the domain name. If the trademark owner decides to proceed, the trademark owner may choose to send a cease and desist letter to the registrant to attempt an informal resolution, or directly file a UDRP or ACPA proceeding (or action for trademark infringement, unfair competition, false advertising, etc.). The registrant might be contacted at the address provided in the WHOIS record, or at an address provided in any website available at the domain name or located through other investigation.

B. Problems with WHOIS Registries

Evaluation of the ownership of domain names at issue in policing efforts may be stymied by the WHOIS record, which is the very place that ownership information has been available to the public in ICANN's effort to make the domain name system transparent.

1. Privacy Shields

Domain name registrants may choose to place ownership information in the WHOIS record under a privacy shield. Privacy shields have become widely used, often by domain name registrants that register or use the domain name for illegitimate purposes. When the registrant's name and contact information are not available, it is more difficult for a trademark owner who believes its rights may be infringed or that cybersquatting is taking place to assess whether the domain name registrant has a legitimate right to use the domain name or whether the domain name was registered or is being used in bad faith.

If the WHOIS information is under a privacy shield, any demand letter can be addressed to the service offering the privacy shield, and that service is supposed to forward the demand letter to the domain name registrant for response. Some privacy shield services will respond by providing WHOIS information for the registrant. However, if neither the privacy shield service nor the registrant responds, the trademark owner may not know whether the failure is with the privacy shield service or the registrant.

If the trademark owner has enough confidence that cybersquatting has occurred without knowing the identity or contact information of the registrant, the trademark owner can proceed by filing a cybersquatting action naming the privacy shield service as the registrant. Upon receipt of a complaint, the registrar for the domain name must reveal the ownership information for the domain name registrant.

2. WHOIS Blackout

Recent changes to the European privacy regulations, known as the European Global Data Privacy Regulation ("GDPR"), which went into effect May 25, 2018, added new restrictions about consent to collection, use and disclosure of personal data. This effort to protect the privacy of European Union "data subjects" (defined as identifiable persons, or persons capable of being identified) has created a major problem for the WHOIS database.

The ownership fields in WHOIS records include, among other things, the name and contact information of the registrant and its administrative and technical contacts. The contact information may contain the personal data of individual registrants, or of administrative and technical contacts for the registrant. GDPR provides, among other things, that EU data subjects may not be required to provide personal data as a condition to receipt of services -- and providing WHOIS information is a condition of obtaining a domain name registration.

When the effective date of GDPR approached, ICANN, and a working group of the Internet community tried to reach a position on application of GDPR to the WHOIS database, with input from representatives of brand owners, and reaching out to the Data Protection Authorities of the EU member states. But efforts to reach a compromise collapsed.

As of May 25, 2018, ICANN's interim solution, known as the Temporary Specification for gTLD Registration Data⁶⁶, was that the publicly available WHOIS data would be limited to the registered domain name, registrant's organization if any, registrant's state or province and country, and an anonymous email address or web form to which an email could be forwarded. (Domain name registrants are required to provide contact information that is not made publicly available, but the accuracy of the contact information has not been checked or verified.)⁶⁷ This interim solution, dubbed the "WHOIS Blackout," has been applied universally to entire WHOIS directory for gTLDs, not just registrants with addresses in the EU, although GDPR is limited to the EU. Further, the interim solution does not distinguish between natural persons (individuals) and entities, although GDPR only protects the personal data of individuals. In addition, the interim solution was applied to the entire existing WHOIS database, not only to new domain name registration information following implementation of GDPR. The interim solution is expected to remain in place for one to two years.

⁶⁶ <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>.

⁶⁷ *Id.*

The interim solution does not necessarily apply to ccTLDs, which are managed by each country code registry operator or "NIC" (Network Information Center), and each operator makes its own decisions including how to respond to GDPR.

Under the interim solution, requests for the contact information of domain name registrants may be submitted to the relevant registrar. The registrar has two options. It may assess the request to determine whether it is legitimate, and release the WHOIS information for requests found legitimate. A legitimate request might be, for example, a claim of trademark infringement with supporting evidence such as a trademark registration. However, registrars operate efficiently and economically through use of automated systems, and it would be difficult to automate a legitimacy assessment. The registrar's other option is to forward the request to the registrant and allow the registrant to decide whether to agree to release its contact information to the requestor. Some would say that places too much control in the hands of the registrant and defeats the intended transparency of the domain name system.

Following the interim solution, ICANN now plans to offer a tiered access model. Essentially ICANN would accredit certain parties (e.g., registers and registrars) as authorized to receive and assess legitimacy of requests for WHOIS information. It is expected that the assessment will be conducted in an automated fashion. WHOIS contact information would be provided in response to requests determined to be legitimate.

The practical impact of ICANN's response to GDPR will be more cybersquatting proceedings under ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP"), and fewer opportunities to avoid or resolve domain name disputes without filing proceedings. Complainants in UDRP actions or plaintiffs in court actions will be frustrated by the additional delay of going through registrars to get information identifying registrants. Investigations by potential complainants in UDRP actions or plaintiffs in court actions will be hampered due to the decreased access to information. Situations where the WHOIS information might indicate a legitimate use or an issue capable of informal resolution between the parties will be obscured by the lack of information (which also may occur when a privacy shield is involved). Requestors would become adverse to the registrars holding the registrant's information. Filing a UDRP proceeding will be the most direct way to get contact information for domain name registrants, and to avoid depending on a registrar to assess the legitimacy of a request or seeking a subpoena or other ruling from a court.

C. Cybersquatting Proceedings

Cybersquatting is, generally, the registration and use of a domain name that causes confusion with a trademark, where the domain name is not used for legitimate purposes and is used in bad faith to profit or otherwise benefit from the connection to the trademark. There are two main avenues to bring cybersquatting proceedings: the Uniform Domain-Name Dispute-Resolution Policy (UDRP) propounded by ICANN,⁶⁸ and administered by the World Intellectual Property Organization ("WIPO") Arbitration and Mediation Service⁶⁹; and the United States federal Anti-Cybersquatting Consumer Protection Act (ACPA),⁷⁰ Both were adopted in 1999, so there is nearly twenty years of history and precedent for both.

⁶⁸ <https://www.icann.org/resources/pages/help/dndr/udrp-en>.

⁶⁹ <http://www.wipo.int/amc/en/domains/>.

⁷⁰ 15 U.S.C. §1125(d).

1. UDRP

To summarize, the UDRP is an extrajudicial procedure that uses ICANN's control over the domain name system to enable "arbitration" before a panel of arbitrators who decide whether cybersquatting has occurred with regard to domain names using gTLDs. If cybersquatting is found, the panel decides whether to cancel the disputed domain name or transfer it to the trademark owner (a "Complainant"). UDRP proceedings are entirely online, with the only pleadings being a complaint and response, with exhibits, that are considered by the panel of specialists in the area⁷¹ who are paid a small amount to decide cases. There is no provision for a reply brief, no examination of witnesses, no live testimony, and no monetary relief. The available relief is transfer of the domain name to the complainant, cancel the domain name registration, or leave the domain name in the ownership of the respondent.

The cost for filing a UDRP action is relatively low (\$1,500 fee for a single panelist; \$4,000 fee for three panelists) and decisions typically are issued within 75 days of filing. While the UDRP does not provide for appeals, either party may elect to bring the dispute to court. If a UDRP decision is not brought to a court within ten days after issuance, the decision will be final and the relief will be implemented.

Unlike other areas of the law, the UDRP has no statute of limitations. Also, panels deciding cybersquatting disputes under the UDRP generally do not reject complaints for laches. But long delays can lead to circumstances that make it difficult to prove the necessary elements of a complaint.

Under the UDRP, complainants must show the following three elements of cybersquatting:

First Element: the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

Second Element: the domain name registrant has no rights or legitimate interests in respect of the domain name; and

Third Element: the domain name was registered and is used in bad faith.

a. First Element

Panels can assess confusing similarity by reference to national trademark laws. Panels generally agree that use of the complainant's mark with a generic term (e.g., *examplerestaurant.com*) or with a derogatory term (e.g., *examplesucks.com*) is considered confusingly similar. Panels also generally agree that a domain name that uses another's mark, but with a typo (e.g., *exmaple.com*) is confusingly similar.⁷²

⁷¹ Co-author Carol Anne Been is a panelist for WIPO, and has decided approximately 50 UDRP cases.

⁷² See, e.g., *Six Continents Hotels, Inc. v. Triptih DOO*, No. D2012-1600 (WIPO Oct. 12, 2012) (former franchisee/respondent's IT consultant registered domain name <holidaysarajevo.com> after termination of franchise agreement for "Holiday Inn Sarajevo"; panel rejected argument that "holiday" is descriptive, and in this context found "Holiday Sarajevo" confusingly similar to "Holiday Inn Sarajevo").

b. Second Element

The UDRP provides instructions on how a domain name registrant may demonstrate rights to and legitimate interests in the domain name, including any of the following circumstances:

(i) before any notice of the dispute, the registrant used, or made demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) the registrant (as an individual, business, or other organization) has been commonly known by the domain name, even if the registrant acquired no trademark or service mark rights; or

(iii) the registrant makes a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

In practice, many respondents default, so panels are faced with deciding legitimate interest without arguments or evidence provided by the respondent. Panels generally have held that a complainant must make *prima facie* case, and then the burden shifts to the registrant to rebut the *prima facie* case. Many decisions note that if the registrant had a legitimate basis to use the domain name, it should have filed a response and so informed the panel; but in the absence of the registrant taking that opportunity, the panel may assume the registrant has no legitimate use or rights.

When a reseller, distributor or service provider adopts a domain name that uses the trademark of the manufacturer or principal, many panels take the position that the reseller, distributor or service provider may have legitimate rights to use the domain name, if domain name and site are used carefully in a manner to avoid confusion with the manufacturer or principal, and further if an agreement prohibits registration and use of the manufacturer's or principal's mark in a domain name.⁷³ This analysis has not generally been extended to franchise cases, where the third element of bad faith use and registration is more often determinative.⁷⁴

Legitimate use may arise even without consent of the trademark owner, if the use involves free speech concerns or the concept of fair use for trademarks. For example, panels generally hold that a criticism site (e.g., examplesucks.com) or a fan site (e.g., iloveexample.com) is a legitimate use if the website hosts legitimate criticism or fan activity, is

⁷³ See, WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition (WIPO Overview 3.0), Section 2.8.1, <http://www.wipo.int/amc/en/domains/search/overview3.0/#item21>.

⁷⁴ Cf. *Cash Converters Pty Ltd. v. Casheez Pty Ltd.*, No. DAU2011-0029 (WIPO Nov. 30, 2011) (denying UDRP complaint based on respondent's legitimate interest because respondent had used domain name well before complaint filed; held insufficient evidence to determine whether franchise agreement was enforceable or breached, which might have changed the analysis of legitimate use); *Clockwork IP, LLC, One Hour Air Conditioning Franchising, LLC v. Wallace*, No. D2009-0485 (WIPO June 1, 2009) (respondent used One Hour before complainant; facts of dispute more appropriate for a court; complainant failed to carry its burden).

clearly delineated from the trademark owner, and makes no commercial use under the mark (e.g., selling t-shirts or buttons).⁷⁵

However, a criticism site that uses the trademark without an additional word suggesting criticism (e.g., example.com) more often might not be considered a legitimate use depending on circumstances (especially outside the United States) because the trademark owner is considered to be entitled to own that domain name.

c. Third Element

With regard to registration of the domain name, questions periodically arise concerning when registration of the domain name took place. In most cases, the domain name was registered after adoption of the mark, so it is easier to show that the domain name registrant was aware of the mark before registering the domain name. In the United States, trademark owners often rely on the constructive notice provision of the Lanham Act, stating that a federal trademark registration provides constructive notice of the trademark owner's national rights.⁷⁶

In some cases where the domain name was registered before the mark was adopted, the circumstances have shown that the registration was in reaction to a public report or announcement that the mark would be adopted in the future.

In addition, in unusual circumstances, panels have found bad faith even when the domain name was registered *before* the mark was adopted, so the registrant could not possibly have been aware of the mark when the domain name was registered. These cases turn on the facts. In one such case, *Milly LLC v. Domain Admin, Mrs. Jello LLC*,⁷⁷ the panel found bad faith in the domain name registrant's change in website content to allude to complainant's later-adopted mark as sufficient to show registration in bad faith. The fact that the domain name registrant could not have had bad faith in registering the domain name did not preclude a finding of bad faith under the circumstances present.⁷⁸

With regard to use of a domain name, the panel decisions generally look to the totality of circumstances in assessing whether the domain name is in use. Some decisions have found use of a domain name for a link farm (a landing page with links to other sites, for which the domain name owner likely is paid per click ("PPC") for consumers who click through to those sites), for an email address using the domain name to conduct phishing (the fraudulent practice of sending emails purporting to be from a reputable source to induce individuals to reveal personal information, such as passwords and credit card numbers, that the sender can monetize), or for misrepresenting the identity of the registrant in WHOIS record. Some panels have even found passive holding/parking of a domain name alone (with no commercial use) is enough to show use to satisfy the bad faith element.

⁷⁵ Cf. *Line-X LLC v. Perfect Privacy, LLC / Jason Nelson*, No. D2018-1288 (Aug. 7, 2018) (domain name lead to site purporting to be forum for complainant's franchisees operated by franchisees as "Line-X Owners Group"; franchise agreement barred registration of domain names with complainant's mark; respondent defaulted; panel held reference to "owners" could falsely suggest complainant authorized domain name and site, showing bad faith).

⁷⁶ 15 U.S.C. § 1072.

⁷⁷ No. D2014-0377 (WIPO May 25, 2014). Co-author Carol Anne Been represented Complainant Milly LLC in this UDRP proceeding.

⁷⁸ See, WIPO Overview 3.0, Section 3.8.

The posting of a disclaimer on the website at the domain name (e.g., This Site is Not Affiliated with Example Brand Owner) usually is not found sufficient by itself to negate a finding of bad faith use of the domain name.⁷⁹ Some of these decisions may rely on the United States trademark cases that recognized trademark infringement based on "initial interest confusion."⁸⁰

With regard to assessment of bad faith based on the conduct of the domain name registrant, the UDRP lists four non-exclusive factors that may show bad faith.⁸¹ The most common factor asserted is that by using the domain name, the registrant intentionally attempts to attract, for commercial gain, Internet users to its website by creating a likelihood of confusion with the complainant's mark.

Several cybersquatting cases involving franchisees as respondents turn on whether registration or use of the domain name was in bad faith. For example, the following cases held registration and use of the domain name were in bad faith: *Thrifty Rent-A-Car Systems, LLC v. Thrifty Morocco*,⁸² (respondent registered and used domain name during franchise relationship, where franchise agreement provided that respondent "shall not register or otherwise use any domain name ... that includes the Marks or any portion thereof"); *Monotag Corp, DBA Signs First v. Byrd*,⁸³ (respondent registered and used domain name during franchise relationship, but no evidence that the franchise agreement barred domain name registration); *Six Continents Hotels, Inc. v. Triptih DOO*,⁸⁴ (former franchisee's IT consultant registered domain name after termination); *RE/MAX Int'l Inc. v. NCR Northcoast Realty*,⁸⁵ (if franchisee controlled respondent, then it acquired domain name during franchise agreement in violation of franchisor's trademark standards; if respondent acquired domain name from franchisee that did not control it, then acquisition of domain name after termination of franchise was treated as registration in bad faith); *Herbalife Int'l of America, Inc. v. myherbalife.com*,⁸⁶ (respondent registered domain name while an independent distributor of complainant's products, under "Internet Guidelines" that prohibited use of complainant's marks in the distributor's domain name; bad faith registration and use shown by breach of agreement and request for compensation to transfer domain name).

As additional examples, the following cases did not find bad faith in the franchisee's or distributor's registration and/or use of the domain name: *Damon's Restaurants, Inc. v. JBR Enterprises, Inc.*,⁸⁷ (respondent was web designer for terminated franchisee; domain names were registered and used during franchise relationship, but other franchisees also owned

⁷⁹ WIPO Overview 3.0, Sections 3.1.4, 3.2.2, 3.6.

⁸⁰ See, e.g., *Brookfield Comm., Inc. v. West Coast Entertainment Corp.*, 174 F.3d 1036 (9th Cir. 1999).

⁸¹ See, Exhibit A, Supplemental Materials on "What Is Bad Faith", provided with this article.

⁸² No. D2017-2061 (WIPO Dec. 20, 2017).

⁸³ No. D2001-0561 (WIPO July 19, 2001).

⁸⁴ No. D2012-1600 (WIPO Oct. 12, 2012).

⁸⁵ No. FA0906001266756 (Nat. Arb. Forum Aug. 4, 2009).

⁸⁶ No. D2002-0101 (WIPO April 13, 2002).

⁸⁷ No. D2007-1603 (WIPO Feb. 14, 2008).

domain names with complainant's mark, no evidence franchise agreement barred use of complainant's marks in domain names nor of complainant policing other franchisees for such use; respondent stopped using domain names upon notice from complainant); *Celebrity Signatures Int'l, Inc. v. Hera's Incorporated Isis Linder*,⁸⁸ (respondent was distributor of complainant's products with no distribution agreement or bar on registering domain name with complainant's mark); *Urbani Tartufi S.N.C. v. Urbani U.S.A.*,⁸⁹ (respondent was related to distributor of complainant's products; complainant consented to domain name at the time of registration).

d. Outcomes of UDRP Proceedings

Approximately 85% or more UDRP cases are decided for the complainant.⁹⁰ In many cases, the registrant has defaulted. Even when the registrant defaults, the complainant still bears the burden to establish all three elements.⁹¹ However, panels have drawn inferences from a respondent's default where the respondent did not take the opportunity to provide contrary evidence or argument in response to the claims, and no conclusion other than cybersquatting seems plausible.⁹²

e. Reverse Domain Name Hijacking

Lest complainants become overzealous in bringing cybersquatting actions that are not well founded, the UDRP also includes a provision to identify reverse domain name hijacking ("RDNH").⁹³ RDNH may arise when a trademark owner asserts cybersquatting in bad faith. A panel may rule that RDNH took place, to protect a domain name owner with legitimate rights. No further consequences apply to the complainant other than the finding of RDNH and a declaration in the decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.⁹⁴

2. Dispute Resolution for ccTLDs

The UDRP was designed for gTLDs. The governing bodies for ccTLDs (a Network Information Service or "NIC") for each ccTLD decides what dispute resolution procedure will apply. Around 75 ccTLDs have adopted the UDRP⁹⁵, including .eu (European Union)⁹⁶, .mx (Mexico)⁹⁷, and .br (Brazil).⁹⁸

⁸⁸ No. D2002-0936 (WIPO Dec. 16, 2002).

⁸⁹ No. D2003-0090 (WIPO April 7, 2003).

⁹⁰ Analysis of WIPO Domain Name Dispute Resolution Statistics, <http://www.wipo.int/amc/en/domains/statistics/>.

⁹¹ See, WIPO Overview 3.0 Section 4.1

⁹² *Id.*

⁹³ See, Rules for Uniform Domain Name Dispute Resolution Policy (promulgated by ICANN) Rule 15(e).

⁹⁴ *Id.*

⁹⁵ <http://www.wipo.int/amc/en/domains/ccTld>.

Other ccTLDs have adopted their own dispute resolution policies and procedures, some of which may be based on some of the UDRP concepts:

<u>ccTLD</u>	<u>Authority and Service</u>	<u>Notes</u>
.uk (United Kingdom) https://www.nominet.uk	Nominet registry uses its Dispute Resolution Service ("DRS")	Includes an appeal process
.ca (Canada) https://cira.ca	Canadian Internet Registration Authority ("CIRA") uses the CIRA Dispute Resolution Policy ("CDRP")	Canadian Presence Requirements
.cn (China) https://www.cnnic.net.cn	China Internet Network Information Center ("CNNIC") uses the China Dispute Resolution Policy ("CDRP")	Two year time limit from registration of target domain name to bring proceeding under CDRP

3. ACPA

The Anti-Cybersquatting Consumer Protection Act (ACPA)⁹⁹, is a section of the US federal trademark law known as the Lanham Act. The ACPA creates a special cybersquatting cause of action that is subject to federal court jurisdiction. As with other federal court cases, ACPA proceedings involve multiple pleadings and motions before a federal judge, under federal court procedures, with live examination of witnesses and introduction of evidence. Additional counts for trademark infringement, dilution, false advertising, and the like may be brought together with an ACPA action. Available relief includes cancelation or transfer of the domain name, plus other trademark remedies such as injunctions and monetary relief. The ACPA also provides for statutory (presumed) damages of \$1,000 to \$100,000, as the court deems just.¹⁰⁰ The cost and duration of ACPA cases is typical of federal court litigation. Appeals to a federal circuit courts of appeal are available.

Under the ACPA, plaintiffs must show the following two elements of cybersquatting:

First Element: The registrant has a bad faith intent to profit from use of the mark or personal name; and

Second Element: The registrant registers, traffics in or uses a domain name that is identical or confusingly similar to a protectable mark.

a. First Element

⁹⁶ <http://www.wipo.int/amc/en/domains/cctld/eu/index.html>, see also www.adr.eu (alternative dispute resolution also authorized by a Czech arbitration court).

⁹⁷ <http://www.wipo.int/amc/en/domains/cctld/mx/index.html>.

⁹⁸ <http://www.wipo.int/amc/en/domains/cctld/br/index.html>.

⁹⁹ 15 U.S.C. § 1125(d).

¹⁰⁰ 15 U.S.C. § 1117(d). See, e.g., *In re Gharbi*, No. 08-11023-CAG, 2011 WL 831706 (Bankr. W.D. Tex. Mar. 3, 2011), *aff'd*, No. A-11-CA-291 LY, 2011 WL 2181197 (W.D. Tex. June 3, 2011) (complainant sought \$100,000 per domain name, but court awarded \$25,000 each, holding conduct of defendant -- Century 21 franchisee -- was not bad enough to justify maximum damages).

The First Element under the ACPA states that the defendant has a bad faith intent to profit from the mark at issue. This element overlaps with the bad faith part of the Third Element under the UDRP.

The ACPA explains bad faith as follows:

(i) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to:

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c).

(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

15 U.S.C. § 1117(d)(1)(B).¹⁰¹ If the defendant did not act in bad faith, or had a reasonable belief that use was fair use or otherwise lawful, this element would not be met.

b. Second Element

This element overlaps with the "registered and is used" part of the Third Element under the UDRP, with two major differences. First, in addition to registration and use, the ACPA adds the notion of "trafficking" in a domain name. Trafficking includes sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.¹⁰² Second, this element lists the three actions concerning the domain name (registers, traffics in or uses) with a disjunctive ("or") rather than a conjunctive ("and"), so any one of these actions, alone, may support a claim of cybersquatting. This is unlike the third element of the UDRP, where the complainant must show that the registrant "registered and is using" the domain name in bad faith. Thus, in cases where only use in bad faith occurred, it may be advantageous for a brand owner to bring a cybersquatting action under the ACPA rather than the UDRP.¹⁰³

In addition, the Second Element of the ACPA includes the concept that the domain name must be identical or confusingly similar to the mark at issue, which must be distinctive at the time of registration of the domain name.¹⁰⁴ This element overlaps with the First Element of the UDRP, which requires that the domain name is identical or confusingly similar to a trademark in which the complainant has rights.

c. In Rem Actions

In rem civil actions against a domain name (rather than against the registrant of the domain name) are available under the ACPA if no personal jurisdiction over the defendant exists in the United States. The action must be filed in the judicial district where the domain name registrar, registry, or other domain name authority involved in the particular domain name is located. The court must find that the brand owner is not able to obtain personal jurisdiction over the registrant. Relief in an *in rem* action is limited to forfeiture, cancelation or transfer.¹⁰⁵

4. Trademark Owners Vote by Their Choice of Jurisdiction

Trademark owners have filed approximately 80-100 federal court complaints with ACPA counts annually since 2015.¹⁰⁶ Approximately 25 of those cases were based on *in rem* jurisdiction each year.¹⁰⁷

¹⁰¹ See, Exhibit A, Supplemental Materials on "What Is Bad Faith", provided with this article.

¹⁰² 15 U.S.C. § 1117(d)(1)(E).

¹⁰³ See, e.g., *In re Gharbi*, No. 08-11023-CAG, 2011 WL 831706 (Bankr. W.D. Tex. Mar. 3, 2011), *aff'd*, No. A-11-CA-291 LY, 2011 WL 2181197 (W.D. Tex. June 3, 2011) (Gharbi was Century 21 franchisee whose webhost owned domain names with Century 21 mark as permitted by franchise agreement; after Century 21 terminated franchise, Gharbi instructed webhost to redirect domain names to new sites; bad faith use only).

¹⁰⁴ 15 U.S.C. § 1117(d)(1)(A)(ii)(I).

¹⁰⁵ 15 U.S.C. § 1125(d)(2)(D).

¹⁰⁶ Analysis of Bloomberg Law, Federal Dockets, 1/1/2015 - 8/27/2017.

Approximately 3,000 UDRP complaints were filed in 2017, an all-time high.¹⁰⁸ Those cases addressed 6,370 domain names.¹⁰⁹ Seventy percent of the domain names used the .com gTLD.¹¹⁰

Of those 3,000 cases, approximately one-third (1,000) were filed by United States complainants who apparently chose the UDRP over the ACPA.¹¹¹ Ten-to-one United States complainants chose the UDRP. Looking at industry sectors, approximately one-third (1,000) of those cases were brought by complainants in the banking, fashion or IT fields. The filers of the most UDRP actions in 2017 were, in this order, Philip Morris (based in the United States); Michelin (based in France); and Electrolux (based in Sweden).¹¹²

VIII. FUTURE OF DOMAIN NAMES

A. What is on the Horizon?

Considering the robust usage of domain names for over 20 years, it is an appropriate time to review whether domain names are losing their luster.

One common complaint is that there are simply too many domain names, which can cause mistake and confusion. At this time there are over 1,500 TLDs, and by some estimates there are over 330 million domain names. Verisign Domain Name Industry Brief: Internet Grows to 330.6 million Domain Names in Q1 2017.¹¹³ While consumers may visit many sites on the Internet, they could only use or recognize a relatively small number of domain names. This vast number of domain names provides a mind-boggling array of choices to remember, and of opportunities for typing or clicking on an unintended domain name.

The most familiar and, thus, most valuable domain names are those that use the gTLD .com. Consumers have been trained to expect .com and often do not notice when a domain name uses another TLD, typing .com anyway which leads them astray.

ICANN's solution to cybersquatting disputes and steep prices for the most valuable domain names has been to add more gTLDs, on the theory that more domain names would be available to all. However, since the public cannot absorb and use more than a certain quantity of information, additional domain names can merely add more noise without reducing confusion.

¹⁰⁷ *Id.*

¹⁰⁸ *WIPO Cybersquatting Cases Reach New Record in 2017*, (Mar. 18, 2018), www.wipo.int/pressroom/en/articles/2018/article_0001.html.

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *WIPO Cybersquatting Cases Reach New Record in 2017*, (Mar. 18, 2018), www.wipo.int/pressroom/en/articles/2018/article_0001.html.

¹¹² See, *WIPO Cybersquatting Cases Reach New Record in 2017*, 3/18/2018, www.wipo.int/pressroom/en/articles/2018/article_0001.html; *WIPO Domain Name Dispute Resolution Statistics*, <http://www.wipo.int/amc/en/domains/statistics/>.

¹¹³ <https://blog.verisign.com/domain-names/verisign-domain-name-industry-brief-internet-grows-to-330-6-million-domain-names-in-q1-2017/>.

Some companies that benefitted from significant traffic and interest in their existing .com websites were not tempted to go through the long and expensive process to obtain their own gTLD. If example.com was successful, a company would be reticent to try to retrain its audience to find its website at kitchen.example. Yet the proliferation of domain names brings significant funding into ICANN's coffers.

Other concerns have been raised that ICANN's governance by committee is messy and slow, with many disparate competing interests, including those of governments, brands, internet companies and consumers.

In addition, how consumers locate information and communicate online has changed in the past 20 years. Consider Google searching: many people no longer type a domain name or URL each time they look for something online. Today an Internet user may type a search request using natural language, review the results, and click on the blurb in the search results that seems most relevant or interesting.¹¹⁴ The Internet user may not even look at the domain name or URL before clicking on the blurb, unless the person is checking to see if blurb comes from a legitimate source. Even those results may be manipulated.¹¹⁵ Predictive search functionality is now widely in place to minimize the need to type a domain name or URL.¹¹⁶

The widespread use of mobile devices and downloading of applications, or "apps", also has reduced consumers' use and recognition of domain names. Rather than typing or looking for a familiar domain name or URL, a mobile device user is more likely to look at the array of apps on the device and recognize a familiar logo, click on that logo, and let the app connect the user to the desired site and information. An app user may never need to use the domain name for the website again.

Social media also have become inserted in how consumers navigate online. Many consumers go to their Facebook page, or other social page, to check news and information of interest to them, whether about their social circles, or about the world and current events, relying on friends or other selected sources to guide them. This is accomplished through clicking on logos and links, not through use of domain names. The reliance on a trusted network has enabled the proliferation of fake accounts that misrepresent their origin and purpose to develop consumers' trust and acceptance.

GDPR also has made it more difficult to determine who is behind a domain name or the site it identifies, as well as more difficult for brand owners to police harmful third party use of domain names for cybersquatting, infringement and fraud. With concerns about the GDPR's privacy requirements applicable to EU data subjects, ICANN has caused the WHOIS database to block access to domain name registrant information, in at least a temporary solution. With domain names becoming harder to scrutinize, companies may try to generate new ways to avoid directing traffic via domain names and URLs.

Lastly, as always is the case, innovation continues to move forward. New technologies are in development that will connect consumers with information and resources in new ways,

¹¹⁴ <https://www.theatlantic.com/technology/archive/2016/12/how-search-engines-are-killing-clever-urls/510785/>.

¹¹⁵ <https://www.law.berkeley.edu/wp-content/uploads/2015/04/Luca-Wu-Yelp-Is-Google-Degrading-Search-2015.pdf>.

¹¹⁶ <https://www.forbes.com/sites/forbestechcouncil/2018/03/26/getting-closer-to-your-customer-with-predictive-merchandising/#768a8d6e516c>.

many of which will not involve public awareness of domain names. The Internet itself is becoming less important, with large companies creating their own networks that replicate the Internet. Domain names formed an important bridge to the Internet in their day, and continue to serve as the address system for the internet.¹¹⁷ But looking to the future, their star may continue to dim as other technology starts to burn brighter.¹¹⁸

B. Checklist for Best Practices

1. Treat Domain Names Like Trademarks

Include domain names in the brand owner's portfolio assessment and management. Balance the amount of desired control over a brand with the risk of challenges and the cost to maintain the selected domains.

2. Treat Domain Name Registrations Like Copyright Registrations

Register them in the brand owner's name and obtain an assignment from the person or entity that is actually registering the domain. Be sure that the brand owner maintains the credentials to transfer domains if necessary.

3. Register Domain Names Containing Main Trademarks (i.e., house marks)

Also consider key trade names, important sub brands, seasonal products, and misspellings.

4. Choose Domain Registrar Carefully

Review the registrar agreement and policies. Conduct some pre-registration due diligence beyond price comparison.

5. Establish Appropriate Protocols for Records Retention

Similar to retaining trademark first use specimens and original documents demonstrating the creation of copyrighted materials, retain records showing the origins of domain names. Docket renewals and evaluations in time to make informed decisions about whether to renew registrations.

6. Manage Domain Name Portfolio and Enforcement

Order watch services or docket internal monitoring of potentially infringing domains (typosquatters, cyber squatters, trademark infringers, etc.). Employ UDRP and other processes to protect the owner's rights. Select what uses by others to challenge and maintain records that will also help support policing of the company's trademarks. Maintain appropriate records for due diligence and valuation purposes

¹¹⁷ <https://thedna.org/domain-name-associations-2017-predictions/>.

¹¹⁸ https://www2.deloitte.com/insights/us/en/focus/tech-trends/2018/reengineering-it-transformation.html?id=us:2ps:3gl:confidence:eng:cons:111215:em:dup1157:ymhrMyQB:1083198774:270785525170:b:Tech_Trends:ReEngineering_Technology_BMM:nb.

7. Avoid Scam Artists

Implement training across the company to avoid being scammed by sophisticated fraudsters. Notify accounting to confirm that all invoices regarding trademarks, domains, and copyrights are legitimate.

8. Be Pro-active

Stay alert to changes on the horizon. Actively managing a domain name portfolio can add value to a brand owner, and strengthen a trademark portfolio.

XI. CONCLUSION

Domain names are not disappearing anytime soon – they are with us for now. Domain names are valuable intellectual property assets on par with trademarks – worthy of a brand owner's time, attention, and budget.

Brand owners should include domain names in their trademark portfolios. This means assessing which domains are worthy of protection, registration, and enforcement. It means balancing the business needs of the brand with the costs to manage and maintain a potentially vast portfolio of domains. Prudent brand owners will create a portfolio management practice that includes registering all domains in the brand owner's name and obtaining appropriate assignments as necessary, retaining log-in credentials and records to demonstrate initial use, policing the domain names and trademarks against infringers, and building up valuable goodwill. They will understand the costs and benefits of employing various dispute resolution proceedings and factor that into their brand strategy. Franchisors have particular concerns when franchisees seek some control over their local online presence. Franchisors should control all online use of house marks and all credentials for online activity even if they grant some level of control to franchisees. They need to implement appropriate training to ensure that anyone using the Franchise brand online respects copyrights, rights of privacy, and other online specific restrictions, in addition to the requirements of a franchise agreement.

As the Internet becomes more ubiquitous and humans interact more closely with technology, domain names continue to provide familiar, user-friendly access to the vast and ever growing universe of information. By employing some simple best practices, brand owners can harness these important property interests for their benefit.

Exhibit A

Supplemental Materials

What Is Bad Faith? Factors To Consider Under the UDRP and ACPA

Uniform Domain-Name Dispute-Resolution Policy (UDRP), Section 4(b),
<https://www.icann.org/resources/pages/help/dndr/udrp-en>

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii) ["your domain name has been registered and is being used in bad faith"], the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. Section 1125(d)(1)(b)

(B)(i)In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to—

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c).

(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

BIOGRAPHIES

Carol Anne Been

carolanne.been@dentons.com

Carol Anne Been is a partner in the international law firm, Dentons US LLP, and is located in the firm's Chicago office. She leads the firm's U.S. Trademark, Copyright, Advertising, Transactional and Strategic IP practice within the Intellectual Property & Technology group, and is a former chair of the IP&T group. Carol Anne has extensive experience in a wide range of intellectual property matters, with an emphasis on trademark, copyright, advertising, social media, ecommerce, privacy, technology transactions, trade secrets, entertainment and publishing law. She works closely with franchisors and other IP and technology owners in prosecution, counseling, transactions, licensing and disputes for intellectual property and online resources worldwide.

Carol Anne assists clients in obtaining domain names and developing domain name policies. For more than 15 years, she has served as a panelist deciding domain name disputes under the Uniform Domain Name Dispute Resolution Procedures (UDRP) of the Internet Corporation for Assigned Names and Numbers (ICANN), working through the World Intellectual Property Organization (WIPO).

Carol Anne is listed in The Best Lawyers in America in the practice area of Trademark Law; designated as a Leading Lawyer in advertising, entertainment, copyright and trademark law; ranked in Chambers USA: America's Leading Lawyers for Business, Intellectual Property, Illinois; and recommended in the area of Trademarks in *The Legal 500*. She has been named twice as "Lawyer of the Year" for Trademark Law in Chicago by The Best Lawyers in America. She frequently writes and speaks on developing issues at the intersection of intellectual property, marketing and technology.

Susan Meyer

smeyer@greensfelder.com

Susan Meyer concentrates her practice in corporate, franchise, and intellectual property law. She is the leader of the firm's Trademark, Copyright, Media, and Advertising Group at Greensfelder, Hemker & Gale, PC in Chicago, Illinois. With experience in business management prior to her legal career, Susan understands the perspective of the business owner. She represents established companies as well as start-ups and helps her clients manage their growth. Susan has represented companies acquiring franchise systems and manages the due diligence process for franchise and licensing transactions. Susan advises franchisors and assists with their franchise compliance. She also serves as outside general counsel to franchisor clients in a broad range of industries. She handles their corporate, franchise, and intellectual property matters. Named among the "Best Lawyers in America" for franchise law this year, she has also been honored in "Who's Who Legal" for franchising for 2017-2018. Susan has presented the American Bar Association's Forum on Franchising Fundamentals 201 program on "Effective Strategies for Working with State Regulators," the Fundamentals 201 program on "Drafting a Disclosure Document," the "Disclosure and Registration" section of the Fundamentals of Franchising program, and co-hosted the Women's Caucus Breakfast. She served as the Secretary for the Illinois Bar Association's standing committee on Franchise and Distribution Law.