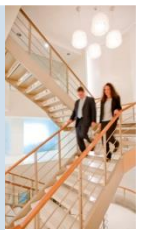
PROGRAM MATERIALS
Program #2941
April 2, 2019

The Business of Online Business: Session One - Domain Names and Domain Name Disputes

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969


DOMAIN NAMES AND DOMAIN NAME DISPUTES

The Business of Online Business

Presented by Shari Claire Lewis, Esq.

Rivkin Radler LLP

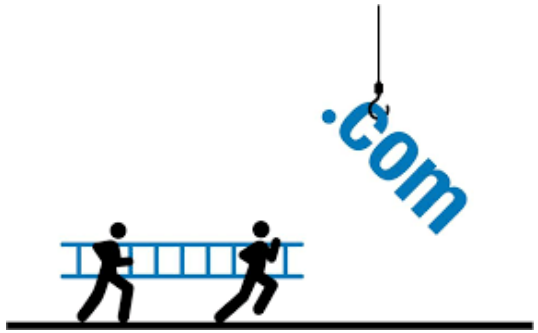
Shari.Lewis@Rivkin.Com

(516) 357-3000

RIVKIN RADLER LLP
ATTORNEYS AT LAW

DOMAIN NAMES

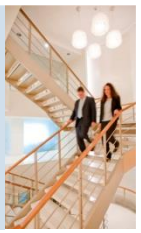
- Building a business presence online
- Name
- Address
- Brand
- Neighbors and neighborhood
- Prior tenants
- Required to operate website, email, weblog, etc.



RIVKIN RADLER LLP
ATTORNEYS AT LAW

DOMAIN NAMES

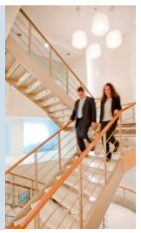
- IP/TCP Protocol
- IP addresses
  - assigned by Dr. Jon Postel
  - long, hard to remember, alphanumeric address
  - “resolver” looked up number in directory
  - content routed to computer in directory
  - *“2606:2800:220:1:248:1893:25c8:1946” = <example.com>*



RIVKIN RADLER LLP
ATTORNEYS AT LAW

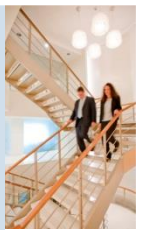
DOMAIN NAMES

- Users informally named their computers
- Elizabeth “Jake” Feinler - developed the top-level domain naming scheme still in use to day
- Users called up Feinler’s Host Naming Registry – associated domain name and IP address manually (1972-1989)
- Domain Name System (“DNS”)
  - gTLDs (generic Top Level Domains)
  - SLDs (Second Level Domain Names)
  - Example.com

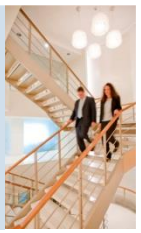


DOMAIN NAMES

- Master server is constantly updating to associate domain names and IP addresses
- Redundant distributed servers constantly updating to match the master server
- Registry – maintains the master server for each TLD
- Registrar/Registrar Operator – (accredited by ICANN)
  - Register SLDs in the TLDs
- Resellers work with registrars to register domain names
- Domain names do not exist absent registration



DOMAIN NAMES



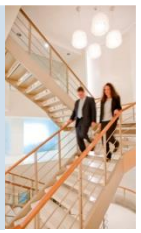
- 1993 – 1998 Network Solutions, Inc. under contract with National Science Foundation – the ".com boom"
- September 1998 ICANN
- Private and international control with mandate:
  - Grow of number of gTLDs
  - Expand number of DNS registrars, from one to 50, initially and now @ 3,000
  - Adoption of UDRP

DOMAIN NAMES

- Generic Top Level Domain Names (gTLDs) –
  - .com, .net, .org
- Country Code Top Level Domain Names (ccTLDs)
  - .us, .cn, .de, .uk, .au, .tv
- Internationalized country code Top Level Domain Names (IDNccTLD)
  - Domain names that display in Cyrillic, Arabic, Chinese, Thai, etc.
  - .中国 (Chinese), .рф (Russia) .پاکستان (Pakistan) etc.

DOMAIN NAMES

- Restricted Top Level Domain Names (grTLDs)
  - must prove qualification to register
  - .name, .pro, .biz
- Sponsored Top Level Domain Names (sTLDs)
  - .gov, .edu, .int, .mil, .aero, .tel, .xxx, .app,
  - Sponsor represents the interests of narrower community and may impose use rules
  - New top level domains may also be “sponsored”



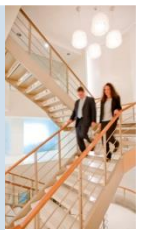
RIVKIN RADLER LLP
ATTORNEYS AT LAW

DOMAIN NAMES

- New Top Level Domain Names (nTLDs)
- Over 1,000 TLDs as of February 2019
- Some have “restricted open” policies, such as for regulated industries (banking, securities, medicine etc.)
- “Sunrise” and “Landrush”
- Brands
- Industries
- Geography
- Fanciful

Cybersquatting

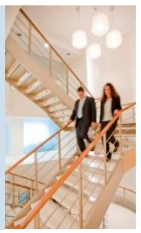
- No one is registering <.coke.com> anymore
- Fights over brands, business names and trademarks
  - Competitive businesses
    - There can be only one
  - Slam sites – “Ihate(insertproductname).com”
  - Free speech, politics, defamation and hate speech
  - Phishing or fraud domain names
  - Record number of cybersquatting cases in 2018 - WIPO



RIVKIN RADLER LLP
ATTORNEYS AT LAW

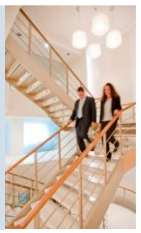
ACPA
(Anti-cybersquatting Consumer Protection Act)

- 15 U.S.C. §1125(d)
- Civil action against a "person"
  - Domain name registrant
  - Domain name registrant's licensee
  - With bad faith intent to profit
- Registers, traffics in or uses as a domain name
  - Personal name
  - Distinctive or famous mark
    - Identifical, confusingly similar or dilutive
  - Trademark , word or name protected under IP laws



ACPA
(Anti-cybersquatting Consumer Protection Act)

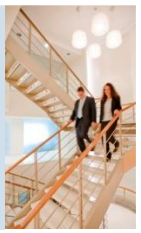
- Plaintiff must establish
  - Valid mark entitled to protection
  - Distinctive or famous
  - Defendant's domain name is identical, confusingly similar, or dilutive of mark holder's IP
  - Defendant used, registered or trafficked in domain name
  - Bad faith intent to profit



RIVKIN RADLER LLP
ATTORNEYS AT LAW

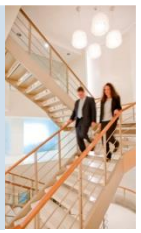
ACPA
(Anti-cybersquatting Consumer Protection Act)

- Elements to consider re: bad faith (non-exclusive list)
  - Registration of trademark or other intellectual property right belonging to another
  - Registration of person's legal name or commonly used name
  - Registrant's prior *bona fide* use of domain name in commerce (defense)
  - Registrant's *bona fide* non-commercial or fair use of the mark in its linked site (defense)



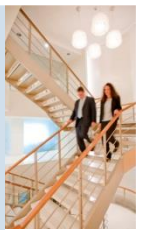
ACPA
(Anti-cybersquatting Consumer Protection Act)

- Elements to consider re: bad faith (non-exclusive list)
  - Registration for purpose of diverting consumers from trademark owner's online location, in order to harm good will, for commercial gain or with intent to tarnish, disparage or confuse visitors as to source
  - Offer to transfer, sell or assign domain name for financial gain w/o prior *bona fide* use or pattern of doing so (domain name speculation)
  - Registrant's use of false and misleading information for registration or pattern of doing so



ACPA
(Anti-cybersquatting Consumer Protection Act)

- Elements to consider re: bad faith (non-exclusive list)
  - Registration of multiple domain names that are similar or identical to claimant's distinctive or famous marks without regard to the goods and services of the parties
  - The extent to which the mark in the domain name is or is not distinctive or famous



ACPA
(Anti-cybersquatting Consumer Protection Act)

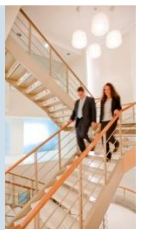
- Injunctive relief
  - Transfer
  - Cancellation
  - Reregistration
- Damages
  - Actual damages

  OR
  - Statutory damages
    - $1,000 - $100,000 per domain name as court considers "just"

UDRP

Uniform Domain Name Dispute Resolution Policy

- Created by ICANN
- Accredited registrars must
  - Include in registration agreements
  - Not transfer registration during UDRP
  - Abide by and enact UDRP decisions unless advised lawsuit filed in proper jurisdiction within 10 days
- Registrants agree:
  - Terms in their registration agreements
  - Registrar enact UDRP decisions unless file lawsuit within 10 days of decision or before

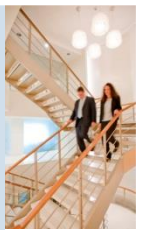


RIVKIN RADLER LLP
ATTORNEYS AT LAW

UDRP

Uniform Domain Name Dispute Resolution Policy

- Streamlined ADR process
  - ICANN approved UDPR Providers, e.g. WIPO, NAM
  - Intended 60 day start to finish (sometimes longer)
  - One or three member panel
  - Rules, form complaints, reported decisions, etc.
  - Provider fees @ $1,500 to $5,000
- BUT:
  - Not exclusive
  - Either party can file lawsuit before, during or after
  - No fines, penalties or damages

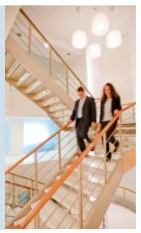


RIVKIN RADLER LLP
ATTORNEYS AT LAW

UDRP

Uniform Domain Name Dispute Resolution Policy

- Claimant must show:
  - Domain name is identical or confusingly similar to trademark or service mark
  - Registrant has no rights or legitimate interest in domain name
  - Domain name has been registered and is used in bad faith

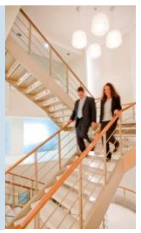


RIVKIN RADLER LLP
ATTORNEYS AT LAW

UDRP

Uniform Domain Name Dispute Resolution Policy

- Registrant's defense
  - Prior *bona fide* commercial use or preparation to use
  - Registrant commonly known by name
  - Legitimate non-commercial use (w/o intent to mislead, divert or tarnish)

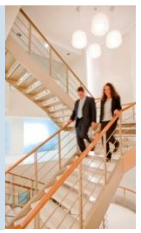


RIVKIN RADLER LLP
ATTORNEYS AT LAW

UDRP

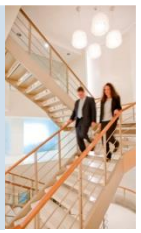
Uniform Domain Name Dispute Resolution Policy

- Bad faith registration or acquisition:
  - to sell, rent or transfer domain name to owner of mark or competitor
  - to prevent mark owner's registration
  - to disrupt competitor's business
  - use of domain name to attract users to website or other online location for commercial gain, by creating likelihood of confusion as to source, sponsorship, affiliation, etc.



REVERSE DOMAIN NAME HIJACKING

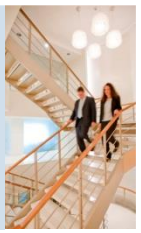
- "Anti-competitive", "anti-democratic", "pro-business"
- Overly aggressive use of UDRP
- Intimidate smaller competitors/secure transfer of domain name where registrant has senior interest
- Original registrant can file for injunctive relief for return of domain name registration under ACPA
- May seek damages, attorneys fees and injunctive relief if complainant made a "knowing and material misrepresentation" in UDRP



RIVKIN RADLER LLP
ATTORNEYS AT LAW

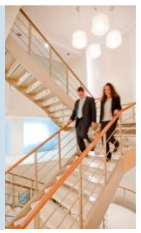
TRADEMARK CLEARINGHOUSE

- ICANN established
- Additional/expedited protection in nTLDs
- Holders submit proof of trademark registration, location, use
- Benefit:
  - "Sunrise Period"
    - Exclusive registration 30 days before general registration
  - "Trademark Claim Period"
    - 90 days after general registration
    - Registrant and mark holder notified of registration
    - Can register to receive notices after 90 day



URS

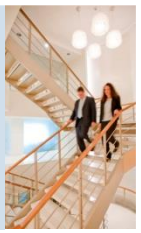
Uniform Rapid Suspension System



- Applies to nTLDs – even faster than UDRP
- Administered by ICANN approved providers
- Intended to be cheaper and faster than UDRP ($375)
- Must show proof of national registration and use by claimant and bad faith registration by registrant
- Registration with Trademark Clearinghouse is proof of use
- Suspension and redirection, but not transfer
- Good for trademark holders only interested in blocking somone's else's use

SCAMS AND ASSORTED ISSUES

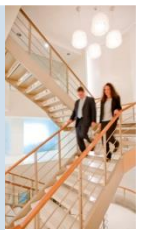
- Abusive registrations
- Phishing Scams
- Chinese and Other Top Level Domain Name Scams
- Elusive Transfers



SCAMS AND ASSORTED ISSUES

Abusive Registrations

- Registration of a domain name to effectuate fraud
- Mislead/misdirect by implication, "typosquatting," coupling generic words with trademark etc.
- National and international disasters – be careful to whom you donate
- ID theft, phishing, tax scams, misappropriation of commercial opportunity



RIVKIN RADLER LLP
ATTORNEYS AT LAW

SCAMS AND ASSORTED ISSUES

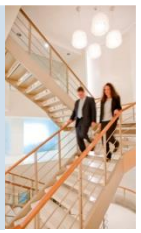
Phishing Scams

- User is duped into revealing personal or confidential information
- Domain name may appear to be legitimate
- Asks for information, provide passwords, send money
- Domain name renewals, domain name “slamming”, donations
- ICANN’s Warning Signs:
  - False sense of urgency
  - Contains fake links (mouse hover)
  - Has an attachment or software download

SCAMS AND ASSORTED ISSUES

Chinese Domain Name Scams

- May 29, 2012 China Internet Network Information Center (CNNIC) relaxed local requirement for .cn
- Domain Name Scam
  - Email from “accredited Chinese registrar” in or outside China
  - Allege that others trying to register trademark/business name in .cn
  - Purpose of email is to offer for trademark/ business to register first.
  - Unnecessary domain name.



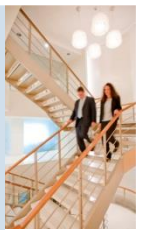
RIVKIN RADLER LLP
ATTORNEYS AT LAW

SCAMS AND ASSORTED ISSUES

Elusive Transfers

- Steal registration account information (user name/password)
- Transfers domain name to new registrar
- Domain name associated with different or same or take down
- Offers domain name for sale on open market or back to prior registrant

RIVKIN RADLER LLP
ATTORNEYS AT LAW



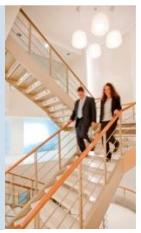
Why should you care?
Your business around the world

- Your online business/professional name and address
- Intellectual property
- Location, location, location
- The friends you keep
- Easy to find
- Protect your image
- Control the message

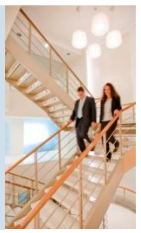
RIVKIN RADLER LLP
ATTORNEYS AT LAW

SOME ISSUES TO CONSIDER

- Who registered you domain name before and for how long?
- What Internet content was associated with the domain name previously?
- What kind of analytics are available concerning visitor use, browsing and hits?
- Did Google or any regulator (FTC, etc.) take any action against prior registrant?
- Was domain name associated with safe site?
- Prior good will or bad business practice?
- Tools

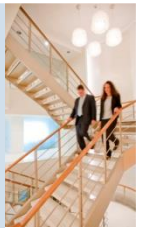


TIPS FOR CHOOSING DOMAIN NAMES



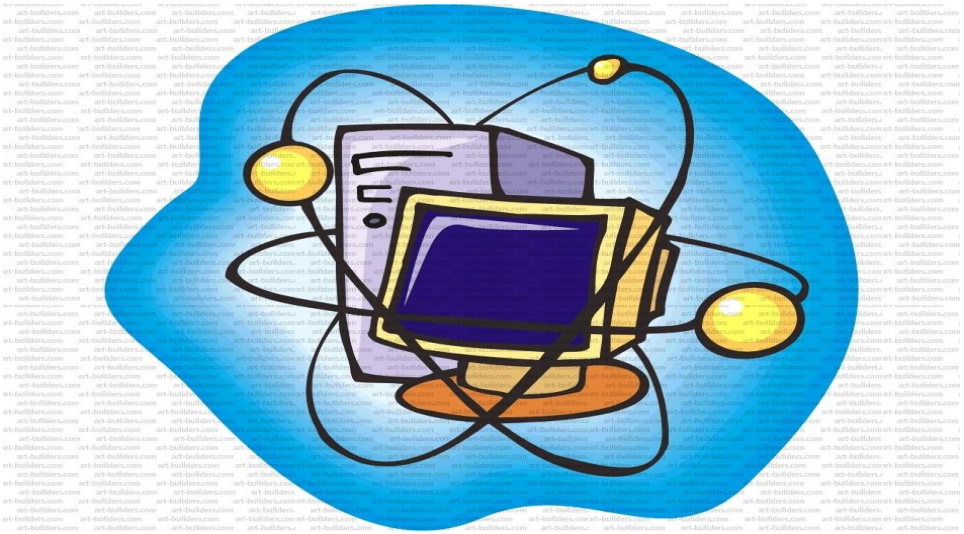
- Make it easy to type.
- Keep it short.
- Use keywords.
- Target your area.
- Avoid numbers and hyphens.
- Be memorable.
- Research it.
- Use an appropriate domain name extension.

-- Registrar GoDaddy.Com



Questions?

Thank you

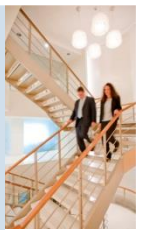


Presented by Shari Claire Lewis, Esq.

Rivkin Radler LLP

Shari.Lewis@Rivkin.Com

(516) 357-3000



For More Information

Presented by Shari Claire Lewis, Esq.
Rivkin Radler LLP
Shari.Lewis@Rivkin.Com
(516) 357-3000

OUR PRIVACY, DATA & CYBER LAW PRACTICE GROUP PERIODICALLY ISSUES NEWSLETTERS ON CURRENT AND DEVELOPING ISSUES. IF YOU WOULD LIKE TO RECEIVE OUR MARCH 12, 2019 NEWSLETTER CONCERNING THE CALIFORNIA PRIVACY LAW OR FUTURE NEWSLETTERS PLEASE EMAIL ME AT Shari.Lewis@Rivkin.Com

THE BUSINESS OF ONLINE BUSINESS: DOMAIN NAMES AND DOMAIN NAME DISPUTES

By: Shari Claire Lewis, Esq., Avigael Fyman, Esq. and Cali Eckler, Esq.[1]

TABLE OF CONTENTS

Page

I. The Internet, World Wide Web and Domain Name System 1
   A. The Internet 2
   B. Domain Name System 3
   C. ICANN 4
   D. ccTLDs, nGTLD's and International Domain Names 5
II. Domain Name Disputes And Cybersquatting 6
   A. The Anticybersquatting Consumer Protection Act 6
   B. The Uniform Domain Name Dispute Resolution Policy (UDRP) 10
   C. Reverse Domain Name Hijacking Claims 11
   D. Trademark Clearinghouse and the Uniform Rapid Suspension System 13
III. Scams and Assorted Issues 14
   A. Abusive Registrations 14
   B. Phishing Scams 17
   C. Chinese Domain Name Scams 19
   D. Elusive Transfers 20
IV. Some Practical Domain Name Practices 22

[1] The authors express their gratitude to Thomas J. Veltre, who assisted in the compilation of source material.

"Location, location, location…"
~ Every real estate agent – ever.

When a business decides to venture onto the Internet, one of its first stops must be the creation of its domain name. Regardless of whether the business intends to operate exclusively online, in a traditional "brick and mortar" setting, or, as is often the case nowadays, through a combination known as "click and mortar", selection of its domain is key to its online success. A domain name is both an online "handle" and address. By choosing its domain name, a business "plants its flag" on the surface of the Internet. Each time someone uses the domain name to access a business' website, weblog, email, etc., the business' discretion in choosing the name and neighborhood in which it resides is on display and will be judged against the choices made by its competitors.

Moreover, because a domain name has no independent or physical manifestation unless and until it is registered, the selection of a domain name can be accompanied by unexpected baggage. For example, a preferred domain name may introduce previously unknown intellectual property issues regarding the business' use of a certain name or someone else's use of that same name. Likewise, a previously registered domain name that was abandoned, like a previously inhabited house, may cause visitors to link the new registrant to the prior registrant's bad contact. Finally, any time we open the door for communication, we make ourselves vulnerable to the bad actors who exploit that opening.

Nevertheless, domain names are critical to the conduct of online commerce and interpersonal exchange. This article will discuss some of the challenges that a business may face in selecting, monitoring and using its domain name. Some background on how and why the domain name system developed is worth considering.

I. The Internet, World Wide Web and Domain Name System

"Let's look it up on the internet… I spent all night surfing the web…
That video went so viral that it broke the internet! …"

As we all know, Internet use is pervasive. As of June 2018, approximately 55% of the world's population has internet access. *https://en.wikipedia.org/wiki/Global_Internet_usage*. According to the latest census figures, percentage of U.S. households who reported using a computer jumped from just 8% in 1984 to 89% in 2016. *https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf*.

Computer usage now engages every facet of 21st Century personal and professional life, such as online banking, entertainment, socializing and accessing health care to name a few. Domain names and the system that was created around them have played a key role in commercial exploitation of the Internet, as domain names eliminated the need for individual users to have extensive computer literacy in order to engage online. For example, most of the general public tends to view the terms "Internet" and "World Wide Web" interchangeably. In reality the Internet and the World Wide Web are distinct, but closely related entities.

The Internet is most easily understood as a type of "infrastructure" that connects or links your computer to millions of interwoven connections and enables them to communicate with each other. The World Wide Web ("WWW") is one information sharing model that uses the Internet. The WWW depends on certain protocols and languages that permit users to access and share information. WWW was developed with the "hope" that it would "allow a pool of information to develop which could grow and evolve" … [because] a 'web' of notes with links between them is far more useful than a fixed hierarchical system." Tim Berners-Lee, *Information Management: A Proposal,* http://www.w3.org/History/1989/proposal.html. The proposal was indeed, prophetic, as WWW continues to dominate Internet use 30 years after it was described.

Other content, such as email, UseNet news groups, instant messaging and FTP also use the Internet, but not the WWW. *See,* https://www.quora.com/What-is-the-difference-between-the-World-Wide-Web-and-the-Internet. [2] However, every Internet usage depends on a naming system that includes domain names.

A. The Internet

In response to the Cold War and fears of Soviet scientific advancement, in 1958, a new office within the Department of Defense was established – the Advanced Research Projects Agency or ARPA. This agency's mission was to explore a broad range of new technologies with emphasis centered on major national issues, including space, ballistic missile defense, and nuclear test detection. Lyon, Matthew; Hafner, Katie (1999-08-19). *Where Wizards Stay Up Late: The Origins of the Internet* (p. 23). Simon & Schuster. A crucial component of ARPA's purpose was analysis of the means by which nuclear launch codes were transmitted to various installations.

However, ARPA's information technology expertise proved to be useful for more than just launching missiles**.** ARPA had contracts with universities and research centers around the country, all of whom needed the latest computers with the most capabilities. Isaacson, Walter *The Innovators* pg 232, Simon & Schuster 2014. The resultant network was referred to as ARPANET and was primarily funded by the Department of Defense. *Id.* During the same era, an interwoven network was developed for purposes of sharing research, academic dialogue and other non-military communications. This network, known as the NSFNET was funded by the National Science Foundation as well as other federal agencies, academic institutions and corporate sponsors. *Island Online, Inc. v Network Solutions, Inc.*, 119 F Supp 2d 289, 292-294 (EDNY 2000).

By the mid-70's the need for these and other disparate networks to be able to connect to each other prompted the development of two "keystone" software protocols – the InterNet Protocol (IP), which helped route "packets" of data through the various networks to their

[2] Interestingly, both the Internet and the WWW are celebrating anniversaries in 2019. The WWW turned 30 in March, and the first "node" of the prototype for the "Internet" went on line 50 years ago, in October of 1969. But the origins of universal computer networking date back much earlier. The Internet - like so many scientific advances in the mid- 20th Century - is a child of the Cold War.

destination computers, and the Transmission Control Protocol (TCP), which instructed the destination computer how to reassemble the packets into the correct order, check for errors and deliver the complete message. This became known as "TCP/IP" – the core technology which enabled the growth of this *Network of Networks* – and is still at the heart of what we call The *Inter*-net. In the 1980's, ARPANET, NSFNET and other networks were interwoven into the Internet in its present form. *The Innovators* pg 383-384.

B. Domain Name System

"The Domain Name Server… is the Achilles heel of the Web.
The important thing is that it's managed responsibly."
~Tim Berners-Lee
Inventor of the World Wide Web
https://www.brainyquote.com/quotes/tim_bernerslee_373104

Domain names and the domain name system are essential components of the Internet's functionality to this day. As such, it is interesting to note their modest beginnings considering their pivotal role in worldwide commerce today.

As part of IP protocol, each computer on the Internet is identified by a unique, lengthy and confusing string of numbers, referred to as its IP address. In the beginning, IP addresses were assigned and maintained by one individual – Dr. Jon Postel – at the University of Southern California's Information Sciences Institute, through the Internet Assigned Numbers Authority or IANA. At the same time, because IP addresses were difficult to remember, an informal practice of network users giving alphabetic names to their computers grew – a practice that spread with network use. Consequently, the cumbersome strings of numbers were made a little more "human-friendly" by the institution of the Domain Name System ("DNS").

The DNS operates much like an old fashioned telephone directory. Easy to remember strings of letters and words are assigned to stand in for the lengthy numerical IP address. Users could then type in a simple name, (like "example.com") and an intermediate computer, a "domain name server", acting as a DNS "resolver" would look up the associated number (in this case *2606:2800:220:1:248:1893:25c8:1946*) and route the message to the designated computer location.

In the early days of ARPANET, to get your domain name, you could simply call up Elizabeth Feinler at the Stanford Research Institute ("SRI") and just ask her for the one you wanted. Her team at SRI managed the Host Naming Registry for the Internet from 1972 until 1989. It was Ms. Feinler and her group that developed the top-level domain-naming scheme of .com, .edu, .gov, .mil, .org, and .net, (collectively "gTLD") which is still in use today. Ms. Feinler is a hero of the Internet whose contributions are sometimes overlooked. *See,* *https://www.internethalloffame.org/inductees/elizabeth-feinler*. Applying the scheme she

developed to "example.com", <.com> is the top level domain ("TLD") and "example" is the second level domain ("SLD"), chosen by the registrant.[3]

Since the need for DNS name resolution (conversion of domain names into IP numbers) is constant, it is necessary to maintain and update the DNS database continuously. That need quickly outstripped the capacities of individual management. Accordingly, new domain name information is obtained and disseminated through a process called DNS registration. DNS registration has evolved into a complex industry involving "registrants", "registrars" "operating registries" and, sometimes "resellers" *https://newgtlds.icann.org/en/announcements-and-media/infographics/dns-industry-ecosystem*. Suffice to say, that registrants register their chosen and available domain with registrars who relay registration information to the relevant registry operator, who is responsible for the management and operation of that registry's TLD.

As the Internet grew, the task of assigning of IP address numbers and domain names could no longer be feasibly performed by the individuals who created the system and was taken over by the National Science Foundation. In 1993, NSF contracted with Network Solutions, Inc. to provide services for DNS registration and network number assignments. *https://www.icann.org/en/history/early-days* For a period of five years Network Solutions was the sole registrar for the Internet during the infamous "dot-com" boom of the 1990s. During this period, Network Solutions was the only place one could go to register SLDs names within the generic top level domain names ("gTLD"), .com, .net, .edu and .gov TLDs.

C. ICANN

In November 1998, President Clinton launched an initiative to increase completion in and promote international participation in DNS registration. It was, in part, because of the enormous growth in commercial use of the Internet beyond its origins in the academic research community that the US Department of Commerce recommended that control of Internet domain names be transferred from the government to a private, nonprofit corporation. As stated in the Proposed Rule: "As Internet names increasingly have commercial value, the decision to add top-level domains cannot continue to be made by entities or individuals that are not formally accountable to the Internet community…" *See, Improvement of Technical Management of Internet Names and Addresses; Proposed Rule (*Federal Register Feb. 20, 1999 (Vol 63, No. 34) pg. 8825 – 8833.

The Internet Corporation for Assigned Names and Numbers (ICANN) was created in September 1998 as a nonprofit corporation to manage Internet addresses, domain names and computer communication protocols with input from the professional internet community world wide. Along with this transfer of Internet management out of government control, ICANN received a mandate that the number of gTLDs be expanded beyond the original .com, .net & .org, .edu, etc., to expand the universe of available names with potential commercial value.

[3] Using the telephone directory analogy, <.com> is the area code and "example" the phone number. You can have many phone numbers in an area code, but each must be unique. On the other hand, there is no bar to the same phone number being used in different area codes except for an occasional wrong number.

One of ICANN's first initiatives was to expand the number of DNS registrars. As a result, in addition to Network Solutions, the role of registering domain names was contracted to a number of competing commercial entities. *Island Online,* 119 F. Supp. 2d at 294. Whereas that original expansion was limited to approximately 50 "accredited registrars", today they number in the hundreds.

Also, within a year of its establishment, ICANN adopted the Uniform Domain Name Dispute Resolution Policy ("UDRP"), its primary "tool" for policing registration of domain names on the Internet. One of the most challenging aspects of the commercialization of the Domain Naming System continues to be the need to balance competing intellectual property rights, free speech interests and competition. These and other "cybersquatting" issues are discussed below.

D. ccTLDs, nGTLD's and International Domain Names

It should always be remembered that in addition to the original gTLDs there are literally hundreds of top level domains, such as country codes, ("ccTLDs") that are administered by individual countries, i.e., .uk, .de, .cn, etc. and sponsored or generic restricted TLDS, where domain registration is limited to certain criteria, such as an industry segment.

In recent years, ICANN has also overseen the explosive growth of generic TLDs, referred to as new generic domain names ("nTLD"). At the present time, ICANN lists literally hundreds of gTLDS, starting with <.aaa> and concluding with <.zw>. *See, http://data.iana.org/TLD/tlds-alpha-by-domain.txt*. ICANN, moreover, cautions that the list is constantly being updated and should be checked regularly. There is some debate, however, about the commercial utility of registering a new top level domain name or a SLD in the more obscure new domains. With certain notable exceptions, (such as <.xxx> for pornography site), many Domain Names in the nTLDs simply redirect to more familiar .com, .net and .org. gTLDs. A copy of ICANN's "New gTLD Fast Facts" is attached at the end of this article.

Another important change introduced by ICANN was the introduction of Internationalized Domain Names ("IDNs"). It is not surprising, given its US origins, that initially, the DNS recognized only the Latin alphabet used in English, i.e., 26 letters "a-z", the numbers "0-9" and the hyphen "-". Starting in 2010, multilingual domain names called Internationalized Domain Names ("IDNs') were enabled. IDNs include diacritical marks as required by some European languages, or non-Latin characters, such as used in Arabic, Chinese, Russian, Thai and other non-European languages. *https://www.icann.org/en/system/files/files/multilingual-internet-01nov13-en.pdf*. With IDNs, it can truly be said that the "World Wide Web" became worldwide.

It was reported that, as of the third quarter of 2018, there were approximately 342 million domain name registrations across all gTLDs. At the same time there were was 149 million registrations in all ccTLDs. *https://www.verisign.com/en_US/domain-names/dnib/index.xhtml*. What is plain is that the Internet of today is a unique entity in global

commerce. It is a completely de-centralized infrastructure, owned by no single country, cooperatively managed on a non-profit basis by an international consortium.

II. Domain Name Disputes And Cybersquatting

"*Domain names and websites are Internet real estate."*
~ Marc Ostrofsky
Author of "*Get Rich Click!:*
The Ultimate Guide To Making Money Online"
https://www.brainyquote.com/quotes/marc_ostrofsky_493875

The phrase "cybersquatting" is derived from "squatting", a term used to describe a person's illegal use of an undeveloped plot of land, or a vacant or abandoned building. As a general matter, cybersquatting involves the abusive practice of registering, trafficking in, or using a domain name in order to profit from the goodwill of a trademark belonging to someone else or to inflict damage on that goodwill.

In the earlier days of the internet, cyber squatters would often engage in registering well-known company or brand names with the hope of reselling them for profit. While these types of cybersquatting schemes are less common today, disputes over the use of trademarks in domain names continue to arise. *See e.g.,* Shari Claire Lewis, *Cybersquatting: Even Today, an Important Concern for Online Businesses,* New York Law Journal, October 15, 2018 available at: *https://www.law.com/newyorklawjournal/2018/10/15/cybersquatting-even-today-an-important-concern-for-online-businesses/.* Indeed, the World Intellectual Property Organization ("WIPO"), reported that a record number of domain name dispute cases were filed with WIPO in 2018. *See, WIPO Cybersquatting Cases Grow by 12% to Reach New Record in 2018,* WIPO Press Release, March 15, 2019 available at *https://wipo.int/pressroom/en/articles/2019/article_0003.html.* It would, therefore, be a mistake to consider cybersquatting a relic of the Internet's early growth that is no longer requiring businesses to be diligent in protecting their online brands.

Two mechanisms have become dominant as the means to resolve domain name disputes. for First, federal law intellectual property law was expanded to accommodate the need for legal determination of competing rights by enactment the Anticybersquatting Consumer Protections Act. Alternatively, domain name registrants are required as a condition of registration agree to submit to the Uniform Dispute Resolution Process for expedited, mediated resolution of the dispute. Each mechanism has its own benefits and detriments and should be considered based on the merits of each claim.

A. The Anticybersquatting Consumer Protection Act

Cybersquatting claims can be brought in the federal courts of the United States under the Anticybersquatting Consumer Protection Act, 15 U.S.C. §1125(d).

The Anti-Cybersquatting Consumer Protection Act ("ACPA") provides that:

> A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person:
>
> **(i)** has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and
>
> **(ii)** registers, traffics in, or uses a domain name that—
>
> **(I)** in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
>
> **(II)** in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or
>
> **(III)** is a trademark, word, or name protected by reason of section 706 of Title 18 or section 220506 of Title 36.

15 USC § 1125(d)(1)(A). A person can be held liable for violating the ACPA section above only if that person "is the domain name registrant or that registrants authorized licensee." 15 USC § 1125(d)(1)(D).

In order to succeed on an ACPA claim, the plaintiff must establish the following five elements: (i) it has a valid trademark entitled to protection; (ii) its mark is distinctive or famous; (iii) the defendant's domain name is identical or confusingly similar to, or in the case of famous marks, dilutive of, the owner's mark; and (iv) the defendant used, registered, or trafficked in the domain name (v) with a bad faith intent to profit. *See* 15 USC § 1125 (d)(1). When determining whether the fifth element (bad faith intent) is present, courts generally consider the following nonexclusive list of factors:

> **(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) of this section.

15 USC § 1125(d)(1)(B)(i).

The ACPA provides that the owner of a mark may bring a civil action against a person who "(i) has bad faith intent to profit from that mark, and (ii) registers, traffics in, or uses a domain name that is confusingly similar to another's mark or dilutes another's famous mark." *See, e.g., AECOM Energy & Constr., Inc. v. Morrison Knudsen Corp.*, 748 Fed. Appx. 115 (9th Cir. 2018). Where a violation of the ACPA is established, the owner of the protected mark may recover either actual damages and profits or an award of statutory damages in the amount of not

less than $ 1,000 and not more than $ 100,000 per domain name, as the court considers just. 15 U.S.C. §1117(d).

At times, cybersquatting claims arise in the context of a broader intellectual property or business dispute. One such recent example can be found in the case of *Grumpy Cat Ltd. v. Grenade Bev. LLC*, 2018 U.S. Dist. LEXIS 91342, 2018 WL 2448126 (C.D. Cal. May 31, 2018). Plaintiff Grumpy Cat Ltd. was the owner of intellectual property rights associated with the internet meme "Grumpy Cat," including a registered trademark.[4] Grumpy Cat had entered into a licensing agreement with defendant Grenade Beverage LLC to sell certain coffee products using the Grumpy Cat name and image. A third party had owned the domain name <grumpycat.com> before the Grumpy Cat memes went viral, and Grumpy Cat had been unable to obtain the domain name from said third party. However, Grenade Beverage subsequently acquired the domain name from the third party, and used it to direct customers to their beverage website. Grenade Beverages also sought to expand their use of the Grumpy Cat name and image to sell other coffee products, and proposed an agreement to transfer the <grumpycat.com> domain name to Grumpy Cat in exchange for a modification to their licensing agreement. Grumpy Cat declined the agreement, and asserted a claim alleging that Grenade Beverage was using the Grumpy Cat name and image beyond what was authorized by the licensing agreement. Following a jury verdict for Grumpy Cat on the claim for breach of the licensing agreement, the Court issued a ruling on Grumpy Cat's claim that Grenade Beverage's ownership and use of the <grumpycat.com> domain name violated the ACPA.

The Court held that the Grenade Beverage did not have the requisite "bad faith" to be in violation of the ACPA. While Grumpy Cat had argued that Grenade Beverage, by proposing to transfer the domain in exchange for a renegotiation of the licensing agreement, had used the domain name as leverage, constituting bad faith, the Court held that there was no bad faith where the domain name was used as part of a business negotiation between collaborators to further the sale of Grumpy Cat-branded products.

Another situation where ACPA claims continue to arise involves websites selling counterfeited luxury goods. In *Chanel, Inc. v. Richardson*, 2018 U.S. Dist. LEXIS 198687, 2018 WL 6097865 (S.D.N.Y. 2018), Chanel, Inc., brought a claim for cybersquatting against an individual who had registered the domain name chanelgraffiti.com and who advertised and sold products that contained Chanel marks and were described as "chanel inspired graffiti bags." There, the Court noted, notwithstanding the fact that the defendant had added an additional word ("graffiti") to Chanel's mark, the domain name was "sufficiently similar" to confuse consumers as to whether the infringing website was affiliated with the mark. Moreover, the Court noted, "the term 'graffiti' does not self-evidently connote a type of criticism or disregard for the brand that rises to a meaningful level of distinction." Similarly, in *Montblanc-Simplo GmbH v. Ilnitsky*, 2018 U.S. Dist. LEXIS 244431, 2018 WL 844401 (E.D. Va. 2018), the Court entered a judgment on default against the operator of montblancpensoutletcheapsale.com,

[4] Wikipedia explains Grumpy Cat as "an American internet celebrity cat . . . known for her permanently 'grumpy' facial appearance, which is caused by an underbite and feline dwarfism . . . She is the subject of a popular internet meme in which negative, cynical images are made from photographs of her." *See* https://en.wikipedia.org/wiki/Grumpy_Cat.

montblancpensoutletcheap.com, montblancpensoutletcheaponsale.com and monblancua.com, who was alleged to have used said websites to sell counterfeit Montblanc products.

B. The Uniform Domain Name Dispute Resolution Policy (UDRP)

While some cybersquatting disputes are resolved in court, the vast majority of such disputes are addressed by the Uniform Domain Name Dispute Resolution Policy, or UDRP, an alternative dispute resolution mechanism set up by ICANN. The UDRP provides that domain name registrants are required to submit to a mandatory administrative proceeding where a third party sets forth an allegation of cybersquatting.

ICANN's Rules for Uniform Doman Name Dispute Resolution Policy is required to be followed by all registrars in resolving domain name disputes. The most up to date version applies to proceedings commenced on or after July 31, 2015 and may be accessed on the ICANN website. *https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en*. However, in response to the General Data Protection Regulation, ("GDPR") on May 17, 2018, ICANN adopted a Temporary Specification meant to balance the need to access registrant personal information for purpose of UDRP proceedings and GDPR privacy limits on access and use of personal data of European Union residents. *See https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf* . The extent to which GDPR privacy will impede the DNS registration scheme or UDRP proceedings has not yet been determined. *See* Discussion below.

In a UDRP proceeding, a complainant has the burden of proving the following three elements: (1) that the registrant's domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; (2) that the registrant has no rights or legitimate interests in respect of the domain name; and (3) that the registrant's domain name has been registered and is being used in bad faith. A copy of a sample complaint is available at the WIPO website, and is attached at the end of this article. *https://www.wipo.int/amc/en/domains/complainant*.

UDRP criteria for demonstrating bad faith are slightly different than those set forth under the ACPA. Under the UDRP, the following are considered evidence of registration and use of a domain name in bad faith: (1) circumstances indicating that the registrant registered or acquired the domain name for the primary 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 the registrant's documented out-of-pocket costs directly related to the domain name; (2) the registrant 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 the registrant has engaged in a pattern of such conduct; (3) the registrant registered the domain name primarily for the purpose of disrupting the business of a competitor; or (4) by using the domain name, the registrant has intentionally attempted to attract, for commercial gain, Internet users to his or her 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 the registrant's web site or location or of a product or service on the registrant's web site or location.

A registrant can demonstrate his or her rights or legitimate interest to the domain name by showing that (1) before receiving 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; (2) the registrant (as an individual, business, or other organization) had been commonly known by the domain name, even if the registrant had acquired no trademark or service mark rights; or (3) the registrant is making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or tarnish the trademark or service mark at issue.

ICANN has enacted a set of Rules that govern UDRP disputes, specifying how to submit complaints, put parties on notice, and respond. ICANN provides a list of approved Dispute Resolution Service Providers on its website. *https://www.icann.org/resources/pages/providers-6d-2012-02-25-en.*

The UDRP is streamlined so that disputes may move from the filing of a complaint to resolution in approximately sixty days. Parties can elect to have their disputes decided by a single-member or a three-member Panel. A party bringing a UDRP complaint selects a dispute resolution provider, approved by ICANN. In the United States, the most commonly used providers are the National Arbitration Forum and the World Intellectual Property Organization, who have their own supplemental rules for the administration of disputes. Providers also set fees for their services, which vary based upon the number of domain names in dispute and the number of panelists and range from around $1,300 to $5,000. Complainants cannot obtain civil damages in UDRP disputes, but may obtain the cancellation or transfer of a domain name.

UDRP dispute resolution procedures are not exclusive and do not prevent either party from submitting the dispute to a court of competent jurisdiction either before or after a UDRP administrative proceeding. If a UDRP administrative panel decides that a domain name registration should be cancelled or transferred, ICANN will implement that decision ten business days after the administrative panel's decision unless it receives official notice that a lawsuit has been commenced. If such notice is received, ICANN will take no further action until it is notified of a resolution between the parties, evidence that the lawsuit has been dismissed or withdrawn, or a Court order determining which party has the right to use the domain name.

In 2019 alone, UDRP proceedings have resulted in the transfer of confusingly similar domain names being used in bad faith to major corporations, law firms, and non-for-profit entities including the Ford Motor Company, Virgin Enterprises, Dell, Discover Financial Services, Capital One, Microsoft, Google, Disney, Clifford Chance LLP, Linklaters LLP, McGuireWoods LLP, Baylor University, and the U.S. Green Building Council. The broad adoption of UDRP proceedings by such major entities indicates that it is viewed as a cost-effective and reliable method for resolving domain name disputes.

C. Reverse Domain Name Hijacking Claims

The UDRP process can be abused by parties engaging in "reverse domain name hijacking" or "reverse cybersquatting." Reverse domain name hijacking refers to the practice of

attempting to secure a domain name by making claims against a domain name's purportedly cybersquatting owner. When such a practice occurs, smaller organizations or individuals may be intimidated into transferring ownership of their domain names in order to avoid legal action, or may lose their domain names as result of a UDRP proceeding, notwithstanding their legitimate claims to the domain name.

The ACPA provides victims of reverse domain name hijacking with some measure of recourse. If a complainant in a UDRP proceeding makes a knowing and material misrepresentation to a UDRP panel, resulting in the transfer of a domain name, the aggrieved party can bring an action under 15 U.S.C. §1114(2)(D)(iv) of the ACPA and may seek damages, including costs and attorney's fees, as well as injunctive relief. Even in the absence of a misrepresentation to a UDRP panel, a domain name registrant whose domain name has been suspended, disabled, or transferred under a UDRP proceeding may, pursuant to 15 U.S.C. §1114(2)(D)(v) and upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by the registrant is not unlawful and may obtain injunctive relief, including the reactivation or re-transfer of the domain name.

Reverse domain name hijacking claims are relatively rare, and cases involving allegations that knowing and material misrepresentations were made to a UDRP panel are even rarer. In *Wang v. Societe du Figaro*, 2018 U.S. Dist. LEXIS 13119 (S.D.N.Y. Jan. 26, 2018), *report and recommendation adopted* 2018 U.S. Dist. LEXIS 106728 (S.D.N.Y. June 26, 2018), the Court rejected plaintiff's claim that the owner and publisher of the French newspaper *Le Figaro* had provided a UDRP panel with false, incomplete, and misleading information in order to gain control of the <lefigaro.news> domain name. Plaintiff, a purported patron of the arts and opera fan, claimed that he had registered the <lefigaro.news> domain name in order to create a general performance arts news and opera blog and that he chose the domain name as a tribute to the similarly titled Mozart opera. The owner of the *Le Figaro* newspaper commenced a UDRP proceeding, which resulted in a finding that plaintiff had no right or legitimate interests in the domain name, that the domain name had been registered in bad faith, and ordered the transfer of the domain name to the newspaper owner. Plaintiff then brought suit in the Southern District of New York, alleging violations of both reverse domain hijacking provisions of the ACPA. The Court concluded that plaintiff did not have a "bad faith intent to profit" from the domain name registration and that thus, his registration and use of <lefigaro.news> was not unlawful. The Court noted that "the bad –faith standard applied by the UDRP panel differs from the standard set out in [the ACPA.] Although [the ACPA] requires domain-name registrants to have 'a bad faith intent to profit,' the UDRP policy's definition of 'bad faith' appears to be broader—without necessarily requiring any intent to profit."

However, the Court rejected plaintiff's contention that the newspaper had made material or knowing misrepresentations to the UDRP panel, entitling plaintiff to damages. To the extent that any representations to the panel were mistaken, they were not material and plaintiff could not establish that defendants knowingly misrepresented any facts to the UDRP panel.

D. Trademark Clearinghouse and the Uniform Rapid Suspension System

In a further effort to protect trademark holders' rights in connection with domain names, ICANN has established the Trademark Clearinghouse, which is a database of verified trademark records from multiple global regions. Trademark holders can submit information about their trademarks, the jurisdiction where the trademark is registered, and proof of use, and the information is verified by ICANN service providers. A copy of ICANN's educational graphic concerning their trademark protection program is attached at the end of this article.

One advantage of registering with the Trademark Clearinghouse is that it provides registrants an early opportunity to acquire domain names when new generic top level domains (gTLDs) become available. If a trademark is registered with the Trademark Clearinghouse and proof of use is shown, a trademark holder has the opportunity to participate in a registry "Sunrise Period." During the Sunrise Period, which begins at least thirty days before domain names for new gTLDs are made available to the public, registrants are offered an advance opportunity to register domain names corresponding to their marks. New gTLDs recently made available to the public include .sport, .fan, and .dev, and the Sunrise Period for .inc begins on March 27, 2019.

Once the Sunrise Period ends and new gTLD domain names are available to the general public, the "Trademark Claim" period begins. During said period, which lasts for at least ninety days after general registration begins, anyone attempting to register a domain name matching a mark that is recorded in the Trademark Clearinghouse will receive a notification regarding the registered mark information. If the notified party proceeds to register the domain name, the Trademark Clearinghouse will send a notice to the trademark holders with matching records in the Clearinghouse, informing them that someone has registered the domain name. Registrants can also opt to receive additional notifications if someone attempts to register a domain name matching their trademark after the claims period expires.

For new gTLDs, ICANN has also introduced an even more streamlined dispute resolution mechanism than the UDRP, known as the Uniform Rapid Suspension System, or URS. As with the UDRP, URS proceedings are administered by ICANN-approved service providers, including the National Arbitration Forum. The URS system is designed to complement the UDRP, providing a lower-cost and still faster path to relief in the most clear-cut cases of infringement.

Filing a URS Complaint costs only $375, and disputes are resolved within a matter of weeks. Under the URS system, a domain name can be suspended and redirected, but not transferred. Thus, the URS dispute resolution mechanism only makes sense where a trademark owner has no interest in acquiring and using the infringing domain name.

A Complainant can gain relief under the URS system if he or she can show that the registered domain name is identical or confusingly similar to a work for which the Complainant holds a valid national or regional registration and that is in current use, that the registrant has no legitimate right to or interest in the domain name, and that the domain was registered and being used in bad faith. In URS proceedings, the fact that a trademark has been registered with and verified by the Trademark Clearinghouse constitutes proof of use. Thus, another benefit of the Trademark Clearinghouse is that it streamlines the burden of proof in URS disputes.

III. Scams and Assorted Issues

"*It's totally outrageous ... for someone to take these domain names and then solicit funds, run them through what looks like a legitimate charity using pictures and other hurricane victims, when in reality that money was running to his hate sites."*

~ Jay Nixon
Ex-Governor of Missouri
https://www.azquotes.com/author/40924-Jay_Nixon

As we all now know, various scams and schemes abound on the Internet, including in connection with the registration and use of domain names. Some scams, such as the one referred to in the quote above, are little more than charity scams that occur on the "virtual corner." In response to a well-publicized tragedy, scammers often rush to register domain names that ostensibly relate to the event, e.g., "__floodvictims.com" or "faminein___.net." The fact that the domain name itself identifies the event give any solicitation for contributions a veneer of legitimacy that may be undeserved. "Contributions" are kept by the domain name registrant, who is usually not associated with any charity. The non-profit organization, Charity Navigator, offers users the ability to check on purported charities and offers a checklist of steps to take to avoid online charitable scams. *See,* *https://www.charitynavigator.org/index.cfm?bay=content.view&cpid=313*.

Another common domain name scheme is carried out by unscrupulous IT vendors that use their own identity and contact information to register the company's domain name. In the event of a breakdown in the contractual relationship, such as a fee dispute, the IT vendor has control of all Internet processes associated with the domain name and can lock the company out, post offensive content or even transfer it away from the company that has built its online presence based on its beneficial ownership of the name. In many cases, the scheme may not be exposed until substantial harm has been done to the actual domain name holder.

A. Abusive Registrations

Abusive registration of a domain name is one method used to effectuate a fraudulent scheme. An abusive registration is a type of cybersquatting. It occurs when a domain name is registered that contains a well-known mark coupled with generic words, typosquatting, (subtracting, adding or switching the order of letters in the name) or other misleading practices that have no legitimate purpose other than to trick or misdirect web users away from the actual site that they seek. Abusive registrations are often addressed through ACPA claims.

With most ACPA-violation domain name scams, it is nearly impossible to identify the individual who is committing the fraud, and therefore, courts often do not have personal jurisdiction over the fraudster. Instead, plaintiffs generally assert an *in rem* cybersquatting action where the plaintiff's remedies are limited to either: (i) the transfer of the domain names to the owner of the mark, or (ii) the forfeiture or cancellation of the domain names. *See Alfieri-Crispin v. Li Ting,* No. 1:15-cv-608, 2015 WL 5560000, at *4 (E.D. Va. Sept. 11, 2015) (citing 15 U.S.C. § 1124(d)(2)(D)(i)).

In an interesting 2018 case from the U.S. District Court for the Eastern Division of Virginia in 2018, *Latham & Watkins LLP v. Hiring-LW.com,* No. 1:17-cv-1368, 2018 WL 3214260, at *2 (E.D. Va. June 11, 2018), the court issued a decision in favor of the international law firm of Latham & Watkins LLP and against the abusive domain name registrant defendant, Hiring-LW.com. Latham & Watkins alleged that the domain name registrant defendant violated the ACPA. The defendant had in fact registered the domain name of "hiring-LW.com" and was utilizing it to impersonate the law firm in order to solicit money from the firm's job applicants. According to the WhoIs database, the domain name was registered under the name, Perfect Privacy LLC., a company that provides "private registration services" to domain name registrants. For a fee, domain name registrants could designate Perfect Privacy LLC as the registrant and required contacts. Thus, using Perfect Privacy LLC allowed the true registrant of the domain name to avoid disclosing their identifying information and remain anonymous.[5]

In this case, Latham & Watkins had learned of various scams being perpetrated against the public using the domain name "hiring-LW.com." The scams were accomplished by impersonation of various members of the law firm. In one version of the scam, the scammer would send emails regarding potential employment with Latham & Watkins using the "hiring-LW.com" domain name that would ultimately lead to the targets receiving deceitful offers for work-from-home positions. The scammers would thereafter mail a check to the victim applicant and direct them to furnish a home office and refund the remaining amounts back to the target. By the time the initial check from the scammers bounced, the victim applicant had already purchased the home office equipment and sent the scammers the "remaining" funds from their personal bank accounts. Other victim applicants were similarly directed to submit a check to cover training materials with a fraudulent promise of future reimbursement. *See id.* at *2. This lawsuit followed.

Not surprisingly, no one filed an answer on behalf of the domain name registrant defendant. As such, Plaintiff moved for default judgment, and at the hearing, no one appeared on behalf of the domain name registrant defendant. Ultimately, the court held that Latham & Watkins had established a violation of the ACPA. In reaching its decision, the Court determined that Latham & Watkins had established the necessary elements.

The court found that the current registrant of the domain name had "bad faith intent to profit from the domain name." The court based this determination on the list of factors set forth in 15 USC § 1125(d)(1)(B)(i). The court highlighted that the Plaintiff had established: (i) that the scammers were using the domain name "for commercial gain by creating actual confusion as to the domain name's ownership in a manner that harmed plaintiff's goodwill in the marks," and (ii) that the use of "LW" in the domain name "is distinctive and famous within the meaning of 15 U.S.C. § 1125(c) as evidenced by plaintiff's registration and long-standing use of the mark." *Id.* at *5. The court also held that Plaintiff had established that the domain name was "confusingly similar to the distinctive mark owned by plaintiff." The court focused on the facts that the scammers were holding themselves out as working for the Plaintiff law firm, that they used the

[5] It is not clear that what impact ICANN's Temporary Specifications, concerning privacy and the WhoIs database, will have on services like those offered by Perfect Privacy LLC.

Plaintiff law firm's email format, and that they offered positions of employment with the Plaintiff law firm.

As Latham & Watkins had established a violation of the ACPA, the court ordered that the registrar change the registrant of record to the name of the Plaintiff. *Id.* Latham also placed a page on its website warning visitors of the hiring and other scams that were being perpetrated, including as to false inheritance, false financial statements, tax liability and attachments leading to phishing sites. *https://www.lw.com/EmailScamWarning*.

In another case example from the same court, the Eastern District of Virginia, *Atlas Copco AB v. Atlascopcoiran.com,* 533 F. Supp. 2d 610 (E.D. Va. 2008), Plaintiff, Atlas Copco AB filed an *in rem* action alleging a violation of the ACPA against various Defendant Domain Names. These domain names were very similar to Atlas Copco's own registered domain name, and included: atlascopcoiran.com, atlascaspian.com, atlascaspian.net, atlascaspian.org, atlascaspian.biz, atlascaspianir.com, atlascaspianiran.com, atlascaspian.us, etc. The disputed domain names had been used by the defendant registrants in connection with a phishing scam. *See* Discussion Below. The court held that it had *in rem* jurisdiction over the Defendant Domain Names; however, the court could not obtain *in personam* jurisdiction over the registrant of these domain names because the individuals were located in Iran, Afghanistan or India. Thus, the court proceeded pursuant to *in rem* jurisdiction solely against the Defendant Domain Names (and not the registrant).

In this case, the court analyzed Plaintiff's motion for summary judgment on the Defendant Domain Names' violation of the ACPA. The court held that the evidence established as a matter of law the requisite elements of Plaintiffs' cyber-piracy claim set forth in the ACPA (15 USC § 1125(d)(1)(A)). In pertinent part, the ACPA provides that "A person shall be liable in a civil action by the owner of a mark . . . if, without regard to the goods or service of the parties, that person – (i) has a bad faith intent to profit from that mark . . ." and "(ii) registers, traffic in, or uses a domain name that . . . (l) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark." *Id.* at 613.

The court found that the domain names were being used by the Defendants with "bad faith intent to profit" from the Plaintiff's trademark. The court also found that the Defendants' use of the domain names in conjunction with a phishing scam established the requisite bad faith intent to profit from the Plaintiff's trade mark. The Plaintiff also sufficiently established that their trademark was distinctive and strong throughout the United States and the world and that the Defendant was using the domain names to "deceive and divert Internet users seeking genuine Atlas Copco-brand products or services." *Id.* at 614.

As a result of the foregoing, the court granted the Plaintiff's motion for summary judgment and ordered that the disputed domain names were to be reregistered in the name of the Plaintiff.

In a case issued by the U.S. District Court for the Southern District of New York in 2007, the court examined whether the domain name "www.chinabarbie.com," which linked to a

pornographic website and sold memberships to the site, violated Mattel's rights pursuant to the ACPA. *See Mattel, Inc. v. Global China Networks, LLC,* No. 07-cv-7418, 2007 WL 3332662 (S.D.N.Y. Oct. 23, 2007). The court held that the disputed domain name, chinabarbie.com, had cyber-squatted upon, infringed upon, and/or diluted Mattel's registered trademarks for the mark "Barbie" in violation of the ACPA. As such, the court ordered that the Domain Name Defendants and the registrar of the subject domain names must transfer the domain name "chinabarbie.com" to Mattel, Inc. *See id.* at *1.

These are just three recent examples where companies were victims of domain name scams and their only available remedy was through the courts. Fortunately, in these examples, the court ordered the governing registrar to change the registrant name of the fraudulent, stolen, or abusive domain names to the plaintiff-company.

B. Phishing Scams

Phishing is "a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly." Merriam-Webster Dictionary, "Phishing," last visited on Mar. 15, 2019, *available at* *https://www.merriam-webster.com/dictionary/phishing*. As the Federal Trade Commission warns, a phishing scam occurs when a scammer uses fraudulent emails, texts, or copycat websites to get the target to share valuable personal information – such as account numbers, Social Security Numbers or log in and passwords credentials, that are then used to steal the target's money, identity or both. *See* *https://www.consumer.ftc.gov/articles/0003-phishing*.

According to the ICANN's blog about phishing, criminals and scammers impersonate trusted senders in email or a website to gain the user's trust so that they can obtain access to sensitive data and/or convince the sender to send them money. *See* ICANN, "What You Should DO If You Receive A Suspected Fraudulent ICANN Email," (Dec. 30, 2016), last visited Mar. 13, 2019, *available at* *https://www.icann.org/news/blog/what-you-should-do-if-you-receive-a-suspected-fraudulent-icann-email*. Unfortunately, using domain names that closely relate to their real counterparts, phishing emails may appear to come from various trusted sources – including your domain name/trademark registrar, or other business partners.

Ironically, even ICANN has itself been misidentified as the source of phishing communications. In response, ICANN has outlined ways to make sure a specific email really came from ICANN directly. ICANN advises that typically the phishing email will ask the reader to reply to the message, call a certain telephone number, click on a link, or open an attached file in order to steal their personal information. ICANN recommends that if you receive a suspicious email, that you should forward the email to *globalsupport@icann.org* so that they can determine if the email is fake and if so, can work to get the email source shut down.

Further, while these emails generally look official, ICANN highlighted three ways to help you to spot a fake email. One, there will often be a false sense of urgency. The scammer will often say that your account will be in jeopardy if something critical is not updated (or paid for) right away. Two, the email will contain fake links. While the link may look real, it may in fact be leading you elsewhere. ICANN instructs users to hover your mouse over the link to check

which website URL the link is connected to prior to clicking on anything. Three, the email will have an attachment. ICANN advises that a real email from ICANN will NEVER include an attachment or software that you are required to download. Attachments can contain malware, and so you should never open one unless you are certain that it is legitimate. ICANN's suggestions as to how to deal with suspicious emails should be followed regardless of the domain name form which they appear to be sent.

In addition to seeking personal information, phishing emails often seek credit card or payment information. Specifically, there is a common phishing scheme that fraudulently offers registration renewals to domain name registrants. In an article published by ICANN in September of 2014, ICANN warned that online scammers have targeted domain name registrants with a "registration renewal scam" in order to fraudulently obtain financial information. *See* ICANN, "Be Careful What You Click: Alert of New Fraudulent Domain Renewal Emails," (Sep. 29, 2014), last visited on Mar. 13, 2019, *available at* *https://www.icann.org/news/blog/be-careful-what-you-click-alert-of-new-fraudulent-domain-renewal-emails*.

Generally, to carry out a registration renewal scam, the scammer will send an email to a domain name registrant that offers an opportunity to renew their registration by selecting the "click here" button to renew online at attractively low rates. These emails appear to be sent by ICANN directly and often even use ICANN's branding and logo in the email message and on the fake renewal webpage. If the registrant clicks the link and enter their information, then the scammers collect the credit card and personal information that victims submit.

ICANN warned that they do not process domain registrations, nor collect fees, from registrants directly. Also, registrants should be advised that the WhoIs Public Internet Directory (accessible here: *http://whois.icann.org/en*) allows a registrant to look up the date in which their registration expires.

Another version of this type of domain name scam begins with an email or mailed letter that comes from a competing domain registrar that is different from the one with whom the registrant has actually registered their domain name (or a fraudulent, non-existent registrar). In this similar scenario, a registrant will receive a letter via email or regular mail advising them that their domain name is going to expire unless the registrant takes immediate action and pays them. This is a scam – and a version of "domain slamming" – where an internet service provider or domain name registrar attempts to trick customers of different registrar companies into unknowingly switching from their existing registrar to the scamming registrar. They do so under the pretense that the customer is simply "renewing" their subscription with their existing registrar, when in fact the registrant is changing to a different registrar (or is simply paying a fraudulent, non-existent registrar). *See* Team MHS, "Domain Registration Scams NEVER Seem to End! Always Look Twice Before Crossing the Streets of Domain Registry," (Jan. 5, 2019), last visited Mar. 14, 2019, *available at* *https://mainehost.com/domain-registration-scams-2/*. Either way, the registrant is being scammed out of money and scammed into changing registries for their domain name.

C. Chinese Domain Name Scams

On May 29, 2012, the China Internet Network Information Centre ("CNNIC") issued new domain name registration rules and relaxed its local presence requirement. *See* CNNIC, "CNNIC Implementing Rules of Domain Name Registration," (Aug. 30, 2012), last visited Mar. 13, 2019, *available at* https://cnnic.com.cn/PublicS/fwzxxgzcfg/201208/t20120830_35735.htm. Now, individuals and foreign companies may register domain names with the .cn website extension in their own name even if they do not have a local presence in China using CNNIC-approved overseas registrars. They also no longer need to have a third-party Chinese trustee. Registrants still need to provide supporting information such as proof of identity/company registration and a signed letter of commitment. In light of these relaxed CNNIC Rules, an individual or a foreign company can register for a .cn domain name easily, regardless of where in the world they do business. Moreover, given the size of China's population and its status as an economic force in the world, many businesses consider expansion of their online presence onto the .cn TLD to be an attractive, cost-effective way to enter the Chinese marketplace.

Unfortunately, the relaxation of the CNNIC Rules has led to a high volume of scams. One example is referred to as the Duplicate Domain Name Scam. This type of scam is frequently carried out by Asian companies who pressure large firms and companies to register identical domain names in Asian Top-Level-Domains. Some examples of Asian Top-Level-Domains include: .cn (China), .hk (Hong Kong), .jp (Japan), and .in (India).

Like most phishing schemes, the Duplicate Domain Name Scam begins with a simple email. The email is generally claimed to be from an accredited Asian registrar, most often located in China. This email will (dishonestly) notify the company that the Asian Registrar has received an application from another company that may negatively affect the registrant company's brand name and/or domain names. The e-mail will further advise that the Registrar has not yet approved this third-party company's application, and they are instead sending this email as a "courtesy" seeking the registrant's permission for the third-party company to register using this very similar brand name. *See* Betsy McLeod, "What You Need to Know about Chinese Domain Name Scams," (Feb. 5, 2017), last visited Mar. 14, 2019, *available at* https://www.bluecorona.com/blog/chinese-domain-name-scams.

The email will also explain that they are providing the registrant with the first-option to register for these additional domain names in order to "protect" their company's brand and website. The additional domain names that the registrant has the first-option to register for will generally include a laundry list of domain names used in Asia. For example, the list will include the company's most frequently used SLDs that are linked to the company's website, used for emails, or other Internet uses, but the proposed list will offer to the register those SLDs in.cn, .in, .com.cn, .org.cn, .net.cn, and many other TLDs. Of course, the Asian Registrar will be offering these additional domain name registrations at a hefty cost for each unique domain name. Generally, unless the registrant regularly does business in China or India, the registrant will have no need to register for these particular domain names.

D. Elusive Transfers

Another type of domain name related scam is known as an elusive domain name transfer. One example of this type of scam is when a scammer steals a registrant's account information and password and fraudulently transfers their domain name to a different registrar in order to take control of it. Then the scammer offers the domain name for sale on the new registrar's sales platform.

That is exactly what happened in the case of *Alfieri-Crispin v. Li Ting,* No. 1:15-cv-608, 2015 WL 5560000, at *2 (E.D. Va. Sept. 11, 2015). In this case, an unknown individual stole the password to the Plaintiff's registrant account and altered the domain name registration record for the domain name "x3.com." *Id.* Plaintiff alerted their registrar that their domain name had been stolen. But the very next day, someone submitted a fraudulent form of authorization and initiated a fraudulent email request for transfer of the domain name away from Plaintiff's registrar to a different registrar. After the theft, Chinese brokers listed the domain name for sale on the domain name market and it was offered for sale on the new registrar's sales platform. Two weeks later, Plaintiff's counsel arranged for the new registrar to place a lock on the "x3.com" domain name in order to prevent further loss or transfer while the lawsuit was pending.

Here, Plaintiff moved for default judgment. In performing the two-prong analysis for violations under the ACPA, the Court held that the Plaintiff had satisfied both elements and thus, that ownership and control of the domain name "x3.com" must be transferred to the Plaintiff.

In a similar case example, based upon a Report and Recommendation of the assigned Magistrate Judge, *Combs v. Doe,* No. C-10-01120, 2011 WL 738052 (N.D. Cal. Feb. 23, 2011), Plaintiff brought a lawsuit claiming that the Defendant stole her domain names and deleted the website. Specifically, Plaintiff claimed that the Defendant hacked into her email account and fraudulently obtained a new password, which enabled the Defendant to transfer the domain names and delete the website. *Id.* at *1. In this case, Plaintiff went to great lengths to attempt to ascertain the Defendant's true identity, to no avail. *Id.* The Plaintiff sought: monetary damages, attorney's fees, declaratory relief and injunctive relief. The court granted Plaintiff $20,000 in actual damages, but denied Plaintiff's claim for attorney's fees because she had failed to cite to any authority for a fees award. The court also granted Plaintiff's request for declaratory relief and stated that "because the host companies require a court order identifying the rightful owner of the Website and Domain Names, declaratory relief is proper and necessary." *Id.* at *3. Finally, the Court also granted Plaintiff's request for a permanent injunction and held that "the registrar should be authorized to transfer the Website and Domain Names to plaintiff, at plaintiff's request and upon providing a copy of the other, whether or not defendant has authorized the transfer." *Id.*

Domain Names, WhoIs and Privacy

"*In digital era, privacy must be a priority*."
~ Al Gore
American Vice President
https://www.brainyquote.com/quotes/al_gore_586409

The question of domain name registration and privacy issue has been evolving for some time. Registrars were obligated as a term of their ICANN accreditation to maintain "WhoIs" databases which publicly listed, *inter alia,* the name and contact information for each registered domain name. The use of accurate information was seen as essential for honest parties to address their domain name disputes. Conversely, inaccurate contact information might be considered a sign of abusive registration intended to mask the identification of the registrant. As DNS registration grew, registrant privacy interests became apparent. As a result, WhoIs data was increasingly provided by private registrations, in which the contact information designated an unknown registrant's paid agent, often a service provided by the registrar itself. In the event of a domain name dispute, the claimant's statement would be forwarded to the registrant with the choice of either transferring the domain name or identifying itself and defending the claim.

In response to European Union's adoption of the General Data Protection Rule which went into effect on May 18, 2018, ICANN adopted its Temporary Specification, effective May 25, 2018. The Temporary Specification modifies WhoIs requirements without disposing of the requirement that registrars and registries continue to operate WhoIs directories under the Registration Data Access Protocol("RDAP") *https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#appendixA*. In that regard, ICANN renewed its commitment to the "mission" of coordinating the "stable operation of the Internet's unique identifier systems", by requiring gTLD registrars and registries to collect registrant information in aid of *inter alia* resolution of domain name registration disputes, maintenance of up to date information concerning registered names and name services, procedures to avoid disruptions of domain name registrations due to suspension or termination of registry operators or registrant, or transfer of registration data when a registrant transfers the registration to a different registrar. *https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#3*

The Temporary Specification is intended to provide a method that will allow ICANN and gTLD registry operators and registrars to comply with existing ICANN contractual obligations, such as providing registrant information for purposes of UDRP, in light of GDPR. *https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf.* It is intended to maintain "robust collection of Registration Data (including Registrant, Administrative, and Technical contact information), but restrict[] most Personal Data to layered/tiered access." Thus, users with "legitimate and proportionate purpose for accessing the non-public Personal Data will be able to request such access through Registrars and Registry." Moreover, users are able to contact the Registrant, or Administrative or Technical Contacts, through an "anonymized email or web form." Interestingly, despite the fact that GDPR protections are only provided to natural persons in the European Economic Area ("EEA"), the

Temporary Specification does not require Registrars to differentiate between individuals and legal entities

Finally, although there is no uniform, worldwide understanding of privacy (or even a national privacy standard in the US), ICANN has stated that the Temporary Specification applies regardless of whether the registrar or registrant is in the EEU and even where the Registrar exclusively registers names on behalf of non-EEA registrants. *https://www.icann.org/resources/pages/gtld-registration-data-specs-faqs-2018-06-22-en*. It nevertheless appears that the Specification itself may provide some differentiation between what registrars and registries may do depending on the involvement of EEU participants.

IV. Some Practical Domain Name Practices

"No one wants a domain with their name on it owned by somebody else."
~Jack Abramoff
Businessman, Lobbyist and Convicted Felon
https://www.brainyquote.com/quotes/jack_abramoff_505663

It is, of course, the goal of every business to build an online presence that is recognizable, easy to find, free from controversy and sets the business apart from the competition. To maximize that potential, domain name selection and continued monitoring are essential.

It is often suggested that a domain name should be relevant to the business i.e., represent the products or services that are being offered and/or the clientele that the business hopes to attract. Some businesses chose to go with truly fanciful names that will set them out from the pack and, once found, be easy to remember. On the other hand, there is well-documented practice of Internet users simply typing in generic descriptive word rather than searching for any specific site. As an example, someone interested in winter sports might initiate his/her search by entering "ski", "skiing" or "skiequipment" followed by ".com" into their browser to see what is returned. A domain name that included those terms – i.e. "samski.com" or "downhillskiing.com" – might have a better rate of being returned on the search – especially if search engine optimization ("SEO") is used. [6]

Conversely, while the domain name should be descriptive, it nevertheless needs to be unique. There is always a danger of accidental or deliberate misdirection from the business' site to that of a competitor based upon user confusion. Indeed, the practice of "typosquatting" counts on such mistakes by registering non-infringing, but similar domain name strings for the purpose of attracting visitors to their sites.

Another important consideration is that the business' domain name does not violate the trademark or other intellectual property right of another. Domain names are like the immortals in Highlander—"there can be only one." Whereas it was once possible for non-competitive businesses to share names in different commercial spheres, that is not possible for domain names. Unfortunately, these issues often first come to the forefront only when two unrelated

[6] The domain names used in the example are, in fact, registered as of the date this article was written.

businesses, perhaps geographically separated in the real word, attempt to inhabit the same online location though their domain name selection. As such, robust trademark practices by businesses should include checking for potential trademark issues before substantial investment is made in the use domain name. It is also important for business to regularly police the Internet to identify new, violating uses of the business' intellectual property as soon as they can be identified.

There are several excellent resources available, both free and for a fee, which can be used to aid in the selection and monitoring of domain names. First and foremost, as discussed above, under its accreditation agreement with ICANN, each registrar must maintain WhoIs data as does ICANN itself. *See,* https://whois.icann.org/en. Even with the new privacy limitations placed on WhoIs data, through a WhoIs search it can be determined whether a domain name is, in fact, registered, its "creation date", last update, registrar and contact for registration abuse.

Other useful tools are available to explore a domain names history even further as prior use of a previously registered domain name can likewise create problems. Domain names exist only if they are registered. If a domain name registration is cancelled, expired or non-renewed, the domain name becomes available for another's use. However, the fact that it is no longer being operated by the prior registrant is not immediately apparent to anyone who accesses the content affiliated with the domain name. Few, if any sites hang "Under New Management" banners on their homepages, but, perhaps they should. A previously registered domain name may have been used, for example, to disseminate pornography or other content that is objectionable to the new registrant and with which it does not wish to associate. Moreover, the fact that a domain name was previously used by a competitive, related enterprise could be either a boon or curse as the new registrant may be able capitalize on prior customer good will or be dogged by the previous registrant's bad business practices. The domain names prior usage may also impact Google's ranking of the site in later searches well-after the registrant has changed.

WhoIs databases reflect current registration status. However, there are online tools that offer WhoIs history that claim to be able to provide identification of the prior registrant, even when that information is no longer offered in the WhoIs database. For example, one such site, *http://research.domaintools.com/research/whois-history/* [7]advertises that it has captured WhoIs data of millions of websites back to 1995, which enable its paid users to explore domain name history.

Another tool is the Internet archive service, "The Wayback Machine." The Wayback Machine, now operated by the non-profit Internet Archive, offers a free tool to search *inter alia* for the historical content of a website. *See* *https://archive.org/web/web.php*. The Wayback Machine's archival mission was begun in 1996 in recognition of the ephemeral nature of Internet content. It now boasts that it contains the history of over 349 billion web pages on the Internet. While it is somewhat random as to which web pages were added and how often, generally speaking, the Wayback Machine offers domain name registrants an opportunity to view at least some of the content that was linked to their domain name in prior usage.

[7] The discussion in this article of any privately owned domain name or website tools should not be considered an endorsement of the product, the safety of using the tool or the results. Readers should make their own determination as to which, if any, of the tools are right for their purpose.

"Norton Safe Web" is a tool that has both free and paid components. It is designed to assist web users in determining the safety of web sites before it is visited. Nevertheless, it can be also be used to assess the safety rating of a website that was previously associated with the domain name that the business is interested in. *https://safeweb.norton.com/.*

Finally, a search of Google and its analytics for the website can yield valuable information about prior use of the domain name and ways to address any issues that were the result of the prior registrant's violation of Google's policies. *https://support.google.com/webmasters/answer/35769?hl=en.* Indeed, Google expressly invites new registrants that whose domain names were associated with a site with "manual actions" against it due to the contact of the prior registrant to "fix the issues listed in the report" and then follow with them for reconsideration. *https://support.google.com/webmasters/answer/9044175?hl=en.* Of course, extensive penalizing conduct by Google concerning the domain name's prior usage may give a business pause as to whether there is so much accumulated ill-will associated with the domain name, that it should reconsider its registration of the domain name.

In the 21st Century, domain names provide "addresses" for the virtual world in which we all live and conduct business. Bob Parsons, billionaire founder and ex-CEO of domain name registrar GoDaddy stated that:

> *"A domain name is your address, your address on the Internet. We all have a physical address; we're all going to need an address in cyberspace. They're becoming increasingly important. I believe we'll get to the point where when you're born, you'll be issued a domain name."* *https://www.brainyquote.com/quotes/bob_parsons_477659*

Although we have yet come that far, domain names should be treated like the valuable commodities they are.

The Internet is Expanding

Learn how to protect your trademark

22 > 1300

In the coming months, the number of generic Top-Level Domains on the Internet will explode from 22 to over 1,300

+3

Rights Protection Mechanisms

are now in place to support and protect trademark holders - before anything happens, and in case something does in the future

Trademark Clearinghouse

STAGE 01

BEFORE THE NEW DOMAINS GO LIVE

The Trademark Clearinghouse is a one-stop-solution to help protect a trademark across every new generic Top-Level domain that comes online

The first stage in protecting your rights is to submit a mark to the Trademark Clearinghouse

Rights Protections

Sunrise Services
Priority access to request domain names associated with your trademark(s)

Trademark Claims Service
Notification to a Rights Holder after registration, allowing for immediate action if the domain registered is infringing rights

Submit your Trademark

http://trademark-clearinghouse.com

STAGE 02

AFTER THE DOMAINS GO LIVE

Uniform Rapid Suspension System

If rights infringement occurs after a domain goes live, the URS comes into effect

Within 24 hours of a valid complaint, an infringing domain will be locked

Find out more @

http://newgtlds.icann.org/urs

STAGE 03

AFTER THE DOMAINS GO LIVE

Trademark PDDRP*

Trademark infringement is often portrayed as being a registrant problem, such as cyber-squatting. But what if a Registry Operator were to be involved?

The Trademark Post-Delegation Dispute Resolution Procedure addresses instances where a Registry Operator is complicit in trademark infringement

Find out more @

http://newgtlds.icann.org/pddrp

ICANN and the Internet community are laying the foundation for a broader, more mature Domain Name System

To find out more about the **biggest change** to the Internet since it was created visit

http://newgtlds.icann.org

ICANN New Generic Top-Level Domains

* Post-Delegation Dispute Resolution Procedure

COMPLAINT TRANSMITTAL COVERSHEET

Attached is a Complaint that has been filed against you with the World Intellectual Property Organization (**WIPO**) Arbitration and Mediation Center (the **Center**) pursuant to the Uniform Domain Name Dispute Resolution Policy (the **Policy**) approved by the Internet Corporation for Assigned Names and Numbers (**ICANN**) on October 24, 1999, the Rules for Uniform Domain Name Dispute Resolution Policy (the **Rules**) approved by ICANN on September 28, 2013, and in effect as of July 31, 2015, and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the **Supplemental Rules**) in effect as of July 31, 2015.

The Policy is incorporated by reference into your Registration Agreement with the Registrar(s) of your domain name(s), in accordance with which you are required to submit to a mandatory administrative proceeding in the event that a third party (a **Complainant**) submits a complaint to a dispute resolution service provider, such as the Center, concerning a domain name that you have registered. You will find the name and contact details of the Complainant, as well as the domain name(s) that is/are the subject of the Complaint in the document that accompanies this Coversheet.

Once the Center has checked the Complaint to determine that it satisfies the formal requirements of the Policy, the Rules and the Supplemental Rules, it will forward an official copy of the Complaint, including annexes, to you by email as well as sending you hardcopy Written Notice by post and/or facsimile, as the case may be. You will then have 20 calendar days from the date of Commencement within which to submit a Response to the Complaint in accordance with the Rules and Supplemental Rules to the Center and the Complainant. You may represent yourself or seek the assistance of legal counsel to represent you in the administrative proceeding.

- The **Policy** can be found at https://www.icann.org/resources/pages/policy-2012-02-25-en

- The **Rules** can be found at https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en

- The **Supplemental Rules**, as well as other information concerning the resolution of domain name disputes can be found at http://www.wipo.int/amc/en/domains/supplemental/eudrp/newrules.html

- A **model Response** can be found at http://www.wipo.int/amc/en/domains/respondent/index.html

Alternatively, you may contact the Center to obtain any of the above documents. The Center can be contacted in Geneva, Switzerland by telephone at +41 22 338 8247, by fax at +41 22 740 3700 or by email at domain.disputes@wipo.int.

You are kindly requested to contact the Center to provide an alternate email address to which you would like (a) the Complaint, including Annexes and (b) other communications in the administrative proceeding to be sent.

A copy of this Complaint has also been sent to the Registrar(s) with which the domain name(s) that is/are the subject of the Complaint is/are registered.

By submitting this Complaint to the Center the Complainant hereby agrees to abide and be bound by the provisions of the Policy, Rules and Supplemental Rules.

Before the:

WORLD INTELLECTUAL PROPERTY ORGANIZATION
ARBITRATION AND MEDIATION CENTER

[NAME AND ADDRESS OF COMPLAINANT] (**Complainant**) -v- *[NAME AND ADDRESS OF RESPONDENT]* (**Respondent**)	**Disputed Domain Name(s):** *[<the disputed domain name(s)>]*

COMPLAINT

(Rules, Paragraph 3(b); Supplemental Rules, Paragraphs 4(a), 12(a), Annex E)

I. Introduction

[1.] This Complaint is hereby submitted for decision in accordance with the Uniform Domain Name Dispute Resolution Policy (the **Policy**), approved by the Internet Corporation for Assigned Names and Numbers (**ICANN**) on October 24, 1999, the Rules for Uniform Domain Name Dispute Resolution Policy (the **Rules**), approved by ICANN on September 28, 2013, and in effect as of July 31, 2015, and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the **Supplemental Rules**) in effect as of July 31, 2015.

II. The Parties

A. The Complainant

(Rules, Paragraphs 3(b)(ii) and (iii))

[2.] The Complainant in this administrative proceeding is *[provide full name and, if relevant, corporate or legal status.]*

[3.] The Complainant's contact details are:

Address: *[Specify mailing address]*
Telephone: *[Specify telephone number]*
Fax: *[Specify fax number]*
Email: *[Specify email address]*

[If there is more than one Complainant, provide the above information for each and arguments and evidence to support the consolidation of multiple Complainants in a single complaint in such cases, for example, where the multiple Complainants truly have a common grievance against the Respondent. Multiple Complainants may demonstrate a common grievance against the Respondent, for example, (1) where Complainants have a common legal interest in a relevant right or rights that are allegedly affected by the Respondent's conduct, or (2) where the multiple Complainants are the target of common conduct by the Respondent which has clearly affected their individual legal interests. See WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Overview 3.0"), section 4.11.]

[4.] The Complainant's authorized representative in this administrative proceeding is:

[If relevant, identify authorized representative and provide all contact details, including postal address, telephone number, fax number, email address; if there is more than one authorized representative, provide contact details for each.]

[5.] The Complainant's preferred method of communications directed to the Complainant in this administrative proceeding is:

<u>Electronic-only material</u>
Method: email
Address: *[Specify one email address]*
Contact: *[Identify name of one contact person]*

<u>Material including hardcopy (where applicable)</u>
Method: *[Specify one: fax, post/courier]*
Address: *[Specify one address, if applicable]*
Fax: *[Specify one fax number]*

Contact: *[Identify name of one contact person]*

B. The Respondent
(Rules, Paragraph 3(b)(v))

[6.] According to *[indicate why the person/entity identified in the Complaint has been identified as the Respondent, e.g., the concerned registrar's WhoIs database. (Information about the concerned registrar can be found on the Internic database at http://www.internic.net/whois.html)]*, the Respondent in this administrative proceeding is *[identify Respondent (the domain name holder), (including full name, and if relevant, corporate or legal status, place of incorporation and principal place of business, or residence) see WIPO Overview 3.0, section 4.4]*. Copies of the printout of the database search(es) conducted on *[date]* are provided as Annex *[Annex number]*.

[7.] All information known to the Complainant regarding how to contact the Respondent is as follows:

[Provide all contact details (postal address, telephone number, fax number, email addresses) for the Respondent, including those that may have been used successfully in the course of pre-complaint dealings and those available from any WhoIs look-up service.]

[If there is more than one Respondent, provide the contact details for each Respondent and describe the relationship between them, which justifies them being named in a common complaint. See WIPO Overview 3.0, section 4.11.]

III. The Domain Name(s) and Registrar(s)
(Rules, Paragraphs 3(b)(vi), (vii))

[8.] This dispute concerns the domain name(s) identified below:

[Identify precisely the disputed domain name(s). You are also invited to indicate the date(s) of domain name registration.]

[9.] The registrar(s) with which the domain name(s) is/are registered is/are:

[Provide the name and full contact details of the registrar(s) with which the domain name(s) is/are registered.]

IV. Language of Proceedings
(Rules, Paragraph 11)

[Paragraph 11(a) of the Rules provides that, subject to the authority of the Panel, the language of the proceedings shall be the same as the language of the Registration Agreement unless the Parties have otherwise agreed to proceeding in a different language. In the absence of such agreement, a complainant may submit a complaint in a language different to the Registration Agreement where a complainant requests that the language of proceedings be the same as that of the complaint and provides brief supporting evidence, including such documentation as pre-complaint correspondence between the parties, the identity of the parties, the nationality and place of residence of the parties, and any other evidence of a respondent's familiarity with the requested language. See WIPO Overview 3.0, section 4.5.]

[10.] To the best of the Complainant's knowledge, the language of the Registration Agreement is *[specify language of Registration Agreement]*, a copy of which is provided as Annex *[Annex number]* to this Complaint. The Complaint has been submitted in *[specify language of Complaint] / [pursuant to an agreement between the parties stipulating that [specify language] should be the language of the administrative proceeding, a copy of which is provided as Annex [Annex number] to this Complaint.] / [The Complainant requests that the language of proceedings be [specify language] and provides the following supporting arguments and evidence.] [Where appropriate, provide supporting arguments and evidence supporting the request that the language of the complaint be the language of proceedings, including any relevant pre-complaint correspondence between the parties, the identity of the parties, the nationality and place of residence of the parties, and any other evidence of a respondent's familiarity with the requested language.]*

V. Jurisdictional Basis for the Administrative Proceeding
(Rules, Paragraphs 3(a), 3(b)(xiv))

[11.] This dispute is properly within the scope of the Policy and the Administrative Panel has jurisdiction to decide the dispute. The registration agreement, pursuant to which the domain name(s) that is/are the subject of this Complaint is/are registered,

incorporates the Policy. *[If relevant, indicate when the domain name(s) was/were registered and specify the provision of the registration agreement that makes the Policy applicable to the domain names(s).]* A true and correct copy of the domain name dispute policy that applies to the domain name(s) in question is provided as Annex *[Annex number]* to this Complaint and can be found at *[insert URL]*.

VI. Factual and Legal Grounds

(Policy, Paragraphs 4(a), (b), (c); Rules, Paragraph 3)

[In completing this Section VI., do not exceed the 5000 word limit: Supplemental Rules, Paragraph 11(a). Relevant documentation in support of the Complaint should be submitted as Annexes, with a schedule indexing such Annexes. Such Annexes should be submitted in conformity with the Supplemental Rules, Paragraph 12(a), Annex E. Case precedents or commentaries, such as the WIPO Overview 3.0, that are referred to for support should be referred to with complete citations (where appropriate, reference may be made by inserting the relevant URL).]

[12.] This Complaint is based on the following grounds:

A. The domain name(s) is(are) identical or confusingly similar to a trademark or service mark in which the Complainant has rights;

(Policy, Paragraph 4(a)(i); Rules, Paragraphs 3(b)(viii), (b)(ix)(1))

- *[In accordance with Rules, Paragraph 3(b)(viii), specify the trademark(s) or service mark(s) on which the Complaint is based and, for each mark, describe the goods or services, if any, in connection with which the mark is used. A separate description may also be given of the goods or services with which the Complainant intends, at the time the Complaint is submitted, to use the mark in the future. If applicable, attach copies of the registration certificates for the relevant marks.]*

- *[In accordance with Rules, Paragraph 3(b)(ix)(1), describe the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights.]*

B. **<u>The Respondent has no rights or legitimate interests in respect of the domain name(s);</u>**
(Policy, Paragraph 4(a)(ii); Rules, Paragraph 3(b)(ix)(2))

- *[In accordance with Rules, Paragraph 3(b)(ix)(2), describe why the Respondent should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the Complaint. Attention should be paid to any relevant aspects of the Policy, Paragraph 4(c), including:*

  - *Whether before any notice to the Respondent of the dispute, there is any evidence of the Respondent's use of, or demonstrable preparations to use, the domain name(s) or a name corresponding to the domain name(s) in connection with a bona fide offering of goods or services;*

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

  - *Whether the Respondent is making a legitimate non-commercial or fair use of the domain name(s), without intent for commercial gain misleadingly to divert consumers or to tarnish the trademark or service mark at issue.]*

C. **<u>The domain name(s) was/were registered and is/are being used in bad faith.</u>**
(Policy, paragraphs 4(a)(iii), 4(b); Rules, paragraph 3(b)(ix)(3))

- *[In accordance with Rules, Paragraph 3(b)(ix)(3), describe why the domain name(s) should be considered as having been registered and used in bad faith by the Respondent. Attention should be paid to any relevant aspects of the Policy, Paragraph 4(b), including:*

  - *Circumstances indicating that the domain name(s) was/were registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name registration(s) to the owner of the trademark or service mark (normally the Complainant) or to a competitor of that Complainant, for valuable consideration in excess of the Respondent's out-of-pocket costs directly related to the domain name(s); or*

  - *Whether the domain name(s) was/were registered in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the Respondent has engaged in a pattern of such conduct; or*

  - *Whether the domain name(s) was/were registered primarily for the purpose of disrupting the business of a competitor; or*

- *Whether by using the domain name(s), the Respondent intentionally attempted to attract for commercial gain, Internet users to the Respondent's 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 the Respondent's web site or location or of a product or service on the Respondent's web site or location.]*

VII. Remedies Requested
(Rules, Paragraph 3(b)(x))

[13.] In accordance with Paragraph 4(i) of the Policy, for the reasons described in Section VI. above, the Complainant requests the Administrative Panel appointed in this administrative proceeding that *["<the disputed domain name(s)> be transferred to the Complainant" / "<the disputed domain name(s)> be cancelled".]*

VIII. Administrative Panel
(Rules, Paragraph 3(b)(iv); Supplemental Rules, Paragraph 8(a))

[14.] The Complainant elects to have the dispute decided by a *[choose one:* "single-member Administrative Panel*" / or* "three-member Administrative Panel*"*].

[ ] *[If a three-member Administrative Panel is designated, the names of three persons must be provided, one of whom the Center shall attempt to appoint to the Administrative Panel in accordance with Paragraph 6 of the Rules and Paragraph 8 of the Supplemental Rules. The names of the nominees may be taken from the Center's published list of panelists at http://arbiter.wipo.int/domains/panel/panelists.html.]*

IX. Mutual Jurisdiction
(Rules, Paragraph 3(b)(xii))

[15.] In accordance with Paragraph 3(b)(xii) of the Rules, the Complainant will submit, with respect to any challenges that may be made by the Respondent to a decision by the Administrative Panel to transfer or cancel the domain name(s) that is/are the subject of this Complaint, to the jurisdiction of the courts at *[choose one of the following:]*

(a) "the location of the principal office of the concerned registrar." or

(b) *"the location of the domain name holder's address, as shown for the registration of the domain name(s) in the concerned registrar's WhoIs database at the time of the submission of the Complaint to the Center." or*

(c) *"the location of the principal office of the concerned registrar AND the domain name holder's address, as shown for the registration of the domain name(s) in the concerned registrar's WhoIs database at the time of the submission of the Complaint to the Center."*

[A Mutual Jurisdiction election must be made for each domain name that is the subject of the Complaint.]

X. Other Legal Proceedings

(Rules, Paragraph 3(b)(xi))

[16.] *[If any, identify other legal proceedings that have been commenced or terminated in connection with or relating to the domain name(s) that is/are the subject of the Complaint and summarize the issues that are the subject of that/those proceeding(s).]*

XI. Communications

(Rules Paragraph 3(b), Supplemental Rules, Paragraphs 3, 4, 12)

[17.] This Complaint has been submitted to the Center in electronic form, including annexes, in the appropriate format.

[18.] A copy of this Complaint has been transmitted to the concerned registrar(s) on *[date]* in electronic form in accordance with paragraph 4(c) of the Supplemental Rules.

XII. Payment

(Rules, Paragraph 19; Supplemental Rules Paragraph 10, Annex D)

[19.] As required by the Rules and Supplemental Rules, payment in the amount of USD *[amount]* has been made by *[method]*. *(Payment by credit card should be made using the Center's* secure online payment facility*. For any payment-related queries or difficulties, please contact the Center Secretariat on (+41 22) 338 8247, or email the Center at* arbiter.mail@wipo.int*).*

XIII. Certification

(Rules, Paragraph 3(b)(xiii); Supplemental Rules, Paragraph 15)

[20.] The Complainant agrees that its claims and remedies concerning the registration of the domain name(s), the dispute, or the dispute's resolution shall be solely against the domain name holder and waives all such claims and remedies against (a) the WIPO Arbitration and Mediation Center and Panelists, except in the case of deliberate wrongdoing, (b) the concerned registrar(s), (c) the registry administrator, (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents.

[21.] The Complainant certifies that the information contained in this Complaint is to the best of the Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under the Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument.

Respectfully submitted,

_____

[Name/Signature]

Date: _____

XIV. List of Annexes

(Rules, Paragraph 3(b)(xiv); Supplemental Rules, Paragraphs 4(a), 12(a), Annex E)

[22.] The Rules provide that a Complaint or Response, including any annexes, shall be submitted electronically. Under the Supplemental Rules, there is a file size limit of 10MB (ten megabytes) for any one attachment, with an overall limit for all submitted materials of no more than 50MB (fifty megabytes).

[23] In particular, paragraph 12 and Annex E of the Supplemental Rules provides that, other than by prior arrangement with the Center, the size of any individual file (such as a document in Word, PDF or Excel format) transmitted to the Center in connection with any UDRP proceeding shall itself be no larger than 10MB. When larger amounts of data need to be transmitted, larger files can be "split" into a number of separate files or documents each no larger than 10MB. The total size of a Complaint or response (including any annexes) filed in relation to a UDRP dispute shall not exceed 50MB, other than in exceptional circumstances (including in the case of pleadings concerning a large number of disputed domain names) where previously arranged with the Center.

Annex 1:

Annex 2:

Annex 3:

Annex 4:

Annex 5:

[Additionally, to avoid any uncertainty, it is requested that any Annexes (and their corresponding filenames) be clearly labeled and sequentially numbered (i.e. Annex 1, 2, 3 etc), and a complete list of Annexes supplied].

New gTLD Fast Facts

The New gTLD Program is an initiative coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN) that is enabling the largest expansion of the domain name system. Top-level domains (TLDs) are the letters found at the end of an Internet address. They fall into one of two categories: those that represent countries/territories (known as country code TLDs or ccTLDs) and those that do not (generic TLDs or gTLDs). Through the program, the number of gTLDs will increase from 22 to more than a thousand.

22 › 1000+

The New gTLD Program has made it possible for communities, governments, businesses and brands to apply to operate a gTLD registry, the database of all domain names registered in a top-level domain. The goal of introducing new gTLDs into the Internet is to enhance competition, innovation and consumer choice. In addition, the New gTLD Program is bringing with it many new safeguards that help to support a secure, stable and resilient Internet.

Competition

Locations. New gTLDs that represent specific regions or geographies make it easy to quickly identify where a business, organization or individual is located. Some local governments have made .LOCATION domains the effective online home for anything related to that region/city.

Communities. New domains also show connections to specific communities. Community-based gTLDs include certain eligibility or use restrictions on domain names to ensure that registered domains have been verified as belonging to a member of that community.

Innovation

Entrepreneurship. The New gTLD Program has spurred new businesses, not only through the creation of registries, but also in marketing, research and technology.

Web Presence. With a digital presence becoming requisite for many industries these days, new gTLDs are providing an avenue for people to start or refresh their online image.

Choice

Internationalized Domain Names (IDNs). The introduction of IDNs – domains in non-Latin scripts – are enabling a multilingual Internet and allowing people to navigate the web in their own language.

Variety. By expanding the DNS, new gTLDs offer additional diversity when selecting a domain name. The domains are also being used as extensions of core websites to highlight specific product or service offerings.

Security and Control

Restricted TLDs. Some new gTLDs are built around the concept of security, providing assurance that visitors can expect a safe experience when they visit these domains.

Branded TLDs. Brands are using new gTLDs to identify which sites are their own, eliminating confusion over fake sites, which can lead to identity theft and counterfeit sales.

New gTLD Program by the Numbers

gTLD Key Stats

1930 Applications received by the deadline (May 2012).

1000+ New gTLD names or "strings" possible.

850+ New gTLDs introduced into the DNS Root Zone.*

23 October 2013 Delegation of first new gTLD (.ةكبش).

Language Options

Internationalized Domain Names (IDNs) are available as generic top-level domains for the first time, enabling new extensions in different language scripts, such as Arabic, Chinese, Greek, Devanagari and more.

Frequently Asked Questions

Q. Are there different types of new gTLDs?

A. New gTLDs have been introduced for a variety of communities, interests and businesses. They can be, among other things, commonly used words, such as .BUILD or .WEBSITE. There are specific subsets of gTLDs, including Geographic (.RIO, .WIEN, etc.), Community (.SKI, .SCOT, etc.), Brands and IDNs (.世界, .дети, etc.).

Q. How can I access a website with a new gTLD extension?

A. Websites with new gTLD extensions can be accessed similarly to any other website – by entering the web address directly into the browser or by clicking the website link provided from search engine results.

Q. Who can operate a new gTLD?

A. Operating a TLD registry is a major commitment. To qualify, applicants had to undergo a rigorous application and evaluation process. At this time, the application window is closed, though there will be additional opportunities to apply for a new gTLD in the future.

Q. How can I register a domain name in a new gTLD?

A. Domain names are available for registration on new gTLDs through many registrars, the same as other TLDs. With new gTLDs being introduced regularly, there are domains of all types and languages to choose from.

Q. Where can I find more information?

A. For more information about the New gTLD Program, visit: http://newgtlds.icann.org. For examples of how people are using new gTLDs, visit: http://www.icann.org/newgtldcasestudies.

About Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN's mission is to help ensure a stable, secure and unified global Internet. To reach another person on the Internet, you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN helps coordinate and support these unique identifiers across the world. ICANN was formed in 1998 as a not-for-profit public-benefit corporation and a community with participants from all over the world. ICANN and its community help keep the Internet secure, stable and interoperable. It also promotes competition and develops policy for the top-level of the Internet's naming system and facilitates the use of other unique Internet identifiers. For more information please visit: www.icann.org.

*As of December 2015

New Generic Top-Level Domains