ICANN Policy Developments on Abusive Domain Name Registrations

Mike Rodenbaugh

Mike Rodenbaugh has been practicing trademark and e-commerce law for 15 years, representing clients in all matters relating to domain names, trademarks, copyrights, and other forms of intellectual property, and in e-commerce, IP licensing and marketing transactions, and dispute resolution efforts. He is active in the International Trademark Association, Anti-Phishing Working Group, and ICANN. He started Rodenbaugh Law in 2007, after more than seven years co-managing trademark and domain name inventory and strategy for Yahoo! Inc., and handling hundreds of different transactions and dispute resolutions for Yahoo!

Mr. Rodenbaugh would like to thank his associate attorney, Erin Dennis Vivion, for her valuable research and drafting assistance in writing this note.

The author's website is www.rodenbaugh.com, and he may be reached at info@rodenbaugh.com.

The Internet Corporation for Assigned Names and Numbers (ICANN), if even recognized, is an enigma to most people. It is a not-for-profit California corporation tasked by the US Department of Commerce to manage the global domain name system (DNS) and IP addressing functions that are fundamental to the operation of the Internet. ICANN has managed these functions for more than 10 years: a period of explosive growth that has seen the DNS expand to more than 183 million names. This total includes 12 percent growth from a year earlier, and 43 percent growth from June 2007.[1]

This article addresses the current, growing problem of abusive domain name registrations, including those registered for cybersquatting, phishing, and malware distribution. This problem undoubtedly will grow with the advent of International Domain Names in alternative scripts, and new Top-Level Domains coming in 2010 and beyond. Yet ICANN still has not suggested any policy to deal with these issues. Current status of ICANN efforts, and further potential policy development options are presented below.

Cybersquatting

Most trademark lawyers are probably aware that ICANN is involved with managing the DNS, and developed the Uniform Dispute Resolution Policy (UDRP) arbitration remedy for trademark cybersquatting. This remedy was intended to deter cybersquatting by providing a "fast-track" arbitration process so that trademark owners would not have to resort to court action in order to recover squatted names. Enacted in 2000, a record number of more than 3000 UDRP complaints were filed in 2007, with some 25 percent settled before a decision, and 85 percent of decisions in favor of the complainant.[2]

Unfortunately, because the cost of filing a UDRP action is anywhere from 200 to 2000 times greater than the cost of registering a .com domain name, literally millions of clearly infringing domains currently are registered to cybersquatters. A 2008 "brand-jacking" report by MarkMonitor found 420,000 cybersquatted domains with respect to just 30 brands.[3] As that statistic indicates, many well-known online brands try to prioritize efforts against more than 10,000 infringing domain registrations at any given time. While most of those are in the .com TLD, increasingly squatters are registering country code domains, as most ccTLD registries no longer impose meaningful restrictions on registrations, registration costs are dropping, and overall Web traffic continues to grow rapidly in most countries.

Abuse of the DNS has become a fundamental tool of trademark infringers, who register domains that are misspellings of trademarks, trademarks with omitted characters, and/or trademarks combined with

other words, numbers, or symbols. The infringers then hijack "direct navigation" traffic intended for the trademark owner, and often try to drive further traffic to the domains via spam, search engines, and other means. Typically they monetize traffic by advertising to it. These advertising costs are often paid indirectly by the trademark owner and its competitors.[4] The registrant and their advertising distributor share ad revenue on every click or pop-up, while a domain registry, registrar, and ICANN share revenue from every registration.

This activity was taken to the extreme over several years of DNS exploitation, with the rise of "domain tasting" and "domain kiting" as profitable business practices. Tasters took advantage of the five-day "Add Grace Period" formerly required in most of ICANN's gTLD registry contracts, including Verisign's contracts to operate .com and .net. They developed software to select thousands or even millions of names at a time, register them all, monetize them and track traffic for almost five days, and then drop almost all of the domains for a full credit of the registration fee. They kept those domains projected to earn more than their registration fee via pay per click (PPC) traffic over 365 days.[5]

Less scrupulous tasters formed many different companies (and/or false identities) to "kite" domains by re-registering their dropped domains for another five days, and continuing the cycle. Thus they avoided registration costs, yet maintained continuous control of kited domains. Several famous brand owners have been aggressive in litigating against these types of cybersquatters. Often their complaints would list thousands of clearly infringing domains held by the defendants, and several examples of alleged kiting.[6]

Eventually, tasting was the subject of a resolution from the ICANN Board, and of a resolution from its GNSO Council (which develops policy with respect to .com, .net, and other "gTLD" domain spaces). The Board resolution was effective as of July 1, 2008. It made non-refundable the portion of each registration fee that is paid to ICANN, currently twenty cents, for all registrations over a 10 percent threshold per registrar, per month. The GNSO resolution, implemented March 31, 2009, makes the entire registration fee non-refundable for any registrar that deletes more than 10 percent of its net new registrations in any month.

These resolutions each are intended to end commercial domain tasting and kiting. The Board resolution resulted in an 80 percent decline in tasted registrations the first month it was implemented.[7] However, at least two large scale tasting operations continued, despite the additional cost.[8] Moreover, a few conglomerates control more than 100 ICANN registrar accreditations each, so there is fear that commercial tasting still can occur by spreading a number of "free deletes" among many registrar accreditations. This will be monitored by the GNSO Council. However, ICANN staff recently published a report showing that deleted domain registrations decreased 99.7% since implementation of the GNSO resolution.[9] At last, ICANN can claim some sort of policy development victory.

These resolutions have certainly slowed the pace of new infringing gTLD registrations by making "tasting" much more costly to accomplish at scale. Yet they do nothing to address the millions of infringing registrations existing now—most having been tasted and proved profitable to their registrant. They do nothing about the ease with which infringing domains can be immediately registered and monetized, or about the high cost of filing a UDRP action. They do nothing to address increasing cybersquatting in the country-code TLDs. And of course, they do nothing to address the certain influx of many new cybersquatted registrations in the hundreds or thousands of new TLDs that ICANN will authorize in the near future.

Therefore, the cybersquatting problem is likely to continue to grow unless and until ICANN implements a policy that actually deters this insidious practice. ICANN seems to have recognized this, and put the new TLD program temporarily on hold in part to address this issue.[10] The ICANN Board commissioned a group of trademark experts to devise detailed proposals for avoiding cybersquatting in new TLDs. The proposals of this Implementation Recommendation Team (IRT) are discussed below.

Phishing and Malware Distribution

Increasingly, domain name registrants are serving malware to unwitting visitors who accidentally arrive at their domains, or who are driven there by spam, DNS poisoning, and other diversionary tactics. Malware comes in many forms, but typically it allows the domain registrant and its accomplices to steal personal information and money from the visitor. Malware also can turn the visitor's computer into a "bot" that can be remotely directed to serve spam, or far worse. Botnets often are used for child porn distribution, distributed denial-of-service (DDOS) attacks, phishing, counterfeiting, and other criminal operations.

The number and level of sophistication of "phishing" attacks continues to increase.[11] Classic phish attacks use spam email, designed to look as if from a trusted financial institution, to lure recipients into opening the email and/or clicking on a link purportedly to the financial institution's Web site. Upon opening the email and/or clicking on the link, the user might receive malware which can capture their financial information. Or once at the fake Web site, the user might enter her user name and password and thereby transmit it to criminals. Criminals exploit the DNS by registering domains, often using stolen credit cards for payment to avoid identity detection, and then using them to send spam and host fraudulent and/or malware distribution sites.

Once these scams are detected, financial institutions and their security vendors work feverishly to have the Web site shutdown. Typically this involves notice to the Web host and/or other ISP if they can be located. Even when located and action taken, however, the fraudulent site can then be moved to a different Web host or ISP, and the domain pointed to the new site. "Fast flux" nameserver and/or IP address changes can happen in seconds, effectively moving the Web site around to make it impossible to take down. The only way to stop this cycle is to stop the resolution of the domain name used as a phishing lure.

Unfortunately, that is not a realistic remedy in many situations, for example when the site is hosted at MySpace, Yahoo!, or any other shared hosting environment. More and more often, small business and individual's websites are hacked, as they often lack robust security. Phishers then use the legitimate sites to launch phish attacks and/or malware exploits. Anti-phish teams contact the owners of hacked sites to explain the situation and how the vulnerability can be fixed. Usually site owners are eager to try to fix the problem because it involves a breach of their site security.

This remedy takes time, but probably is the most fair and effective way to address the problem of phish attacks launched from hacked domains. The prominent shared hosting environments, including MySpace and Yahoo!, have become very effective at detecting phish sites and otherwise quickly responding to phish complaints. Yet, many Web sites fail to adapt even minimal security precautions, and a compromised Webserver from an otherwise legitimate site provides a valuable distribution tool for the phisher. As a result, phishers increasingly are hacking any site they can.

However, in many other situations, a domain is used solely for fraudulent activity. Sometimes the domains are obvious trademark infringements like "pay-pal.com." More often they are simply junk domains like "aaefraf.com" which are then "masked" to visitors and spam recipients, who do not realize that the actual landing URL is different than the one they see in their browser address bar and/or Weblink. While many domain registrars and registries will take action upon complaints and after conducting their own investigation, other registrars and registries will not act or even investigate.

Domain registrars generally are low margin businesses, and many registrars (and their downstream resellers) have no customer service to contact. So, while each may profit from every registration, many are not willing to assume the cost of customer service to address obvious abuse. That needs to change, especially as the name space expands significantly in the near future.

ICANN has recognized that rapid expansion of the DNS may contribute to rapid expansion of criminal exploitation of the DNS. Indeed this is another of the issues that, in part, gave reason for ICANN to temporarily delay the rollout of new TLDs.[12] However, to date there has been little communication from ICANN Staff as to their intentions to address this issue. Further word is expected with the next iteration of the New gTLD Draft Applicant Guidebook (version 3), to be published this Fall.

New TLDs and IDNs

In 2010, ICANN will usher in another wave of new TLDs, such as .web, .berlin, .sport and .africa. It is expected there will be several hundred applications early next year,[13] and ICANN Staff has reported that there is no technical reason that the "root zone" of the Internet could not support more than 60 million new TLDs![14] Each new TLD creates a probability of systemic cybersquatting and other DNS abuse, as has been seen in all unrestricted TLDs launched to date.

For example, even today there appear few active (non-PPC parked) Web sites in .biz, in comparison to the number of domains registered—and it launched in 2001. Trademark owners have dutifully paid for their 'defensive registrations' in .biz for years, many after paying to register their "IP Claims" with the .biz registry when it launched, for the privilege of keeping clearly infringing domain names away from a competitor or infringer. They have done the same in .info and other unrestricted gTLDs, as well as many ccTLDs.

Now, International Domain Name (IDN) registrations are becoming more prevalent. These are domains in scripts other than ASCII characters, such as Cyrillic, Chinese, Japanese, Korean, Arabic, Hebrew, etc. IDNs have been available for registration at the second level[15] and beyond for many years. But relatively few Internet users had the knowledge and technology to use them. That is changing, particularly since Microsoft's Internet Explorer version 7 incorporated IDN functionality. The most savvy and global trademark owners register IDN versions of their marks as domains, but still these alternative scripts provide ample opportunity for cybersquatters, phishers, and other miscreants to exploit.

Next year, there likely will be top-level IDN names introduced as new TLDs. The uptake of IDNs marks huge progress for the Internet, as it allows more people to interact in their native language. But it also is a serious concern because law enforcement efforts are already overburdened, and certainly ill-equipped to deal with domains in non-ASCII scripts. It also is expected that many users of IDN domains will be relatively new to the Internet, and thus more easily victimized by online criminals. To be sure, trademark owners have much to be concerned about the growing popularity of IDNs and the prospect of dozens or hundreds of new TLDs in the near future.

Defensive (*aka* "sunrise") registration schemes have been used in previous TLD launches to mitigate cybersquatting, but they are not sustainable across many more new TLDs. ICANN registrars and registries, by offering trademark terms to their owners ahead of "land rush" registrations to the general public (and then complying with UDRP decisions), have thought they did enough to prevent cybersquatting—while profiting from every defensive as well as infringing registration. But this has failed to deter wide scale cybersquatting, and has led to unfair and recurring costs to brand owners for defensive registrations. This "sunrise" scheme is surely not scalable across many new TLDs.

Most trademark owners will not pay to defensively register in many, if any, new TLDs, because the value of holding these domains in previous TLDs largely has been disproved. Instead, many more are likely to invest in infringement monitoring services, cease and desist notices, and in legal action against infringers and their accomplices, likely including registrars and registries (and perhaps also ICANN) as defendants more often. Several well-known brand owners have had significant success extracting settlements from large-scale squatters, and this trend may continue as the squatters' portfolio values grow and they have more to fear from adverse judgments.[16]

Ideally, ICANN can develop a global policy that deters abusive registrations, rather than allow courts and governments around the world to impose various rules upon ICANN and its contracting parties' registration practices.

Policy to Address Abusive Registrations

Today, other than the UDRP, ICANN has no policy in place to deter or prevent abusive registrations in existing or new TLDs. Yet, while difficult to quantify, the "abusive registration" problem is undoubtedly enormous and growing. In this increasing threat environment, at least ICANN has developed policy to slow the flow of new cybersquatting cases. But it has done nothing with respect to phishing, malware, etc., or with respect to the millions of existing cybersquatted domains, and millions more possible in new TLDs.

Anti-Cybersquatting Policy Development

The cybersquatting problem has morphed over time such that the existing UDRP remedy is ineffective in the face of the massive volume, speed, and sophistication of many modern trademark cybersquatters. It was enacted at a time when domain registrations cost at least $50 and cybersquatters profited primarily by selling domains to trademark owners or to other squatters. Today domains often cost less than $10, and squatters can register thousands of domains in minutes and then immediately monetize traffic via pay-per-click and other forms of advertising. Most well-known trademark owners have more domain name registrations, and more domain name infringement matters, than they can manage. Most of their registrations have been recovered from squatters and/or defensively registered to keep from squatters. Few trademark owners have any appetite to buy still more domains, from either squatters or registries.

The Implementation Recommendation Team, commissioned by the ICANN Board in March, 2009, prepared detailed proposals to address the probability of cybersquatting in new TLDs. This IRT produced five significant recommendations contained in their Fnal Report.[17]

Of these, one is most controversial and thus least likely to move forward. The "Globally Protected Marks List" would give a small subset of the most famous trademark owners special rights to block domain name registrations that precisely correspond to their trademark. The definition of "globally protected" was not completed in time for the Final Report, but in any event this special protection would apply only to precise matches of registered trademarks, rather than commonly cybersquatted strings (*e.g.*, combinations and typos). However, the other recommendations were less controversial, and likely would provide much better protection against cybersquatting in new TLDs that we have today.

The foundational proposal is to create an "IP Clearinghouse" allowing trademark owners to submit information about their trademark rights to one database service provider. This seeks to overcome the challenge that brand owners have faced in past TLD launches, having to register their trademark rights with each new TLD registry in order to have first right to purchase corresponding domain names during the "sunrise period." If the IP Clearinghouse is created, they would only need to submit their info once, and all new TLD registry operators will have equal access to the data. When someone tries to register a domain that corresponds to a trademark, they would receive a notice of the trademark owner's rights, and would have to promise not to use the domain name in an infringing manner. This may provide a deterrent to some would-be infringers, as at least it should eliminate the commonly attempted defense of "innocent infringement."

Of course, willful infringers will still make this promise, since they know that trademark owners cannot possibly police every infringement in a timely manner, and they can profit in the meanwhile. Therefore the most important proposal is to allow a much quicker and cheaper suspension of domain resolution in 'clear and convincing' cases of cybersquatting. For a few hundred dollars, trademark owners

would swear out a complaint under the Uniform Rapid Suspension (URS) process. If the complaint is not timely answered, or the standing trademark specialist is otherwise convinced, resolution to the domain will be suspended. This contrasts with the current Uniform Dispute Resolution Policy (UDRP) which costs more than $1000 to file (plus thousands of dollars in investigation and legal fees) and takes many months for a decision, all the while the infringer profits from the domain.

Unfounded (and sometimes ridiculous) opposition has been raised as to the substance of the IP Clearinghouse and URS proposals.[18] But it is obvious that the UDRP has been entirely ineffective in deterring cybersquatting in the existing TLDs. So, after ten years of the UDRP, it is clear that new methods are needed to deal with this rampant problem. The IP Clearinghouse and URS proposals, in conjunction with one another, would strike a reasonable balance between trademark rights, protection of the public, and protection of domain name registrants.

Policy Development re Other Malicious Use of DNS

The IRT's proposals only seek to address trademark cybersquatting. Other forms of DNS abuse are more harmful, and equally within ICANN's remit to address. As recommended by the GNSO's Fast Flux Working Group, ICANN further must explore ways for its contracting parties to detect "fast flux" DNS changes and investigate for malevolent exploits. It should consider minimum response requirements for registrars and registries to address complaints of abuse, and ought to adopt a policy that allows registrars and registries to suspend DNS to clearly abusive domains. All of these suggestions are to be explored by ongoing working groups commissioned by the GNSO Council. But the work is painstakingly slow, while the harm from malicious DNS exploits continues to grow.

Of course, the UDRP was never intended to deal with phishers and "drive-by downloaders," much less IDNs or new TLDs. Yet the DNS is increasingly abused by criminals, and IDNs and new TLDs open up huge new namespaces for criminal and cybersquatting activity. Domain registration systems allow essentially unauthenticated purchases, and then permit automated fast flux DNS exploits that make it impossible for law enforcement to detect and stop a huge amount of criminal activity. The anti-phishing community has witnessed, time and time again, massive abuse against one registry or registrar that has a vulnerability. Once the vulnerability is fixed, the criminals move on. Once hundreds or thousands of new TLDs are launched, criminals will have many more targets to exploit.

Many ICANN-accredited registrars and registries make efforts to deal with these problems on their systems, yet some do nothing. As it stands today, too many refuse to act, and instead knowingly profit from illegal activity. ICANN has accredited nearly 1000 different registrar entities, many of whom 'resell' their services through hundreds or thousands of affiliates. Too many of these vendors have no or minimal customer service to respond to abuse complaints. There could and should be a minimum response process for registrars to respond to complaints, and a process for registries to take action when their registrars have not.

ICANN's GNSO has examined how it might address fast flux DNS exploits. The Security and Stability Advisory Committee (SSAC) issued an Advisory about the problem in March 2008,[19] and in May 2008 the GNSO Council resolved to form a Working Group to consider the issues around "fast flux" hosting, and whether ICANN contracting parties could help to mitigate criminal DNS exploits. This Working Group issued its Final Report in August, 2009.[20] The group recommends that another ongoing working group continue to look at ways to respond to all forms of DNS abuse, and that the GNSO Council encourage the adoption of a Fast Flux Data Reporting System to better monitor fast flux DNS exploits.

ICANN is looking broadly at registration abuse policies of its contracting parties. The GNSO Council has recognized that such policies are inconsistent among the contracting parties.[21] The ICANN Staff has published an Issues Report outlining further work to be done as a precursor to a formal "Policy

Development Process" (PDP) under the ICANN Bylaws.[22] The Council has commissioned a Working Group to perform that work this year. Indeed ICANN has promised to address these "overarching issues" of trademark infringement and DNS exploitation in new TLDs, through consultation with Internet community stakeholders and appropriate policy development.[23] In addition, the SSAC has issued its Advisory 038 which recommends registrars to provide a public point of contact for abuse matters, and have asked for coordination with the Registration Abuse Policies Working Group recently commissioned by the GNSO.[24]

Meanwhile the Anti-Phishing Working Group[25] has been working with registry representatives to develop domain name suspension processes for domains used in phish attacks. Generally only domains that are used solely for phishing or malware distribution would be eligible for suspension—domains resolving to shared hosting environments generally would not be eligible. And only accredited anti-phishing teams would be able to file a suspension request, after taking specified steps to verify the criminal behavior. If the registrar or registrant has not remedied the problem within a certain timeframe, then the domain would be suspended by the registry and the registrant could then appeal. It is hoped this process will prove effective in minimizing "false positive" complaints and also in minimizing the time that domains are kept live during active phish or malware attacks. If it proves effective, then it could be adopted voluntarily by other registries, and/or might be adopted as a Consensus Policy applicable to all gTLD registries.

This sort of "takedown" decision is made every day by many ISPs, registrars and registries, but they are not made quickly, uniformly or often enough. These parties all fear liability in the case of a wrong decision, where a legitimate Web site is taken down. While that may be a real concern, there never appears to have been a lawsuit against a registrar or registry for doing so, and relevant, industry-standard contractual provisions—between ICANN and registries, registries and registrars, and registrars and registrants—already clearly prohibit abuse of a domain in violation of third party rights. So these contractual provisions should provide cover in the rare event of a "false positive" domain suspension, done in good faith to protect the public from crime, which can be quickly reversed in the rare case of error.

The harm of temporarily suspending a legitimate Web site pales in comparison to the massive and growing harm caused by criminally abusive domain registrations, materially assisted by ICANN contracting parties and indeed by ICANN itself. These parties should not be allowed to continue to take revenue from clearly abusive registrations, without policies in place to deal with complaints of abuse. Just as search engines and other online marketplaces have had to adopt trademark and other policies to deal with illegal activity on their systems, ICANN's contracting parties must evolve to do the same. This will result in a safer and more profitable Internet for everyone.

---

[1] The Verisign Domain Report, The Domain Name Industry Brief, Vol. 6, Issue 2, (June 2009) at 2, *http://www.verisign.com/Resources/Naming_Services_Resources/Domain_Name_Industry_Brief/.*

[2] *E.g.* World Intellectual Property Organization, IP Services, Domain Name Statistics, *Total Number of Cases per Year, http://www.wipo.int/amc/en/domains/statistics/cases.jsp*; World Intellectual Property Organization, IP Services, Domain Name Statistics *Case Outcome by Year(s) (Breakdown), http://www.wipo.int/amc/en/domains/statistics/outcome.jsp*; Laura MacInnis, "U.N. Agency Ousts Record Number of 'CyberSquatters,'" *Reuters*, Mar. 27, 2008, *http://www.reuters.com/article/technologyNews/idUSL275020020080327*.

[3] MarkMonitor, "Brandjacking Index" (Summer 2008) at 8 and 13, *http://markmonitor.com/download/bji/BrandjackingIndex-Summer2008.pdf.*

[4] *See* Phil Lodico, "Deriving Value from Web Sites: Search Engine Marketing, Search Engine Optimization, and Parking, INTA," *Trademark Law and the Internet* 2009, *http://inta.org/meeting_portals/09TLI/cm/Follow_the_Money-Lodico.pdf*.

[5] *See* Mike Rodenbaugh, Patrick Jones, and Olof Nordling, "Outcomes Report of the GNSO Ad Hoc Group on Domain Name Tasting," Oct. 4, 2007, *http://www.gnso.icann.org/drafts/gnso-domain-tasting-adhoc-outcomes-report-final.pdf*.

[6] *See, e.g.,* Mike Masnick, "Dell Sues Cybersquatters for Elaborate Shell Game," *Techdirt*, Nov. 29, 2007, *http://techdirt.com/articles/20071129/015252.shtml*; Kevin Kingsbury, "Verizon Wins Suit Over Internet Addresses," *Wall Street J*, Dec. 26, 2008, *http://online.wsj.com/article/SB123013196536432935.html*; Anne Broache, "Luxury Retailers Go After Alleged Cybersquatters—Again," *CNET News*, Mar. 23, 2007, *http://news.cnet.com/8301-10784_3-6170192-7.html*.

[7] ICANN, Announcement, "AGP Deletes Down by 84 percent," Nov. 13, 2008, *http://www.icann.org/en/announcements/announcement-13nov08-en.htm*.

[8] Posting of Mike Rodenbaugh to *http://gnso.icann.org/mailing-lists/archives/council/msg05729.html* (Nov. 19, 2008, 17:19:28).

[9] ICANN, Announcement, "The End of Domain Tasting," Aug. 12, 2009, *http://www.icann.org/en/announcements/announcement-12aug09-en.htm*.

[10] Draft Applicant Guidebook: What You Told Us, Feb. 18, 2009, *http://icann.org/en/announcements/announcement-3-18feb09-en.htm*.

[11] Anti Phishing Working Group, "Phishing Activity Trends Report 2d Half 2008," July-December 2008, *http://apwg.org/reports/apwg_report_H2_2008.pdf*.

[12] Draft Applicant Guidebook: What You Told Us, Feb. 18, 2009, *http://icann.org/en/announcements/announcement-3-18feb09-en.htm*.

[13] *See* ICANN, Topics, "New gTLD Program," *http://www.icann.org/en/topics/new-gtld-program.htm*.

[14] ICANN Staff Draft Paper, "DNS Stability: The Effect of New Generic Top Level Domains on the Internet Domain Name System," Feb. 6, 2008 at 4, *http://www.icann.org/en/topics/dns-stability-draft-paper-06feb08.pdf*.

[15] .com is a top level domain (TLD), yahoo.com is a second level name, yahoo.co.uk is a third level name.

[16] *See, e.g.,* Masnick, Kingsbury, and Broache, *supra* n.6.

[17] Final Report on Trademark Protection in New TLDs, *http://www.icann.org/en/announcements/announcement-4-29may09-en.htm*.

[18] The Public Comment forum: *http://forum.icann.org/lists/irt-final-report/*.

[19] ICANN Security and Stability Advisory Committee, Advisory on Fast Flux Hosting and DNS: "Fast and Double Flux Attacks," SAC 025, March 2008, *http://www.icann.org/en/committees/security/sac025.pdf*.

[20] Final Report of the GNSO Fast Flux Hosting Working Group, Aug. 6, 2009, *http://gnso.icann.org/files/gnso/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf*.

[21] Motion Proposing an Issues Report on Aspects of Registry-Registrar Agreements, Sept. 25, 2008, *http://gnso.icann.org/resolutions/#200809*.

[22] Marika Konings, "GNSO Issues Report on Registration Abuse Policies," Oct. 29, 2008, *http://gnso.icann.org/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf*.

[23] Draft Applicant Guidebook: What You Told Us, Feb. 18, 2009, *http://icann.org/en/announcements/announcement-3-18feb09-en.htm*.

[24] SAC 038: Registrar Abuse Point of Contact, Feb. 25, 2009, *http://www.icann.org/en/committees/security/sac038.pdf.*

[25] The APWG is a wholly separate entity from ICANN, though part of its mission is to influence ICANN policies relevant to the anti-phishing community, particularly through its Internet Policy Committee.