ELECTION LAW JOURNAL
Volume 8, Number 1, 2009
Mary Ann Liebert, Inc.
DOI: 10.1089/elj.2008.0013

Candidates, Squatters, and Gripers: A Primer on Political Cybersquatting and a Proposal for Reform

Matthew T. Sanderson

I. INTRODUCTION

During last year's election, were you hoping to read-up on Barack Obama's abortion stance? Too bad, if you went to Obama ForPresident.com. It featured crossword puzzles and fantasy football rather than public-policy papers. Were you looking to volunteer for U.S. Senate candidate John Sununu? If you visited JohnSununu.com, it allowed you to sign up for a free online dating service but not to sign on to a political campaign. Did you want to help finance John McCain's bid for the presidency? During much of the 2008 campaign season, a contribution submitted through the official-looking JohnMcain.com would have supported a man in Houston, Texas, without one nickel funding McCain's run for the White House.[1]

All three of these web sites were intuitively linked to prominent U.S. politicians, but none were owned by the candidates or their campaigns. These sites exemplified a broader trend. Without any legitimate affiliation, people nab rights to web sites that evoke politicians' names. They do it for profit. They do it for spite. They do it to broadcast criticisms. They do it out of egotism or to indulge their idea of fun. Most importantly, they do it often and they do it everywhere. "Political cybersquatting," as this practice is known, is occurring with increasing frequency around the world.[2]

This article discusses political cybersquatting's causes and proximate harms. The next section offers necessary background information on Internet processes and governance. The following section describes the political-cybersquatting problem by showing that (1) candidates are seriously injured by cybersquatting, (2) candidates are exceptionally exposed to cybersquatting, and (3) candidates cannot rely on existing preventive and remedial methods to consistently solve their cybersquatting problems. Finally, the article proposes a new specialized top-level domain,

Matthew Sanderson is a graduate of the University of Utah and of Vanderbilt University Law School. He served as Campaign Finance Counsel for McCain-Palin 2008, Senator John McCain's presidential campaign committee, and is now an associate in the Political Activity Law practice group of Caplin & Drysdale, Chartered. Mr. Sanderson has published several articles on campaign finance and election law, including Federal Campaign Finance Law: A Primer for the Lobbyist, ABA Lobbying Manual (with Trevor Potter, 2009); From Intent to Outcome: Balloting and Tabulation Around the World, ABA International Election Principles (2008); and Voodoo Economics: A Look Abroad for a Supply-Side Solution to America's Campaign Finance Riddle, Vanderbilt Journal of Transnational Law (2008). He and his wife Emily have two sons, Isaac and Miles. Special thanks to Chuck Fish, Chad Pehrson, Bryson Morgan, Aaron Randall, and Todd Steggerda for their helpful comments and insight.

[1] As late as February 2008, JohnMcain.com featured a "Contribution" web page that was nearly identical to the "Contribution" page of JohnMcCain.com, the official web site of Senator John McCain's presidential campaign.

[2] Jacqueline D. Lipton, *Who Owns Hillary.Com?: Political Speech and the First Amendment in Cyberspace*, 49 Boston College L. Rev. 55, 60–61 (2008) (defining "political cybersquatting").

".pol," as a way to mitigate political cybersquatting's harms.

II. INTERNET BASICS

Basic knowledge of Internet processes is essential to fully appreciating political candidates' vulnerabilities and remedies in the online context. This section briefly highlights the emergence of the Domain Name System and the Internet Corporation for Assigned Names and Numbers (ICANN). It also describes ICANN's role in maintaining and regulating the Internet.

A. The Domain Name System's emergence

The Internet's development was (and continues to be) a decentralized and un-hierarchical affair. But to function, the Internet relies on a highly centralized system.[3] Computers are assigned a unique identifying number called an Internet protocol (IP) address.[4] Much like a street address, an IP address helps computers identify and locate a specific computer.[5] Early in the Internet's development, users would type a 32-bit number to access a web page.[6] However, these long numbers were cumbersome and difficult to remember.

To make the Internet more user friendly, domain names—"human-friendly address[es]" for computers—were created[7] and the Domain Name System (DNS) was born.[8] By convention, domain names contain three parts.[9] In www.vanderbilt.edu, for example, "edu" is a top-level domain (TLD), "vanderbilt" is a second-level domain (SLD),[10] and all other parts would be "lumped together as third-or-higher-level domains."[11] Computers still utilize IP address numbers, but domain names serve a mnemonic function and make the Internet easier to use. An Internet user can simply type <http://www.vanderbilt.edu> into a web browser and Vanderbilt University's web site appears a split second later.[12] In that split second, the browser converts <http://www.vanderbilt.edu> into an IP address number so it can request Vanderbilt's home page from the machine at Vanderbilt's IP address.[13] To do this, it accesses the DNS—a dynamic database that matches unique domain names to unique IP addresses.[14] The browser first requests information from its default domain-name server, which may already contain the IP address that matches <http://www.vanderbilt.edu> because of a recent, identical request from another browser.[15] If it doesn't, the default server forwards the browser's request up a hierarchy of domain-name servers until a server's database can match <http://www.vanderbilt.edu> to an IP address.[16] At the top of this hierarchy is a "root" server that points to the full, authoritative databases for each TLD—both generic (.com, .edu, .net, .org)[17] and

---

[3] A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 20 (2000).

[4] Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOCIETY, <http://www.isoc.org/internet-history/brief.html> (2003).

[5] David S. Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters: The Dwindling Utility of the Anticybersquatting Consumer Protection Act*, 46 IDEA 415, 418 (2006).

[6] Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 38.

[7] WORLD INTELLECTUAL PROPERTY ORGANIZATION, THE MANAGEMENT OF INTERNET NAMES AND ADDRESSES: INTELLECTUAL PROPERTY ISSUES—FINAL REPORT OF THE WIPO INTERNET DOMAIN NAME PROCESS 23 (1999), *available at* <http://www.wipo.int/amc/en/processes/process1/report/finalreport.html>.

[8] Susan P. Crawford, *The ICANN Experiment*, 12 CARDOZO J. INT'L & COMP. L. 409, 412 (2004). For an excellent, simplified description of the DNS's functions, *see* How Stuff Works, *How Domain Name Servers Work*, <http://www.howstuffworks.com/dns.htm>.

[9] Tamarah Belczyk, *Domain Names: The Special Case of Personal Names*, 82 B.U. L. Rev. 485, 490 (2002).

[10] *See* Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 39.

[11] A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 39 (2000).

[12] "http://www.vanderbilt.edu" is known as a Uniform Resource Locator or URL and may contain variations on "http://www." One could, for example, "ftp" instead of "http" or omit "www" completely.

[13] A. Michael Froomkin, *When We Say US, We Mean It!*, 41 HOUS. L. REV. 839, 857–858 (2004).

[14] *See* Lily Blue, *Internet Domain Name Governance: Antitrust Litigation and ICANN*, 19 BERKELEY TECH. L.J. 387, 388 (2004).

[15] Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 43 (2000).

[16] Kim G. von Arx and Gregory R. Hagen, *Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control*, 9 RICH. J.L. & TECH. 4 (2002).

[17] For a complete listing of generic TLDs, see Internet Assigned Numbers Authority, *Generic Top-Level Domains*, <http://www.iana.org/gtld/gtld.htm>.

country-coded (.us, .ca, .uk, .eu).[18] If a domain name is not matched to an IP address, it is invisible to nearly all Internet users.[19] Because the root is the ultimate source of domain-name and IP-address information for all DNS servers, its control "provides singular power in cyberspace."[20]

A domain name appears in the DNS only if it is properly registered.[21] Current DNS registration is arranged through registrars—firms that collect payment, registrant information, and "ensure . . . each domain name is unique."[22] Domain names using generic TLDs like ".com" are available on a "first-come, first-serve" basis; a registrar neither verifies registrants' ownership claims, nor checks for trademark conflicts.[23] Domain names that include limited-use TLDs like ".gov" and ".edu" and ".biz" are subject to some restrictions.[24] Registrants of ".edu" domains, for example, must be "post-secondary institutions that are institutionally accredited."[25] After a registrar verifies a domain name's availability, it contacts the appropriate registry, which acts as a depository for all domain names within a particular TLD.[26] A domain name and an IP address matched in a registry's depository that is recognized by the root will propagate throughout the Internet so users may access the machine at the IP address.[27]

B. ICANN'S origin and functions

From the beginning, a series of private entities held and maintained the Internet's root under U.S.-government contract.[28] But this arrangement was subject to increasing criticism in the late 1990s by those who believed the U.S. government should not solely control a global resource like the Internet.[29] In 1998, the Clinton Administration responded to international pressure by producing an informal policy statement widely known as "the White Paper," which suggested that a new private, non-profit entity incorporated in the United States take over day-to-day control of the DNS. The proposed corporation would be untethered to government control, at least as compared to previous root holders.[30] Soon after the White Paper's publication, a group answered the government's call and formed ICANN, a private non-profit corporation incorporated and headquartered in California.[31] The U.S. government subsequently authorized ICANN to control the root on an experimental basis.[32]

ICANN is authorized to perform only "technical coordination" tasks necessary to maintain the DNS,[33] but its actions often have strong and

---

[18] For a full listing of country-specific TLDs approved by ICANN and currently in use, *see* Internet Assigned Numbers Authority, *Country-Coded Top Level Domains*, <http://www.iana.org/root-whois/index.html>. Almost all country-coded TLDs are derived from the International Organization for Standardization's ISO Standard 3166. *See* ISO STANDARD 3166, *available at* <http://www.iso.org/iso/english_country_names_and_code_elements> (Int'l Org. for Standardization 2007).

[19] Jennifer Arnette-Mitchell, *State Action Debate Reborn Again: Why the Constitution Should Act as a Checking Mechanism for ICANN's Uniform Dispute Resolution Policy*, 27 HAMLINE J. PUB. L. & POL'Y 307, 314 (2006).

[20] Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 17.

[21] ICANN, *FAQs*, <http://www.icann.org/faq/#registerdomain>.

[22] Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 17, n. 19; Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 443. A list of registrars can be found at <http://www.internic.net/regist.html>.

[23] Juliet M. Moringiello, *Seizing Domain Names to Enforce Judgments: Looking Back to Look to the Future*, 72 U. CIN. L. REV. 95, 100 (2003).

[24] ICANN, *Top-Level Domains (gTLDs)*, <http://192.0.34.163/tlds/>.

[25] EduCause, *".Edu" Policy Information*, <http://www.educause.edu/edudomain/policy.asp> (last visited Nov. 25, 2007).

[26] Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 443 (2006).

[27] Aaron J. Burnstein, *Stopping Internet-Based Tobacco Sales Through Domain-Name Seizure*, 16 HEALTH MATRIX 279, 295 (2006).

[28] Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 52–62.

[29] Angela Proffitt, *Drop the Government, Keep the Law: New International Body for Domain Name Assignment Can Learn from United States Trademark Experience*, 19 LOY. L.A. ENT. L.J. 601, 608 (1999).

[30] Management of Internet Names and Addresses, 63 Fed. Reg. at 31,741 (1998), *available at* <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>.

[31] Reece Roman, *What if ICANN Can't?: Can the United Nations Really Save the Internet*, 2006 SYRACUSE SCI. & TECH. L. REP. 6, 9 (2006); ICANN, *Bylaws for the Internet Corporation for Assigned Names and Numbers*, <http://www.icann.org/general/bylaws.htm>.

[32] Dept. of Commerce and ICANN, *Memorandum of Understanding* (1998), *available at* <http://www.icann.org/general/icann-mou-25nov98.htm>.

[33] Dept. of Commerce and ICANN, *Joint Project Agreement* (2006), *available at* <http://www.icann.org/general/JPA-29sep06.pdf>.

apparent policy implications.[34] For instance, ICANN creates new generic TLDs (gTLDs), which may seem like a strictly technical activity.[35] Yet the creation of a TLD may involve controversial public policy, as with a proposal to establish an ".xxx" TLD for the adult entertainment industry.[36] In that instance, policy concerns over legitimizing pornography and restricting Internet free-speech eventually sank the proposal.[37] ICANN also conditions domain-name registration upon the registrant paying a fee, submitting to ICANN arbitration in the event of a domain dispute, and disclosing accurate contact information.[38] ICANN thus uses control of the DNS's authoritative root to ensure that domain-name holders can be contacted and forced into ICANN-sponsored arbitration in the event of a dispute—a policy that favors trademark holders when trademarks are used in domain names.[39]

III. POLITICAL CYBERSQUATTING

Domain-name disputes are a built-in consequence of the DNS structure[40] because the DNS relies on uniqueness to operate.[41] The DNS pairs a unique domain name with its matching, unique IP address. Uniqueness breeds conflict over one-of-a-kind resources. Multiple parties are certain to claim rights to words that form the SLD portion of a unique domain name.[42] This inherent DNS feature alone leads to frequent clashes between potential rights-holders.[43]

Political candidates have experienced domain-name controversies. Some candidates have sparred with corporations, as when the Boston-based brewer of Samuel Adams beer claimed rights to domain names held by Samuel Adams, a mayoral candidate in Portland, Oregon.[44] Other disputes have involved private individuals, as when Senators John Kerry and John Edwards sought to acquire KerryEdwards.com from Indiana native Kerry Edwards for their 2004 general-election campaign.[45] Still other political candidates' domain conflicts have been caused by "cybersquatters."[46] This section focuses on cybersquatting by describing its general occurrence and explaining the problems it poses for political candidates.

A. Cybersquatting outside of the political context

Commercial cybersquatting is the deliberate registration of a domain name with the intent to profit by either ransoming the name to the highest bidder or diverting web traffic.[47] Commercial cybersquatting grew along with the Internet. As the number of Internet users

---

[34] Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 96–105.

[35] *See* ICANN General Names Supporting Organization, *GNSO Policy Work on New gTLDs*, <http://gnso.icann.org/issues/new-gtlds/>.

[36] Christopher Rhoads, *Red-Light District: Plan for Adult Area Sparks a Fight on Control of Web*, WALL ST. J., May 10, 2006, at A1.

[37] Patty Chan, *Safer (Cyber)Sex with .XXX: The Case for First Amendment Zoning of the Internet*, 39 LOY. L.A. L. REV. 1299, 1317–1318 (2006).

[38] *See, e.g.*, eNom, *Registration Agreement*, <http://www.enom.com/terms/agreement.asp>. Domain-name holders' contact information is generally publicized, but some avoid this by paying an anonymous-registration fee. William M. Bulkeley, *Should Owners Of Web Sites Be Anonymous?*, WALL STREET J., Apr 27, 2006, at B1. Anonymous registrants are still reachable through their domain-name registrar. *See, e.g.*, Aplus.net, *Domain Name Privacy*, <http://domains.aplus.net/domainprivacy.html>.

[39] "Currently, this power is used to require domain name registrants to publish their addresses and telephone numbers on a worldwide readable list and to agree that any trademark holder in the world aggrieved by their registration can demand arbitration regarding ownership of the name under an eccentric set of rules and standards." Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 21.

[40] Marshall Leaffer, *Domain Names, Globalization, and Internet Governance*, 6 IND. J. GLOBAL LEGAL STUD. 139, 147 (1998).

[41] This is subject to minor exceptions, as when resources are interchangeable. Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 38.

[42] Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 418–419.

[43] *See* Jason Rhodes, *Last Call for Cybersquatters?: The Anti-Cybersquatting Consumer Protection Act*, 2003 SYRACUSE L. & TECH. J. 1 (2003).

[44] KPTV Blog, *Brewer, Ore. Candidate Bump Heads Over Campaign Site* (Oct. 26, 2007, 9:34 PDT), *available at* <http://www.kptv.com/news/14431394/detail.html?taf=ptl1>.

[45] Howard Wolinsky, *Indiana Man Hopes to Sell His $25 Web Domain for Highest Bid*, CHICAGO SUN-TIMES, July 9, 2004, at 4.

[46] Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 419.

[47] *See* WORLD INTELLECTUAL PROPERTY ORGANIZATION, THE MANAGEMENT OF INTERNET NAMES AND ADDRESSES: INTELLECTUAL PROPERTY ISSUES—FINAL REPORT OF THE WIPO INTERNET DOMAIN NAME PROCESS 23 (1999), available at <http://www.wipo.int/amc/en/processes/process1/report/finalreport.html>; Belczyk, *Domain Names*, *supra* note 9, at 501.

and the amount of Internet-related commerce exploded, domain names became increasingly valuable commodities. Speculators snatched up domain names with real-world significance, like Panavision.com[48] and Chanel Perfumes.com.[49] Commercial cybersquatting is still on the rise as individuals and corporations employ new methods to circumvent existing laws and earn profits.[50] Despite the threat of lawsuits, they can turn their small domain-name registration fee into a healthy profit by "exploit[ing] the settlement value of cases."[51] And several signs suggest that commercial cybersquatters find cybersquatting opportunities through searching news reports,[52] utilizing advanced technologies and techniques,[53] and exploiting ICANN's new DNS policies.[54] Commercial cybersquatters' increased sophistication suggests that their activities will continue, if not expand, for the foreseeable future.

Cybersquatters may also procure domain names for non-commercial motives[55]—a practice often called "cybergriping" or "cyberfraud."[56] Many non-commercial cybersquatters register domains that contain others' trademarked or well-known names to either disseminate damaging information or deny others domain-name registration opportunities. An individual might, for example, register a domain like SearsRoebuck.com to air grievances against Sears department store.[57] Non-commercial cybersquatting differs from commercial cybersquatting in that it usually "raise[s] competing social interests . . . in the free speech area" to a greater extent.[58]

Commercial and non-commercial cybersquatters may register domain names that contain common misspellings of trademarked or well-known names.[59] This widespread tactic is known as "typosquatting."[60] An attorney, for example, registered EsteLauder.com, a common misspelling of cosmetics giant Estée Lauder's web site.[61] He intended to divert web traffic from Estée Lauder's site and collect consumer complaints to use in his product-liability practice.

Domain names perform a role similar to that of trademarks and trade names.[62] They help Internet users quickly locate online products, services, and information in a setting that lacks many real-world "indications of source and authenticity."[63] Domain names that match trademarks or well-known names can also preserve and expand consumers' goodwill toward

---

[48] *See generally*, Panavision Intern., L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).

[49] *See generally*, Chanel, Inc. v. Cologne Zone, WIPO Arb. and Mediation Center , D2000-1809 (2000), *available at* <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1809.html>.

[50] Press Release, World Intellectual Property Organization, *Cybersquatting Remains on the Rise with Further Risk to Trademarks from New Registration Practices* (Mar. 12, 2007), *available at* <http://www.wipo.int/pressroom/en/articles/2007/article_0014.html>.

[51] Froomkin, *Wrong Turn in Cyberspace*, *supra* note 3, at 61.

[52] Press Release, World Intellectual Property Organization, *Cybersquatting Remains on the Rise with Further Risk to Trademarks from New Registration Practices* (Mar. 12, 2007), *available at* <http://www.wipo.int/pressroom/en/articles/2007/article_0014.html>; AT&T Knowledge Venture II, L.P. v. Rnetworld, Case No. D2007-0035 (WIPO Arb. and Mediation Center 2007), *available at* <http://www.wipo.int/amc/en/domains/decisions/html/2007/d2007-0035.html>.

[53] Press Release, World Intellectual Property Organization, *Cybersquatting Remains on the Rise with Further Risk to Trademarks from New Registration Practices* (Mar. 12, 2007), *available at* <http://www.wipo.int/pressroom/en/articles/2007/article_0014.html>. The practice of "parking" pay-per-click advertisements on otherwise blank web pages to generate revenue before auctioning off the domain to the highest bidder is described in Mattel, Inc. v. Adventure Apparel, No. 00 Civ. 4085, 2001 U.S. Dist LEXIS 13885 at 13 (S.D.N.Y. 2001).

[54] Press Release, World Intellectual Property Organization, *Cybersquatting Remains on the Rise with Further Risk to Trademarks from New Registration Practices* (Mar. 12, 2007), *available at* <http://www.wipo.int/pressroom/en/articles/2007/article_0014.html>.

[55] Jacqueline D. Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 WAKE FOREST L. REV. 1361, 1383 (2005).

[56] *See generally* Blossom Lefcourt, *The Prosecution of Cybergripers Under the Lanham Act*, 3 Cardozo Pub. L. Pol'y & Ethics J. 269 (2004).

[57] Sears, Roebuck, and Co. v. Hanna Law Firm, Case No. D2000-0669 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0669.html>.

[58] Lipton, *Beyond Cybersquatting*, *supra* note 55, at 1403.

[59] *See, e.g.*, Electronics Boutique Holdings Corporation v. Zuccarini 33 Fed.Appx. 647 (2002).

[60] Lipton, *Beyond Cybersquatting*, *supra* note 55, at 1384-1385.

[61] Estée Lauder Inc. v. Hanna, Case No. D2000-0869 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0869.html>.

[62] Michael S. Denniston and Margaret Smith Kubiszyn, *www.yourclient.com: Choosing Domain Names and Protecting Trademarks on the Internet*, 61 ALA. L. REV. 40, 41–42 (2000).

[63] Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 416–417.

an individual or a corporation.[64] Cybersquatters are motivated by opportunities to accrue benefits—economic or otherwise—by duping an Internet user into believing a domain is affiliated with a trademarked or well-known name.[65] This so-called "free riding" unfairly exploits others' efforts to build public brands and reputations.[66] Cybersquatting is also problematic because consumers "may be misled about the source of the [information,] product or service offered on the Internet."[67] This presents a "high likelihood that the consumer will be 'deceived and defrauded, or at a minimum, confused.' "[68]

Even in an era when Internet users utilize powerful search engines like Google and Yahoo! to locate online content, domain names are important.[69] First, many search engines give greater priority to web sites when their domain names include the search terms.[70] Second, domain names are convenient mnemonics that allow Internet users to bypass search-result lists and directly access information. Third, domain names facilitate user-to-user "buzz" about a web site because they are a more convenient reference than a description of general content or search steps. Because domain names retain importance, cybersquatting is a significant obstacle to the Internet functioning optimally.[71]

B. Political cybersquatting

Cybersquatters first began by gobbling-up corporations' and celebrities' domain names, but some have since entered the political arena. They actively seek and acquire "domain names that are intuitively linked to candidates and their campaigns."[72]

"Political cybersquatting" appears to be widespread. Prior to the 2004 U.S. presidential election, for example, 1,604 domain names evoked the name of either President George W. Bush or Senator John Kerry. Less than 1 percent of these domains were held by the candidates' campaigns.[73] Cybersquatting has affected campaigns for nearly all political offices in the United States. Candidates for U.S. Senate,[74] U.S. House,[75] governor,[76] lieutenant governor,[77] attorney general,[78] state senate,[79] state house,[80] mayor,[81] and county commissioner[82] have all been recent cybersquatting targets. Even several domains using the name of a judicial candidate in Angelina County, Texas, were snatched by a cybersquatter.[83] Political cybersquatting is now a worldwide phenomenon. Cybersquatters hold domains associated

---

[64] Joshua Clowers, *On International Trademark and the Internet: The Lanham Act's Long Arms*, 13 RICH J.L. & TECH. 4, 4 (2006).
[65] *See* William M. Landes and Richard A. Posner, *The Economics of Trademark Law*, 78 TRADEMARK REP. 267, 270 (1986).
[66] Clowers, *On International Trademark and the Internet*, *supra* note 64, at 5.
[67] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741, 31,747 (1998), *available at* <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>.
[68] Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 416–417.
[69] Thus, wallstreet.com sold for over $1 million. *See* Denniston and Kubiszyn, *www.yourclient.com*, *supra* note 62, at 41.
[70] *See, e.g.*, Raj Krishnan, Improve Snippets with a Meta Description Makeover, Official Google Webmaster Central Blog (Sept. 27, 2007 at 6:46 ET), *available at* <http://googlewebmastercentral.blogspot.com/2007/09/improve-snippets-with-meta-description.html>.
[71] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741, 31,747 (1998), *available at* <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>.
[72] Matthew Coleman, *Domain Name Piracy and Privacy: Do Federal Election Regulations Offer a Solution?*, 19 YALE L. & POL'Y REV. 235, 235 (2000).
[73] Tim Gnatek, *No Jackpot for Domain-Name Speculators*, N.Y. TIMES, Oct. 14, 2004, at G3.
[74] *See, e.g.*, Sam Attlesey, *Dot.Com Campaign: Cyber-Savvy Hoping to Gain by Reserving Political Domains*, DALLAS MORNING NEWS, Feb. 5, 2001, at 1A.
[75] *See, e.g.*, Greg Gordon, *Buy-and-Switch Web Tactic Throws Politicians for a Loop*, STAR TRIB., Apr. 4, 2002, at 1B.
[76] *See, e.g.*, Jo Mannies, *Candidates Find It's Risky to Drop Rights to Campaign: Web Sites' Names Can be Used Later for Porn*, ST. LOUIS POST-DISPATCH, Sept. 7, 2001, at A1.
[77] *See, e.g.*, Nicole Usher, *Political Pranks on Web Sites Can Frustrate, Sidetrack Voters*, DALLAS MORNING NEWS, Aug. 18, 2002 (page unavailable online).
[78] *See, e.g.*, Attlesey, *Dot.Com Campaign*, *supra* note 74, at 1A.
[79] *See, e.g.*, Gordon, *Buy-and-Switch Web Tactic Throws Politicians for a Loop*, *supra* note 75, at 1B.
[80] Mike Madden, *Dot.Com Name Game Enters Political Arena From Ed Rendell to Steve Forbes' Wife, Addresses are Scooped Up by Speculators*, PHILADELPHIA INQUIRER, Feb. 7, 2000, at A1.
[81] *See, e.g.*, Edward Epstein, *Willie Brown Finds Web Name Taken; Contractor for Reilly Registered Net Sites*, S.F. CHRONICLE, Aug. 10, 1999, at A1.
[82] *See, e.g.*, Kevin Krause, *Several Candidates Face Stiff Costs for Buying Web Sites' Domain Names Bought by Entrepreneurs Hoping to Resell Them*, DALLAS MORNING NEWS, Feb. 20, 2004, at 14B.
[83] Greg Jefferson, *Bolanos Sues Bonilla Over Web Sites*, SAN ANTONIO EXPRESS-NEWS, Oct. 8, 2006 at 2B.

with prominent political leaders from Spain,[84] the United Kingdom,[85] France,[86] Germany,[87] Venezuela,[88] Mexico,[89] Japan,[90] China,[91] Russia,[92] and other nations.[93] And political cybersquatters themselves are often located outside of the United States.[94]

Political cybersquatting is an "analog to traditional cybersquatting" for four principal reasons.[95] First, political cybersquatters, like cybersquatters generally, often horde domain names.[96] Individuals and corporations hold portfolios of domains that match political candidates' names. Joseph Culligan of Florida, for example, has possessed more than 530 political domain names, including President BillClinton.com, ImpeachAlGore.com, Reelect PresidentBush.com,FirstLadySabrinaForbes.com, SenatorJonCorzine.com, RobertTorricelli.com, and FirstLadyLauraBush.com.[97] Culligan offered PresidentHatch.com to U.S. Senator Orrin Hatch for $45,000.[98] Similarly, cybersquatter Peter Lucas once owned over 100 candidate-related domain names, including Clinton2008.com and Frist2008.com.[99] Second, political cybersquatters and traditional cybersquatters use similar techniques, such as typosquatting. During U.S. Senator Hillary Clinton's campaign in 2000, for example, typing in Hillary200.org (one "0" less than the campaign's Hillary2000.org site) would take you to a Clinton parody site.[100] Likewise, typing in JohnKery.com (one "r" less than U.S. Senator John Kerry's site) linked to an anti-abortion web site called PlannedChildhood.org.[101] Third, political cybersquatters' motives are both commercial and non-commercial. Some seek to auction a campaign domain to the highest bidder, like the cybersquatter who reportedly sold Forbes2000.com to presidential candidate Steve Forbes for over $10,000.[102] Others seek to sell products to Internet users looking for campaign sites, like the cybersquatter who registered JohnKerryForPrez.com to sell long-distance phone plans and calling cards.[103] Non-commercial motives for political cybersquatting

---

[84] Convergencia Democratica de Catalunya v. arm as, Case No. DTV2003-0005 (WIPO Arb. and Mediation Center 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>.

[85] Jeffrey Archer v. Alberta Hotrods, Case No. DTV2006-0431 (WIPO Arb. and Mediation Center 2006), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0431.html>.

[86] According to the WhoIs database, a domain name identical to the name of French President Nicholas Sarkozy, www.sarkozy.com, is registered by Phillips Paul in Dallas, Texas. The site links automatically to <http://www.lepolitique.com>, a political web site.

[87] According to the WhoIs database, a domain name associated with German Chancellor Andrea Merkel, Andrea Merkel.com, was registered by Chris Hoffman in Santa Monica, California. The site ultimately links to an anti-abortion web site at <http://www.plannedchildhood.org/>.

[88] According to the WhoIs database, HugoChavez.com, a domain name identical to the name of Venezuelan President Hugo Chavez, is held by Li Chow of Chong Qing, China.

[89] FelipeCalderon.com, a domain identical to the name of Mexican President Felipe Calderon, has been registered anonymously. The site provides advertisements and links for beauty supplies and health insurance, among other things.

[90] JunichiroKoizumi.com, a domain identical to the name of former Japanese Prime Minister Junichiro Koizumi, is held by Adam Dicker of Georgetown, Kentucky. The site offers links to apartment and dating services.

[91] According to the WhoIs database, HuJintao.com, a domain identical to the name of China's President, Hu Jintao, is owned by Gregg Ostrick of Birmingham, Alabama. The site markets movie posters.

[92] VladimirPutin.com, a domain that is identical to the name of Russian President Vladimir Putin, is held by Vital Domains, Ltd. of London, UK. The site is used as an anti-Putin blog.

[93] I did a brief search of world-famous politicians and came up with the list presented in the text. Given the frequency with which political cybersquatting occurs in the United States, it is safe to assume that politicians from unlisted nations have also been the target of cybersquatting.

[94] *See, e.g.*, Madden, *Dot.Com Name Game Enters Political Arena*, *supra* note 80, at A1.

[95] Lipton, *Who Owns Hillary.Com?*, *supra* note 55, at 60.

[96] Admittedly, some political cybersquatters are also "one-timers" like Barbara Gilmartin, a social worker who bought EdRendell.com—namesake of Pennsylvania Governor Edward Rendell—for the simple "novelty of having it." Madden, *Dot.Com Name Game Enters Political Arena*, *supra* note 80, at A1.

[97] Ibid.

[98] Andrew J. Glass, *Internet Domain Names Become a Pain for Public Figures*, ATLANTA J. & CONST., Aug. 22, 1999, at A11.

[99] Dave Levinthal, *Master of Your Domain? Check Before You Run: For Political Cybersquatters, the Name of the Game is Profit*, DALLAS MORNING NEWS, Apr. 4, 2004, at 8A.

[100] Andrew J. Glass, *Internet Domain Names Become a Pain for Public Figures*, *supra* note 98, at A11.

[101] This is a fairly common method used by commercial and non-commercial cybersquatters. Another example is that typing in BarackObamma.com (adding an "m" to BarackObama.com, an official campaign web site, took you to a blog piece entitled "Losing Faith in Obama").

[102] Levinthal, *Master of Your Domain? supra* note 99, at 8A.

[103] Gnatek, *No Jackpot for Domain-Name Speculators*, *supra* note 73, at G3.

include a desire to criticize,[104] parody,[105] inconvenience,[106] or impersonate[107] a political candidate. Fourth, political cybersquatting, like cybersquatting generally, free-rides on efforts to build public reputations, fosters online deception and confusion, and prevents Internet users from reliably employing domain names to locate online information.

While political cybersquatting and its commercial antecedent are alike in many respects, cybersquatting is particularly pernicious when it involves political candidates. As explained below, web sites are especially vital to modern political campaigns, political campaigns' organizational structures and operating environments leave candidates exceptionally exposed to cybersquatting, and candidates cannot rely on existing preventive and remedial measures to consistently solve cybersquatting problems.

1. Web Sites Are Vital to Modern Political Campaigns

Web sites are critical to today's political campaigns. Any campaign's core purpose is to inform and mobilize a large number of people within a relatively short period. Oftentimes this must be done on a "shoestring" budget. Web sites efficiently perform three vital campaign functions. First, a campaign web site is an invaluable fundraising tool. Candidates use their sites to solicit contributions directly, to sell campaign paraphernalia, to publicize fundraising events, and to recruit fundraisers. These efforts have paid off handsomely. Total online fundraising in the United States exceeded $100 million in 2006.[108] In a single day, long-shot 2008 U.S. presidential candidate Ron Paul raised $6 million from over 24,000 contributors online.[109] Other candidates have attracted record numbers of new donors largely because the Internet allows the general public to make political contributions more easily than in the past.[110] Second, a campaign web site is an effective organizational tool. Candidates use web sites to enlist volunteers, facilitate voter-to-voter communications, and encourage grassroots events. In particular, Barack Obama's ability to organize supporters through the Internet is often cited as a major reason for his successful run for the Democratic Party's presidential nomination in 2008.[111] Third, campaign web sites are a useful communication tool. The number of people who list the Internet as their primary source for political news has recently doubled and a substantial percentage seek political information from candidates' web sites.[112] Web sites thus offer candidates an important alternative to paying for expensive ads or relying on uncertain broadcast news coverage. Candidates speak directly to voters through sites that supply policy proposals, offer detailed biographies, provide press releases, disclose campaign contributors, feature candidate blogs, and furnish web videos. U.S. presidential candidates Hillary Clinton and Fred Thompson signaled campaign sites' importance by announcing their respective candidacies through online videos on their web sites.[113]

Even with many of today's Internet users turning to powerful search engines to locate online content, candidate web sites are most effective as campaign tools if they are affiliated with desirable domain names.[114] Domains en-

---

[104] Gordon, *Buy-and-Switch Web Tactic Throws Politicians for a Loop*, *supra* note 75, at 1B.
[105] Usher, *Political Pranks on Web Sites Can Frustrate, Sidetrack Voters*, *supra* note 77.
[106] Mannies, *Candidates Find It's Risky to Drop Rights to Campaign Web Sites' Names*, *supra* note 76, at A1.
[107] Jon H. Oram, *Will the Real Candidate Please Stand Up?: Political Parody on the Internet*, 5 J. INTELL. PROP. L. 467, 471 (1998).
[108] Michael Cornfield and Lee Rainie, *The Web Era Isn't as New as You Think*, WASHINGTON POST, Nov. 5, 2006, at B3.
[109] Kenneth Vogel, *Ron Paul Becomes $6 Million Man*, THE POLITICO (Dec. 17, 2007 11:34 EST), *available at* <http://www.politico.com/news/stories/1207/7421.html>.
[110] *See, e.g.*, Mike Dorning, *Clinton Edges Obama in Donors*, CHICAGO TRIBUNE, Oct. 3, 2007, at 6.
[111] Ben Adler, *Can McCain Compete with Obama Online?* THE POLITICO (June 15, 2008 16:37 EST), <http://www.politico.com/news/stories/0608/11086.html>.
[112] Lee Rainie and John Horrigan, *Election 2006 Online*, Pew Internet and American Life Project 15 (Jan. 17, 2007), *available at* <http://www.pewinternet.org/pdfs/PIP_Politics_2006.pdf> (showing that 20 percent of the 60 million Americans who seek political information online visited candidates' web sites).
[113] Dan Balz, *Hillary Clinton Opens Presidential Bid*, WASHINGTON POST, Jan. 21, 2007, at A1; John King, *Thompson: I Can Stop Hillary* Clinton, CNN Politics Blog (Sept. 6, 2007 21:19 EDT), *available at* <http://www.cnn.com/2007/POLITICS/09/06/thompson/index.html>.
[114] Lisa Leiter, *Parody in the Home Pages Scrambles "the Real Thing,"* WASHINGTON TIMES, Mar. 25, 1996, at 16 ("the domain name itself is important in a political campaign").

sure better search-result placement, serve as a mnemonic for voters, and facilitate voter-to-voter "buzz" about a site. Easy-to-remember domain names also guard against cybersquatters who constantly devise new tactics to manipulate search-engine results.[115] One cybersquatter, for example, nabbed KenCalvert.com and used metatags (information that search engines use to find search-related web content) related to U.S. Congressman Ken Calvert to steer search-engine users to a pornographic web page.[116] Internet users who knew Ken Calvert's true domain name did not fall victim to the cybersquatter's tactics.

Because campaigns must reach a broad public, political cybersquatting can harm a campaign by seizing a key outreach tool from a candidate's hands.[117] Cybersquatters who "appropriat[e] an official-sounding name" hinder a candidate's "ability to recruit supporters, communicate with the press, . . . disseminate [a] message to the undecided voters," and raise funds by drawing web traffic away from the candidate's site.[118] Voters, too, have an interest in knowing that the online location where they volunteer, read, and contribute is an official campaign site. Political cybersquatting's diverting effects can be significant. In 1996, for example, non-commercial cybersquatters who registered Dole96.org, Clinton96.org, Forbes96.org, and Buchanan96.org said that 20 percent of the inquiries they received were intended for the campaigns.[119] For part of the 2008 election cycle, the cybersquatted site JohnMcain.com featured a "contribution" web page identical to an official campaign "contribution" web page at JohnMcCain.com.[120] It is uncertain whether any supporters of Republican presidential candidate John McCain were defrauded out of money, but that danger was certainly present.

2. Political Campaigns' Organizational Structures and Operating Environments Make Candidates Vulnerable to Cybersquatting

Characteristics common to campaign organizations and political campaigns render candidates uniquely vulnerable to cybersquatting.

a. Campaign organizations are short-term and relatively late-starting.

Two features of political campaign practices make candidates particularly easy cybersquatting targets.[121] First, campaign organizations are typically short-term enterprises that operate in a time-sensitive environment. Campaigns must obtain their domain names quickly. Candidate-related domain names therefore provide an inviting mark for cybersquatters hoping to convert candidates' urgency into a premium domain-name price. Cybersquatters also exploit campaign organizations' transitory nature by buying up candidate-related domains after the election season. They free-ride on a candidate's reputation and capture a campaign site's post-election web traffic to sell products or exact revenge. After former U.S. Senator John Ashcroft failed in his re-election bid, for example, an Armenian company purchased his campaign domain and linked it to a pornographic web site.[122] Similarly, Pat Robertson's discarded campaign site once helped visitors "hook up with swingers

---

[115] *See, e.g.*, Heather Greenfield, *Political Bloggers Coordinate "Google Bombs,"* MSNBC Politics Blog (Oct. 25, 2006 16:00 CDT), <http://www.msnbc.msn.com/id/15418130/> (describing an effort by Bloggers to "Google bomb"—manipulate search results by repeatedly clicking on sites—certain candidates in the run-up to the 2006 election).

[116] Kenneth Calvert v. Domain Strategy, Inc., Case No. FA0306000162075 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/162075.htm>.

[117] *See, e.g.*, Kevin Krause, *Several Candidates Face Stiff Costs for Buying Web Sites' Domain Names Bought by Entrepreneurs Hoping to Resell Them*, DALLAS MORNING NEWS, Feb. 20, 2004, at 14B.

[118] Coleman, *Domain Name Piracy and Privacy*, *supra* note 72, at 246.

[119] Lisa Leiter, *Parody in the Home Pages Scrambles "the Real Thing,"* WASHINGTON TIMES, Mar. 25, 1996, at 16.

[120] Interview with Benjamin Olson, Deputy E-Campaign Director, John McCain 2008, Inc. (May 15, 2008).

[121] Other campaign organization features may come into play as well. For example, the fact that campaigns are largely run by volunteers may mean that there is a lack of awareness about cybersquatting or the need to combat it. *See* Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, N.Y. TIMES, Nov. 18, 2006, at A15.

[122] Mannies, *Candidates Find It's Risky to Drop Rights to Campaign Web Sites' Names*, *supra* note 76, at A1. *See also* Kenneth Calvert v. Domain Strategy, Inc., Case No. FA0306000162075 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/162075.htm>.

looking for sex."[123] Other expired campaign web sites were used to sell Pokemon video games, college term papers, and debt consolidation services.[124]

Second, campaign organizations often launch well after the press and the public anticipate a candidate's run for office. This gives cybersquatters a significant head start. Cybersquatter Chris Hayden registered Hillary2000.com, Clinton2000.com, and HillaryClinton2000.com in 1998—long before then-First Lady Hillary Clinton began concrete preparations for her 2000 U.S. Senate campaign.[125] Even more astounding, Australian Brett Maverick registered Hillary2008.com in 1999.[126] Other politicians have likewise fallen prey to cybersquatters. Thirty-nine domains incorporating George W. Bush's name were registered by cybersquatters prior to the beginning of his first presidential campaign. BarackObama2008.com was nabbed only hours after the U.S. Senator's eloquent address at the 2004 Democratic National Convention. RudyForPresident.com, an obvious reference to former New York City Mayor Rudy Giuliani, was registered eight days after the terrorist attacks of September 11, 2001.[127] Cybersquatters also register domains related to potential presidential tickets. By late 2006, most conceivable presidential-ticket combinations for 2008 were taken by cybersquatters, including McCainGiuliani2008.com and ClintonGore2008.com.

Candidates in this respect are perhaps even more vulnerable to cybersquatting than corporations, the typical targets of conventional cybersquatting. Business corporations usually exist for long and indefinite periods, so cybersquatters cannot exploit short-term status. Most corporations also have an early advantage over cybersquatters in registering domain names because they rarely invite press coverage before they start up.

b. Political campaigns are divisive.

Political campaigns' divisive nature also exposes candidates to cybersquatting.[128] Campaigns are inherently divisive because candidates compete directly in a zero-sum game. This winner-take-all environment prompts some candidates to purchase their opponents' domain names. The campaign of former U.S. Congressman Henry Bonilla, for example, registered at least a dozen domains that included the name of Bonilla's opponent, Rick Bolanos. It posted statements on the sites that read "Coming soon—information for the benefit of voters in the 23rd Congressional District," to give an impression that Bolanos had neglected to create a campaign web site.[129] Likewise, San Francisco mayoral candidate Clint Reilly registered several domains based on his potential opponents' names.[130] The Texas Republican Party has also cybersquatted TXDemocrats.com—a close resemblance to the Texas Democratic Party's web site, TXDemocrats.org.[131] Other examples of political-opponent cybersquatting abound.[132]

Campaigns also debate contentious policy issues, thereby energizing potential non-commercial cybersquatters to register candidate domain names. Cybersquatters may want to criticize,[133] silence,[134] or even demonize[135] a candidate because of her stance on hotly debated issues.

Campaigns are generally more divisive than a competitive commercial environment. Cor-

---

[123] Peter Hartlaub, *Click on a Former Candidate's Web Site You Never Know What You'll Find, From Pokemon to Hooking Up*, S.F. CHRON., Oct. 28, 2004, at E1.
[124] Ibid.
[125] Glass, *Internet Domain Names Become a Pain for Public Figures*, *supra* note 98, at A11.
[126] Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, *supra* note 121, at A15.
[127] All of the above examples and the following are described in *id.* at A15.
[128] Other characteristics of political campaigns also come into play, like the public nature of campaigns. Candidates, even in races for local office, receive publicity. Greater publicity means greater probability of cybersquatting.
[129] Jefferson, *Bolanos Sues Bonilla Over Web Sites*, *supra* note 83, at 2B.
[130] Edward Epstein, *Willie Brown Finds Web Name Taken*, *supra* note 81, at A1.
[131] Usher, *Political Pranks on Web Sites Can Frustrate, Sidetrack Voters*, *supra* note 77.
[132] *E.g.*, Nathan Bierma, *What's In a (Web) Name? Pols Race to Nab Domains*, CHICAGO TRIB., Dec. 05, 2002, at 2.
[133] Editorial, *George W. and the Cybersquatter*, CHICAGO TRIB., Dec. 14, 1999, at 26 (describing the activities of Zack Exley, who registered gwbush.com before George W. Bush's campaign could get it).
[134] *E.g.*, Mannies, *Candidates Find It's Risky to Drop Rights to Campaign Web Sites' Names*, *supra* note 76, at A1.
[135] Friess, *As Candidates Mull '08, Web Sites Are Already Running*, *supra* note 121, at A15.

porations do not always operate in a winner-take-all setting. They may not even have direct competition in their specialized market or geographic region. Moreover, for obvious commercial reasons, corporations seldom deal with issues that make them lightning rods for criticism and non-commercial cybersquatting. It is hard to imagine, for example, a state-wide business's CEO discussing abortion, immigration, or gay marriage the way a gubernatorial candidate must often do. Candidates are therefore unusually vulnerable to cybersquatting because of the intense, conflict-ridden environment in which they operate.

3. Existing Cybersquatting Preventive Measures and Remedies Are Ill-Suited to Help Candidates

Given candidates' unique vulnerabilities, they often confront cybersquatting threats and problems. Their choices are to seek to purchase domain names preemptively, to negotiate with cybersquatters, or to attempt to wrench domain names from them. Each choice has its advantages, but none can reliably avoid or solve political cybersquatting problems.

a. Purchasing domain names may prove impractical, expensive, and strategically foolish.

Candidates can preempt cybersquatters by purchasing domain names long before their campaigns begin. This most effectively forestalls cybersquatters when candidates register multiple variations and misspellings (i.e., JohnSmith.com, JonSmith.com, JohnSmithForCongress.com, SmithForCongress.com, JohnSmith2008.com, Smith2008.com, SmithForCongress2008.com, etc.) under as many TLDs as possible (i.e., ".com," ".org," ".net," ".info," ".us," ".mobi," etc.).[136] The Republican National Committee has an effective advance-buying program. It holds "dozens of web domains for defensive purposes," including GeorgePBush.com, for the nephew of President George W. Bush and son of former Florida Governor Jeb Bush.[137] But advance purchasing has three main shortcomings. First, some candidates might not be able to purchase domains well in advance. Many politicians decide to run for office only shortly before election season begins. Presidential tickets are particularly helpless. To beat cybersquatters to the punch, presidential candidates would need to think of potential running mates years before securing their party's nomination.[138] Second, the "sheer number of permutations of a potential candidate's name . . . make[s] domain registration an endless guessing game."[139] This either leaves opportunities open to cybersquatters or forces candidates to spend money on a vast number of domains.[140] Third, candidates who register domains in advance often unintentionally signal their intention to run for office.[141] Many candidates fail to realize that domain-name registrants' information is typically made available to the public.[142]

After a domain name is purchased or otherwise obtained, a candidate can prevent post-election cybersquatting by holding the domain indefinitely. Short-term campaign organizations may have difficulty doing this, but candidates can ask their parties to hold a domain.

b. Negotiation gives political cybersquatters the opportunity to extract high prices or gain access to candidates.

Negotiation is an option available to all cybersquatting targets, including candidates. Candidates can make first contact by using a cybersquatter's information found in the WHOIS—a database of domain-name registrants.[143] Nego-

---

[136] The ".mobi" TLD will likely become more crucial to campaigns in the future, as it provides a special TLD for Internet users on their handheld devices. *See* <http://mtld.mobi/> for more information.

[137] Levinthal, *Master of Your Domain? supra* note 99, at 8A.

[138] George W. Bush's 2000 campaign held BushPataki.net, BushEngler.com, and BushRidge.net more than six months before the New Hampshire primary. *See* Michael Zuzel, *Bush Caught in Web of His Own Making*, THE COLUMBIAN, June 15, 1999, at A11.

[139] Bierma, *What's In a (Web) Name? supra* note 132, at 2.

[140] Attlesey, *Dot.Com Campaign*, *supra* note 7, at 1A.

[141] *See, e.g.*, J. Scott Orr, *Bushwhitman.com: Eminent Domain? GOP Campaign Owns Rights—Just in Case*, STAR-LEDGER, Sept. 27, 1999, at 1.

[142] Public disclosure can be avoided, however, by paying an anonymous registration fee. William M. Bulkeley, *Should Owners Of Web Sites Be Anonymous? supra* note 38, at B1.

[143] Internet users can search the WhoIs at <http://www.whois.net/>.

tiation offers some advantages. It may lead to a cybersquatting problem's quick resolution. Even if it doesn't, negotiation lets candidates gather evidence of "bad faith" registration that may be needed later to take the domain from a cybersquatter, as discussed in the next section. Negotiation, though, obviously gives many cybersquatters exactly what they want—a chance to receive an exorbitant sum in exchange for a domain. In the political-cybersquatting context, an additional disadvantage is that cybersquatters can potentially leverage their unique asset to accomplish corrupt aims. Political cybersquatters may register low-face-value domain names as a way to extract favors from, or gain access to, candidates.[144] Cybersquatter Peter Lucas, for example, once said "Don't I kind of destroy the myth of one man, one vote? . . . I guess I hold a little more power than the average person."[145]

c. Wresting domain names from political cybersquatters is difficult because of existing processes' shortcomings.

Candidates may use several methods to capture domain names held by cybersquatters. U.S. candidates sometimes file claims under the Anticybersquatting Consumer Protection Act (ACPA).[146] ACPA authorizes civil claims against any person who, with "bad faith intent to profit," registers, traffics in, or uses a domain name that reflects the trademark or personal name of another.[147] Its remedies include domain-name transfer, domain-name cancellation, actual damages, treble damages, and statutory damages.[148] ACPA is not ideal for solving political-cybersquatting problems because: (1) litigation is too costly and slow for most candidates; (2) non-commercial cybersquatters may not have the requisite "bad faith intent to profit;" and (3) jurisdictional issues may prevent American courts from reaching foreign cybersquatters.[149] We turn instead to a remedial method that holds more promise for political-cybersquatting victims: ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP).[150]

ICANN intended UDRP to be "an administrative alternative dispute resolution policy [that] creates a procedure specifically designed to provide a fast and cheap means for resolving domain-name disputes."[151] It is available to complainants worldwide and promises global remedies.[152] UDRP suits candidates better than ACPA, but some features prevent it from reliably solving political-cybersquatting issues. Its distinctive procedures and substantive elements are explained below.

i. UDRP procedures are advantageous for political candidates, but . . .

UDRP's speed, price, and remedies make it an attractive option for resolving political cybersquatting disputes.

As intended, UDRP provides fast resolution to cybersquatting conflicts. From complaint submission to final remedy, the process takes an average of 47 days—much faster than litigation.[153] A complainant initiates the UDRP process[154] by filing a complaint with one of three ICANN-authorized UDRP providers—World Intellectual Property Organization (WIPO), National Arbitration Forum (NAF), and Asian Domain Name Resolution Centre (ADNDRC).[155] A complaint must provide the complainant's contact information, list the contested domain name(s), spec-

---

[144] An Australian cybersquatter hoped to trade Hillary 2008.com for a position within Senator Hillary Clinton's presidential campaign. *See* Friess, *As Candidates Mull '08, Web Sites Are Already Running*, *supra* note 121, at A15.
[145] Levinthal, *Master of Your Domain? supra* note 99, at 8A.
[146] Anticybersquatting Consumer Protection Act, Pub. L. No. 106-1131, 113 Stat. 1501 (1999). Other options include the Lanham Act and the Federal Trademark Dilution Act.
[147] 15 U.S.C. § 1125(d)(1).
[148] 15 U.S.C. § 1125(d)(1)(C).
[149] Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 420–421.
[150] Department of Commerce, The Anticybersquatting Consumer Protection Act of 1999 Section 3006 Concerning the Abusive Registration of Domain Names 8 (2000), *available at* <http://www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/repcongress.pdf>.
[151] American Girl, LLC v. Nameview, Inc. 381 F.Supp.2d 876 (E.D. Wis. 2005).
[152] Lipton, *Beyond Cybersquatting*, *supra* note 55, at 1372.
[153] Jay P. Kesan and Andres A. Gallo, *The Market for Private Dispute Resolution Services—An Empirical Re-Assessment of ICANN-UDRP Performance*, 11 Mich. Telecomm. Tech. L. Rev. 285, 342 (2005).
[154] For a clear diagram of the UDRP process, see *id.* at 303.
[155] ICANN, *Approved Providers for Uniform Domain-Name Dispute-Resolution Policy*, <http://www.icann.org/udrp/approved-providers.htm> (last visited Nov. 7, 2007). The International Institute for Conflict Prevention & Resolution (CPR) was a UDRP provider until January 1, 2007.

ify the sought-after remedies, and describe the complaint's grounds. Within three days of receipt, the provider reviews the complaint and forwards it to the respondent. The respondent need not receive actual notice of the complaint. A proceeding commences upon the respondent's actual notice or when the complaint is sent to the respondent via post, email, and fax. A response is due within 20 days after notice is *sent.* If a response is not submitted, the dispute is decided only on the basis of the complaint.[156] Once either 20 days elapse or a response is submitted, the provider forms a one- or three-member dispute-resolution panel within five days. Panels decide UDRP cases without discovery and oral arguments. The complaint and the response are the only source of factual information. Within 14 days of its formation, a panel sends its written decision to the provider, which then forwards the decision to the parties, to the appropriate registrars, and to ICANN within three days. A UDRP proceeding or final panel decision does not preclude the complainant or the respondent from filing an action in court. In fact, ICANN allows losing respondents a chance to file an "appeal" in court by waiting 10 days to implement a UDRP-panel decision.[157]

A proceeding's exact speed and procedure differs depending on the provider used. NAF resolves domain-name disputes slightly faster than the 47-day UDRP-wide average.[158] WIPO's processing speed is a little below par.[159] Additionally, NAF's policy toward additional submissions is noteworthy. NAF complainants and respondents may make an extra submission within five days of either the response or the complainant's additional submission by paying a $400 fee.[160] This procedure particularly suits complainants who cannot uncover enough respondent information to effectively anticipate counterarguments in their original complaints.

In addition to being fast, UDRP is cheap. Its "cost is [generally] much lower than the expected costs of resorting to court action to resolve [a] conflict."[161] A particular UDRP proceeding's exact costs depend on the provider, the number of domain names at issue, and other factors. They are likely to range from $1,000 to $7,000. UDRP offers complainants two principal remedies: cancellation and transfer.[162] A domain name is cancelled—made available to the general public for registration—in the unusual circumstance where neither the complainant nor the respondent can establish rightful ownership.[163] Domain-name ownership is more often transferred from the respondent to the complainant.[164] UDRP complainants in general have had success seizing domain names from cybersquatters. Critics suggest that UDRP is complainant-friendly because of providers' incentive to favor complainants in order to attract business.[165] This assertion has support. Two providers seen as relatively respondent-friendly, eResolutions and CPR, went out of business.[166] Decisions by the remaining providers' panels overwhelmingly favor complainants. Eighty-four percent

---

[156] Respondent "default" happens with regularity. According to 2002 statistics, 53 percent of all decisions were made without a response. UDRPinfo.com, *Outcome Data for Respondent Default Decisions* (2002), <http://www.udrpinfo.com/dcsn.php#data> (last visited Nov. 17, 2007).

[157] ICANN, Uniform Domain Name Dispute Resolution Policy (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[158] Jay P. Kesan and Andres A. Gallo, *The Market for Private Dispute Resolution Services—An Empirical Re-Assessment of ICANN-UDRP Performance*, 11 MICH. TELECOMM. TECH. L. REV. 285, 364 (2005).

[159] Jay P. Kesan and Andres A. Gallo, *The Market for Private Dispute Resolution Services—An Empirical Re-Assessment of ICANN-UDRP Performance*, 11 MICH. TELECOMM. TECH. L. REV. 285, 364 (2005).

[160] National Arbitration Forum, Dispute Resolution for Domain Names Supplemental Rules ¶ 7 (2007), *available at* <http://domain.adrforum.com/users/icann/resources/UDRPSuppRules20071101.pdf>.

[161] Kesan and Gallo, *The Market for Private Dispute Resolution Services*, *supra* note 153, at 317.

[162] Requests for other types of remedies are often denied. *See, e.g.*, Yahoo! Inc. v. Cupcakes, WIPO Arb. and Mediation Center D2000-0777 (2000), *available at* <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0777.html.

[163] *See, e.g.*, Kasuku Ltd. v. The Kikoy Co., CPR Institute for Dispute Resolution, CPR0504 (2005), *available at* <http://www.cpradr.org/ICANN/icanndecisioncpr0504-050505.pdf>.

[164] *See, e.g.*, CIT Group, Inc. v. SearchTerms and Modern, Ltd., WIPO Arb. and Mediation Center D2005-0921 (2005), *available at* <http://www.wipo.int/amc/en/domains/decisions/html/2005/d2005-0921.html>.

[165] Kesan and Gallo, *The Market for Private Dispute Resolution Services*, *supra* note 159, at 299–300.

[166] *See* Pamela Segal, *Attempts to Solve the UDRP's Trademark Holder Bias: A Problem that Remains Unsolved Despite the Introduction of New Top Level Domain Names*, 3 CARDOZO ONLINE J. CONF. RES. 1, 13 (2001).

of WIPO disputes,[167] 86 percent of NAF decisions,[168] and 88 percent of ADNDRC judgments result in a domain-name transfer.[169] Once a panel rules in favor of a complainant, ultimate enforcement of the remedy is perfect because ICANN holds the Internet's root and respondents agree to UDRP panels' jurisdiction when they first register a domain name.[170]

Procedurally, UDRP is an attractive option for political candidates with cybersquatting problems because of its speed, cost, and remedies. UDRP's 47-day procedure offers quick relief to candidates, who must often race to make web site arrangements well before Election Day. Its low-cost process appeals to all candidates, but particularly to cash-starved local- and state-level candidates. Also, UDRP's remedies are "precisely the kinds of remedies a politician will want in a political cybersquatting case."[171] Candidates presumably care much more about acquiring a contested domain name to disseminate their message than wringing money from a cybersquatter. UDRP's speed, cost, and remedies are even more appealing because UDRP does not foreclose other remedial methods like court action and negotiation.

ii. UDRP complaint elements are difficult for candidates to consistently satisfy.

While the UDRP is procedurally advantageous to candidates, its substantive requirements—particularly the requirement that candidates hold a trademark or service mark—make it difficult, and sometimes impossible, to wrest domain names from political cybersquatters. All complainants, including political candidates, must demonstrate all three of the following elements:

- One or more domain names is identical or confusingly similar to a trade or service mark in which the complainant has rights;
- Respondent has no rights or legitimate interests in the contested domain name(s); and
- Respondent registered the contested domain name(s) in bad faith.[172]

Precision and prediction as to these elements' meanings are somewhat difficult because UDRP decisions often do not apply *stare decisis*[173] and UDRP panelists sometimes employ erratic reasoning.[174] Moreover, UDRP introduces additional volatility by allowing panelists to resolve disputes based on "any rules and principles of law [they] deem[] applicable."[175] Bearing in mind potential uncertainty, these UDRP elements and their application to political cybersquatting are analyzed below.

---

[167] Press Release, World Intellectual Property Organization, *Cybersquatting Remains on the Rise with Further Risk to Trademarks from New Registration Practices* (Mar. 12, 2007), *available at* <http://www.wipo.int/pressroom/en/articles/2007/article_0014.html>.

[168] Calculated using NAF's Domain-Name Dispute Search Engine at <http://domains.adrforum.com/decision.aspx> on Nov. 15, 2007. Decisions that favored complainants numbered 6,500—including 6,439 transfers, 27 cancellations, and 32 split decisions where at least some contested domains were turned over to complainants. The total final decisions numbered 7,555, with 200 additional cases pending and 1,035 cases withdrawn.

[169] Calculated from ADNDRC's case listing at <http://www.adndrc.org/adndrc/hk_statistics.html>. Out of 169 final decisions, 148 favored of the complainants.

[170] Kevin Heller, *The Young Cybersquatter's Handbook: A Comparative Analysis of the ICANN Dispute*, 2 CARDOZO ONLINE J. CONFLICT RESOL. 2, 4 (2001).

[171] Jacqueline D. Lipton, *Who Owns Hillary.Com?*, *supra* note 2, at 92.

[172] ICANN, Rules for Uniform Domain Name Dispute Resolution Policy ¶ 3(b)(ix) (1999), *available at* <http://www.icann.org/dndr/udrp/uniform-rules.htm>. *See also* ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(a) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[173] R. Jonas Geissler, *For Sale Signs in Cyberspace: Whether Federal Rule of Evidence 408 Should be Adapted to the Uniform Dispute Resolution Policy for Internet Domain Names to Bar Evidence of Offers to Settle from Arbitration Proceedings*, 2002 B.C. INTELL. PROP. & TECH. F. 111801 (2002).

[174] Wayde Brooks, *Wrestling Over the World Wide Web: ICANN's Uniform Dispute Resolution Policy for Domain Name Disputes*, 22 HAMLINE J. PUB. L. & POL'Y 297, 323 (2001).

[175] ICANN, Rules for Uniform Domain Name Dispute Resolution Policy ¶ 15(a) (1999), *available at* <http://www.icann.org/dndr/udrp/uniform-rules.htm>. Some UDRP panels have attempted to cabin this potentially wide-ranging discretion. *See* Which? Ltd. v. James Halliday, Case No. D2000-0019 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0019.html> (holding that panels should apply substantive law from the respondent's jurisdiction). But other panels have disregarded attempts to limit panels' looks at "any rules and principles of law." *See generally*, Geissler, *supra* note 173.

aa. Identical or Confusingly Similar to a Mark in which the Complainant Has Rights

To prevail, a UDRP complainant must have rights in a trade or service mark and show the respondent's domain name is identical or confusingly similar to that mark.[176]

(1). Possessing rights in a mark.

Proving rights in a trademark or service mark is often political candidates' hardest hurdle to clear in the UDRP process.[177] Although UDRP primarily protects corporate names, candidates can show rights in phrases that predominately feature a personal name.[178] Occasionally, candidates have established rights through trademark registration.[179] But registration is not necessary to prevail in a UDRP case.[180] Personal names that qualify as unregistered or common-law marks "suffice to support a domain name complaint."[181] Candidates must prove the famous or distinctive "character of the mark or name on which their claim is based."[182] Candidates must also show that their personal name has attained a "secondary meaning"[183] as an identifier of goods or services.[184]

A number of complainants, including candidates, have established marks by using their personal names "to promote someone else's goods or services, or for direct commercial purposes in the marketing of [their] own goods and services."[185] The first-ever UDRP case involving a personal name found that British author Jeanette Winterson had common-law rights in her name because it was associated with book sales.[186] Celebrities like actress Julia Roberts,[187] football quarterback Dan Marino,[188] and singer Mick Jagger[189] were found to hold marks in their names under similar logic. Some candidates have also cited commercial, non-political uses of their personal names to establish marks. Former British Parliament Member Jeffrey Archer relied on his worldwide success as an author.[190] Similarly, the panelist for U.S. Senator Hillary Clinton's claim to Hillary

---

[176] ICANN, Rules for Uniform Domain Name Dispute Resolution Policy ¶ 3(b)(ix)(1) (1999), *available at* <http://www.icann.org/dndr/udrp/uniform-rules.htm>.

[177] Lipton, *Who Owns Hillary.Com?*, *supra* note 2, at 68–69.

[178] Department of Commerce, The Anticybersquatting Consumer Protection Act of 1999 Section 3006 Concerning the Abusive Registration of Domain Names 10 (2000), *available at* <http://www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/repcongress.pdf>; Belczyk, *Domain Names*, *supra* note 9, at 505–506.

[179] Bill Sizemore v. DIS, Inc., Case No. FA0312000221173 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/221173.htm>. *See also*, 2008 Democratic National Convention Committee, Inc. v. Fernstrom Inc., Case No. FA0703000933062 (Nat'l Arb. F. 2007), <http://domains.adrforum.com/domains/decisions/933062.htm>.

[180] Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>.

[181] *McCarthy on Trademarks and Unfair Competition*, § 25:74.2 (4th ed. 2002). *See also* British Broad. Corp. v. Renteria, Case No. D2000-0050 (WIPO Arb. and Mediation Center 2000).

[182] Monty and Pat Roberts, Inc. v. Bill Keith, Case No. D2000-0299 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0299.html>. *See also* Steven Rattner v. BuyThisDomainName, Case No. D2000-0402 (WIPO Arb. and Mediation Center 2000).

[183] *See* E.H. Schopler, *Doctrine of Secondary Meaning in the Law of Trademarks and Unfair Competition*, 150 A.L.R. 1067 (2008).

[184] Brown v. Julie Brown Club, Case No. D2000-1628 (WIPO Arb. and Mediation Center 2001), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1628.html>.

[185] Convergencia Democratica de Catalunya v. ar mas, Case No. DTV2003-0005 (WIPO Arb. and Mediation Center 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>.

[186] Jeanette Winterson v. Mark Hogarth, Case No. D2000-0235) (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0235.html>.

[187] Julia Fiona Roberts v. Russell Boyd, Case No. D2000-0210 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html>.

[188] Daniel Marino, Jr. v. Video Images Prods., et al., Case No. D2000-0598 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0598.html>.

[189] Mick Jagger v. Denny Hammerton, Case No. FA0007000095261 (Nat'l Arb. F. 2000), <http://domains.adrforum.com/domains/decisions/95261.htm>.

[190] Jeffrey Archer v. Alberta Hotrods, Case No. D2006-0431 (WIPO Arb. and Mediation Center 2006), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0431.html>.

Clinton.com noted her achievements as a best-selling author of four books.[191] Oregon politician Bill Sizemore emphasized use of his name in carpet sales and radio broadcasting as the basis for a mark.[192] Candidates active in business, book writing, songwriting, entertainment, and other commercial endeavors before and/or during their political careers may thus successfully establish a mark under UDRP. However, many candidates cannot make this type of showing, especially those who are not well-known or who avoid using their public fame for commercial activities.[193]

Past UDRP decisions leave open the question of whether candidates establish rights in their names through political activities that are largely non-commercial. Early cases favored candidates. Anne McLellan, a Canadian Member of Parliament and Attorney General used UDRP to seize a domain bearing her name. The panel ruled that McLellan:

> [E]stablished common law trademark rights in her name sufficient to support a complaint under the ICANN Policy. Anne McLellan is well known in Canada as the Member of Parliament for the federal riding of Edmonton West, and also as the Minister of Justice and Attorney General of Canada. She is the most senior Government of Canada official in the province of Alberta.[194]

McLellan showed a mark in her personal name strictly through her political activities. Likewise, then-gubernatorial candidate Mark Warner established a mark in his personal name solely due to his efforts as "a former candidate for the U.S. Senate and . . . presumptive candidate for Governor of the Commonwealth of Virginia in 2001."[195] This candidate-favorable climate changed considerably in 2001, when WIPO issued an ICANN-requested report that lengthily examined UDRP's protection of personal names. Notably, the report concluded:

> Persons who have gained eminence and respect, but who have not profited from their reputation in commerce, may not avail themselves of the UDRP to protect their personal names against parasitic registrations.[196]

While this passage seemingly precludes candidates whose names carry "no commercial value"[197] from establishing marks, post-WIPO-report cases have diverged along two separate lines of decisions.

One line of decisions has firmly held that UDRP only protects personal names that have been "commercially exploited."[198] Spanish political party Convergencia Democratica de Catalunya, for example, brought a UDRP claim on behalf of party leader Artur Mas. The party cited its extensive political activities using Mas' name, but the party's claim failed because Mas' name was "not [used] in commerce to distinguish goods or services."[199] New York State Senate candidate Virginia Fields said her election as the first African-American woman on the New York City Council and her candidacy for Mayor of New York—in all, 17 years of public service and political campaigns—entitled her to a mark in her personal name. But the UDRP panel rejected Fields' assertion because her name had never "been used or advertised as an indication of the source of any goods or

---

[191] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>.

[192] Bill Sizemore v. DIS, Inc., Case No. FA0312000221173 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/221173.htm>.

[193] *See, e.g.*, The Reverend Dr. Jerry Falwell and The Liberty Alliance v. Gary Cohn, Case No. D2002-0184 (WIPO Arb. and Mediation Center 2002), <http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0184.html>.

[194] Anne McLellan v. smartcanuk.com, Case No. AF-303 (eResolutions 2000), <http://www.disputes.org/decisions/0303.htm>.

[195] Mark Warner 2001 v. Mike Larson, Case No. FA0009000095746 (Nat'l Arb. F. 2000) <http://domains.adrforum.com/domains/decisions/95746.htm>.

[196] *See generally*, SECOND WIPO INTERNET DOMAIN NAME PROCESS, THE RECOGNITION OF RIGHTS AND THE USE OF NAMES IN THE INTERNET DOMAIN NAME SYSTEM ¶ 199 (2001), *available at* <http://www.wipo.int/amc/en/processes/process2/report/html/report.html>.

[197] Lipton, *Beyond Cybersquatting*, *supra* note 55, at 1425 (2005).

[198] Kathleen Kennedy Townsend v. B.G. Birt, Case No. D2002-0030 (WIPO Arb. and Mediation Center 2002), <http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0030.html>.

[199] Convergencia Democratica de Catalunya v. ar mas, Case No. DTV2003-0005 (WIPO Arb. and Mediation Center 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>.

services."[200] Kathleen Kennedy Townsend, John F. Kennedy's niece and Robert F. Kennedy's daughter, was the sitting Lieutenant Governor of Maryland and a prospective gubernatorial candidate when she was cybersquatted. Despite Townsend's obvious political fame and thorough campaign preparations, UDRP panels twice refused to recognize a mark in her personal name.[201] In sum, many panels appear unwilling to find that generic political activities establish a mark in a candidate's personal name. These decisions' *dicta* offer candidates some hope, however. Despite its ultimate conclusion, the *Fields* panel conceded that "there may be circumstances where a political figure uses his or her name in a manner that would establish trademark use."[202] The first *Townsend* decision specifically left open the possibility that use of a candidate's name in fundraising could show a mark.[203] And the second *Townsend* decision considered name uses in fundraising, Internet publicity, and campaign merchandizing before ultimately rejecting the claim for lack of standing.[204]

Other decisions have preserved earlier reasoning in *McLellan* and *Warner* by holding that candidates' generic, non-commercial political activities may establish marks. A panel found that Hillary Clinton's personal name was a mark due to "use and exposure of the mark in the marketplace *and* . . . [in] political activities, including a successful Senate campaign."[205] It specifically mentioned that Ms. Clinton is an "internationally known political figure who has received world-wide press coverage."[206] U.S. Congressman Ken Calvert was deemed to hold a mark in his personal name by virtue of his time as a federal officeholder and his previous use of a campaign web site.[207] One decision even held explicitly that U.S. Senate candidate Douglas Forrester's campaign fundraising established a mark in his personal name.[208] These decisions align closely with a series of U.S. federal court rulings.[209] Their willingness to disregard the 2001 WIPO report presumably flows from a belief that UDRP is overly "focused on the protection of *commercial* trademark interests."[210] This argument reasons that political cybersquatting is just as likely as conventional cybersquatting to misdirect web traffic and "diminish the goodwill associated with" well-known names.[211]

Aside from different doctrinal approaches to UDRP, other factors may explain this post-WIPO-report divergence. The table below summarizes all UDRP political-cybersquatting cases in reverse chronological order.

The UDRP provider is perhaps the most influential factor in explaining the divergence between the two lines of decisions. Of the dispute decisions that discussed mark establishment, *all* of NAF's post-WIPO-report decisions found

---

[200] Fields for Senate, v. Toddles, Inc., Case No. D2006-1510 (WIPO Arb. and Mediation Center 2007), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-1510.html>.

[201] Kathleen Kennedy Townsend v. B.G. Birt, Case No. D2002-0030 § 4 (WIPO Arb. and Mediation Center 2002), <http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0030.html>; Friends of Kathleen Kennedy Townsend v. Birt, Case No. D2002-0451 (WIPO Arb. and Mediation Center 2002), <http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0451.html>.

[202] Fields for Senate, v. Toddles, Inc., Case No. D2006-1510 (WIPO Arb. and Mediation Center 2007), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-1510.html>.

[203] Kathleen Kennedy Townsend v. B.G. Birt, Case No. D2002-0030 § 6 (WIPO Arb. and Mediation Center 2002), <http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0030.html>.

[204] Friends of Kathleen Kennedy Townsend v. Birt, Case No. D2002-0451 (WIPO Arb. and Mediation Center 2002), <http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0451.html>.

[205] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm> (emphasis added).

[206] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>.

[207] Kenneth Calvert v. Domain Strategy, Inc., Case No. FA0306000162075 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/162075.htm>.

[208] Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>.

[209] United We Stand America, Inc. v. United We Stand, America, New York, Inc., 128 F.3d 86, 90 (1997); Brach Van Houten Holding, Inc. v. Save Brach's Coalition for Chicago, 856 F.Supp. 472, 475–76 (N.D.Ill.1994); Partido Revolucionario Dominicano (PRD) Seccional Metropolitana de Washington-DC, Maryland y Virginia v. Partido Revolucionario Dominicano, Seccional de Maryland y Virginia, 312 F.Supp.2d 1 (D.D.C. 2004); National Rural Electric Cooperative Association v. National Agricultural Chemical Association, 26 U.S.P.Q. 2d 1294 (D.C.D.C. 1992).

[210] Jacqueline D. Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 WAKE FOREST L. REV. 1361, 1363 (2005) (emphasis added).

[211] Jefferson, *supra* note 83, at 2B.

TABLE 1. UDRP POLITICAL-CYBERSQUATTING CASES IN REVERSE CHRONOLOGICAL ORDER

Dispute	*Date*	*Provider*	*Response?*	*Complainant*	*Non-Political Activities Mentioned?*	*Political Activities Mentioned?*	*Mark Found?*
Mary Bono	6/18/2007	NAF	No*	Campaign	No	No	Yes
Democratic National Convention	4/10/2007	NAF	Yes	Convention Committee	No	No	Yes
Virginia Fields	3/14/2007	WIPO	Yes	Campaign	No	City Council, State Senate	No
Jeffrey Archer	6/1/2006	WIPO	No	Former Candidate	Author	No	Yes
Hillary Clinton	3/18/2005	NAF	No	Candidate	Author	First Lady, U.S. Senate	Yes
Bill Sizemore	2/26/2004	NAF	Yes	Candidate	Radio Show, Business	OR Governor	Yes
Artur Max	12/19/2003	WIPO	No	Party	No	Party Leader, Web site	No
Doug Forrester	9/3/2003	NAF	No	Candidate	No	U.S. Senate, Fundraising	Yes
Ken Calvert	8/1/2003	NAF	No	Candidate	No	U.S. House, Web site	Yes
Friends of Kathleen Townsend	7/31/2002	WIPO	Yes	Campaign	Famous Family	MD Lt. Governor, MD Governor, Fundraising, Merchandise	No
Kathleen Townsend	4/11/2002	WIPO	Yes	Candidate	Famous Family	MD Lt. Governor, MD Governor	No
Mark Warner	11/15/2000	NAF	Yes	Campaign	No	U.S. Senate, VA Governor	Yes
Anne McLellan	9/25/2000	eRes	No	Candidate	No	Canadian Parliament Member	Yes

*The Respondent in Mary Bono responded to ICANN through a series of emails and, in the process stipulated that he did not want to own "marybono.net" any longer. Mary Bono Committee v. Michael Grace, Case No. FA0705000990456 (Nat'l Arb. F. 2007). <http://domains.adrforum.com/domains/decisions/990456.htm>.

a mark based at least partially on political use. *None* of WIPO's panels reached the same conclusion. This is not surprising, as WIPO decisions rely heavily on the 2001 WIPO report and thus deny marks based on non-commercial use.[212] NAF decisions do not. Another important factor is the respondent's failure to respond. Where no response is submitted, a UDRP panel *may* choose to "view the Complaint in a light most favorable to [the] Complainant, and . . . accept all reasonable allegations and inferences in the Complaint as true."[213] As a result, unrebutted complaints often establish marks through political use.[214]

[212] Kathleen Kennedy Townsend v. B.G. Birt, Case No. D2002-0030 § 4 (WIPO Arb. and Mediation Center 2002), <http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0030.html>.

[213] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>. *See also* Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>; Kenneth Calvert v. Domain Strategy, Inc., Case No. FA0306000162075 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/162075.htm>.

[214] *But see* Convergencia Democratica de Catalunya v. ar mas, Case No. DTV2003-0005 (WIPO Arb. and Mediation Center 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>.

Even if some candidates can establish a mark through political activities, Federal Election Commission (FEC) rules significantly hamper political newcomers in U.S. federal campaigns. Rigorous financial disclosure requirements are triggered when an individual receives or spends $5,000 "seek[ing] nomination for election, or election, to federal office"[215]—precisely the type of activity a political newcomer would undertake to establish a mark in her personal name. Some candidates therefore face a dilemma: either comply with burdensome reporting requirements or fail to establish a mark in their personal names for UDRP purposes.

Demonstrating rights in a mark presents a high hurdle for all political candidates. But for some, it is an impassable obstruction to bringing a successful UDRP claim. UDRP, at best, provides an uncertain and incomplete solution to political cybersquatting.

(2). Identical or confusingly similar

Once a mark is established, candidates and other complainants typically have little difficulty proving that a contested domain name is identical or confusingly similar.[216] UDRP panels ignore TLDs and other technical domain-name components when considering whether a mark and a domain name are identical or confusingly similar.[217] UDRP panels have found domain names to be confusingly similar when they:

- Simply add generic or descriptive words like "direct," "online," "my," "i-," or "e-" to a mark ;[218]
- Attach the word "sucks" to the end of a mark;[219]
- Contain a one- or two-letter difference with a mark (a.k.a. typosquat);[220]
- Employ lettering that is phonetically similar to a mark;[221]
- Give an overall impression of similarity with a mark;[222] or
- Involve circumstances that implicate a sufficient number of so-called *Polaroid* factors (used in mainstream trademark disputes).[223]

Complainants may use these and other circumstances to prove that domain names are confusingly similar to marks.

bb. No Rights or Legitimate Interests in the Domain Name

After establishing that a contested domain name is identical or confusingly similar to her mark, a complainant must show the respondent has no rights or legitimate interests in the domain name.[224]

Complainants must gather evidence about respondents and contested domain names to make this showing. Complainants often search the WHOIS database—an online listing of each domain-name registrant's name, address, and technical information.[225] However, such a search is often complicated or impossible when

---

[215] 11 C.F.R. § 100.3(a).

[216] Anne Gilson LaLonde, *Litigation Alternatives: UDRP and Trademark Office Proceedings*, 904 PLI/PAT 561, 571 (2007).

[217] Hannover Ruckversicherungs-AG v. Ryu, Case No. FA0112000102724 (Nat'l Arb. F. 2002), <http://domains.adrforum.com/domains/decisions/102724.htm>; Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>.

[218] LaLonde, *Litigation Alternatives*, *supra* note 216, at 571.

[219] *See, e.g.*, Cabela's Inc. v. Cupcake Patrol, Case No. FA0006000085080 (Nat'l Arb. F. 2000), <http://domains.adrforum.com/domains/decisions/95080.htm>.

[220] *See, e.g.*, Playboy Enters. Int'l, Inc. v. Sand WebNames, Case No. D2001-0094 (WIPO Arb. and Mediation Center 2001), <http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0094.html>.

[221] *See, e.g.*, Microsoft Corp. v. MikeRushton, Case No. D2004-0123 (WIPO Arb. and Mediation Center 2004), <http://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0123.html>.

[222] *See, e.g.*, Guinness UUDV North America v. Ukjent, Case No. D2001-0684 (WIPO Arb. and Mediation Center 2001), <http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0684.html>.

[223] *Polaroid* factors include: (1) the strength of the complainant's mark; (2) the degree of similarity between complainant's mark and respondent's mark; (3) the proximity of the products or services; (4) the likelihood that the complainant will bridge the gap; (5) evidence of actual confusion; (6) respondent's good faith in adopting the mark; (7) the quality of respondent's product or service; and (8) the sophistication of buyers. *See, e.g.*, Zippo Manufacturing Co. v. Neatwork Communication, Case No. D2000-1128 (WIPO Arb. and Mediation Center 2001), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1128.html>. *See also* Polaroid Corp. v. Polarad Electronics Corp., 287 F.2d 492, 495 (2d Cir. 1961).

[224] ICANN, Rules for Uniform Domain Name Dispute Resolution Policy ¶ 3(b)(ix)(2) (1999), *available at* <http://www.icann.org/dndr/udrp/uniform-rules.htm>.

[225] Jeffrey J. Look, *Law and Order on the Wild, Wild West (WWW)*, 24 U. ARK. LITTLE ROCK L. REV. 817, 821 n. 22 (2002).

a respondent is registered anonymously.[226] Complainants may also document a web site's past uses by searching the Internet Archive's "Wayback Machine," which is a repository for past Internet content.[227]

Complainants can make a prima facie showing of respondents' lack of rights or legitimate interests in domain names by making three factual showings:

- Before receiving notice of a UDRP dispute, the respondent did not use or make demonstrable preparations to use the domain name in connection with a bona fide offering of goods or services;[228]
- The respondent has not been commonly known by the domain name;[229] and
- The respondent is not making a legitimate noncommercial or fair use of the domain name.[230]

If a complainant makes this prima facie demonstration, the burden of proof shifts to the respondent, who prevails only by disproving any one of the complainant's assertions.[231] By failing to respond, a respondent concedes a lack of rights or legitimate interests in the disputed domain name.[232]

Political candidates are situated similarly to other complainants in their ability to both show that respondents' domain-name use lacks a connection with goods and services and demonstrate that respondents are not commonly known by disputed domain names.[233] However, establishing that respondents are not making legitimate noncommercial or fair uses of domain names is somewhat more complicated for candidates because non-commercial cybersquatting—especially in the political context—raises "competing social interests to those of the trademark holder, usually in the free speech area."[234] UDRP panels take different approaches on whether respondents' "criticism" and "fan" sites are a legitimate non-commercial or fair use. Some panels look at the web site's use and typ-

---

[226] *See generally*, Jeffrey S. Sobek, *Balancing Individual Privacy Rights and the Rights of Trademark Owners in Access to the WhoIs*, 38 J. MARSHALL L. REV. 357 (2004). ICANN has implemented a new policy regarding completeness of WHOIS information that makes anonymous registration more difficult, however.

[227] Internet Archive, *Home Page*, <http://www.archive.org/index.php> (last visited Nov. 17, 2007).

[228] Complainants must prove that respondents did not use or demonstrably prepare to use domain names in connection with a bona fide offering of goods or services before receiving notice of a UDRP dispute. ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(c)(i) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>. The meaning of "bona fide offering of goods or services" is often contended in UDRP disputes. UDRP panels have said web sites do not offer bona fide goods or services when they feature hyperlinks to unrelated sites (Disney Enters., Inc. v. Dot Stop, Case No. FA0302000145227 Nat'l Arb. F. 2003, <http://domains.adrforum.com/domains/decisions/145227.htm>), redirect Internet users to commercial sites (Black & Decker Corp. v. Clinical Evaluations, Case No. FA0205000112629 Nat'l Arb. F. 2002, <http://domains.adrforum.com/domains/decisions/112629.htm>), offer generic search engines (Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 Nat'l Arb. F. 2005, <http://domains.adrforum.com/domains/decisions/414641.htm>), forward users to pornographic web sites (Kenneth Calvert v. Domain Strategy, Inc., Case No. FA0306000162075 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/162075.htm>), display multiple pop-up advertisements (Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 Nat'l Arb. F. 2005, <http://domains.adrforum.com/domains/decisions/414641.htm>), or present "public comment" opportunities (Mark Warner 2001 v. Mike Larson, Case No. FA0009000095746 Nat'l Arb. F. 2000, <http://domains.adrforum.com/domains/decisions/95746.htm>).

[229] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(c)(ii) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>. Showing that "nothing in Respondent's WHOIS information implies that Respondent is 'commonly known by' the disputed domain name" is generally enough. Tercent Inc. v. Yi, Case No. FA0301000139720 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/139720.htm>. Respondents cannot rebut complainants' assertions with "casual and unsubstantiated nicknames." LaLonde, *Litigation Alternatives*, *supra* note 216, at 574. Moreover, respondents must have "been commonly known by the domain name prior to registration." RMO, Inc. v. Andy Burbidge, Case No. FA0103000096949 (Nat'l Arb. F. 2001), <http://domains.adrforum.com/domains/decisions/96949.htm>.

[230] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(c)(iii) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[231] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>.

[232] Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>.

[233] *Infra* notes 295 and 296.

[234] Lipton, *Beyond Cybersquatting*, *supra* note 55, at 1403.

ically conclude that "the exercise of free speech for criticism and commentary . . . demonstrates a right or legitimate interest."[235] Others read the UDRP language more literally and examine the domain name's use. These decisions usually hold that "a right to free speech and a legitimate interest in criticizing . . . is a very different thing from having a right or legitimate interest" in a domain name identical to another's mark.[236] More forcefully, one panel noted: "Respondent's [non-commercial cybersquatting] is not the equivalent of exercising the right of free speech outside Complainant's business street address but of impermissibly blocking traffic to that street address."[237] In other words, Internet-user confusion far outweighs any nominal speech expressed through the domain name itself.[238] This logic has also been applied in the political context. DougForrester.com, namesake of U.S. Senate candidate Douglas Forrester, featured "an anti-abortion and anti-Planned Parenthood website" authored by a cybersquatter.[239] A UDRP panel concluded that, despite First Amendment interests, the cybersquatter's use of the domain was not "fair" because he exploited "the goodwill [Forrester] ha[d] built up around his name to redirect Internet users to its website which espouses a variety of opinions that are not endorsed by [Forrester]."[240]

cc. Domain Name Registered and/or Used in Bad Faith

A UDRP complaint's final element is met by showing that the respondent registered and/or used contested domain names in bad faith.[241] Bad faith is shown when the respondent:

- Acquired a domain name primarily to sell, rent, or otherwise transfer to the complainant or to the complainant's competitor for valuable consideration;
- Engaged in a pattern of cybersquatting;
- Registered the domain name primarily to disrupt a competitor's business; or
- Created a likelihood of confusion with the complainant's mark in an intentional effort to attract Internet users for commercial gain.[242]

UDRP panels have recognized additional signs of bad faith.[243] Political candidates and

---

[235] Bridgetsone-Firestone v Myers, Case No. D2000-0190 ¶ 6 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0190.html>; *See also* Springsteen v. Burgar, D2000-1532, § 4 (WIPO Arb. and Mediation Center 2001), <http://arbiter.wipo.int/domains/decisions/html/2000/d2000-1532.html>.

[236] Compagnie Generale des Matieres Nucleaires v. Greenpeace Int'l, Case No. D2001-0376 (WIPO Arb. and Mediation Center 2001), <http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0376.html>.

[237] Jenner & Block LLC v. Defaultdata.com, Case No. FA0207000117310 (Nat'l Arb. F. 2002), <http://domains.adrforum.com/domains/decisions/117310.htm>.

[238] Direct Line Group Ltd. v. Purge I.T., Case No. D2000-0583 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0583.html>. *See also* Name.Space Inc. v. Network Solutions, 202 F.3d 573, 585 (2d Cir. 2000).

[239] Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>.

[240] Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>.

[241] UDRP panels often refer to ACPA cases for their cues on bad faith. For a brief but helpful review of ACPA's bad faith elements, *see* Joseph J. Weissman, *The Anticybersquatting Consumer Protection Act: Developments Through Its First Six Years*, 95 TRADEMARK REP. 1058 (2005).

[242] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(b) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[243] Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>. Previous panels have found bad faith from actions not specifically listed in UDRP, including: (1) Holding a domain name passively, *see, e.g.*, Full Sail, Inc. v. Ryan Spevack, Case No. D2003-0502 (WIPO Arb. and Mediation Center 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0502.html>; (2) Registering a domain name with actual or constructive knowledge of a mark reflected in the domain name, *see, e.g.*, Exxon Mobil Corp. v. Fisher, Case No. D2000-1412 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1412.html>; (3) Registering a domain "immediately after a widely covered event," *see, e.g.*, Douglas Forrester v. Chris Hoffman, Case No. FA0307000170644 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/170644.htm>; (4) Taking advantage of another's failure to renew a domain name, *see, e.g.*, June Bug Enterprises v. Kyamko, Case No. FA0409000337694 (Nat'l Arb. F. 2001), <http://domains.adrforum.com/domains/decisions/337694.htm>; (5) Creating "an illicit association between the adult oriented con-

other complainants are equally able to satisfy this UDRP-complaint element.

(1). Selling, renting, transferring

Complainants may prove bad faith if respondents acquire domain names primarily to sell, rent, or otherwise transfer to the complainant or to the complainant's competitor for valuable consideration exceeding out-of-pocket costs.[244]

Respondents' offers to sell domains to complainants may prove primary intent to sell, rent, or otherwise transfer.[245] One important issue in offering such proof is whether a panel applies U.S. Federal Rule of Evidence 408,[246] which states that offers of "valuable consideration in compromising or attempting to compromise [a] claim" are not admissible.[247] Applying Rule 408 prevents complainants from "bait[ing] domain name registrants . . . into 'negotiations' aimed primarily at conjuring up evidence to be used in a UDRP proceeding."[248]At least one panel refused to admit a respondent's sale offer because it was "made in the context of negotiations aimed at settling the parties' on-going domain name dispute."[249] Many have expressly rejected Rule 408's application in UDRP because it makes evidence-gathering more difficult for complainants, thereby emboldening cybersquatters.[250] Still other panels have reserved the right to apply Rule 408, but look at respondents' offers to sell on a case-by-case basis.[251] Despite these differences, panels agree that complainants may not use sale offers as evidence of bad faith after "baiting" a respondent.[252] Former Virginia Governor Mark Warner's UDRP claim, for example, ultimately failed for lack of bad faith because the respondent made an offer to sell only after Warner "requested an offer."[253]

Past panels have inferred a respondent's intent to sell, rent, or otherwise transfer a domain from a variety of circumstances, including respondents':

- Linking a domain name to a "for sale" notice;[254]
- Submitting "for sale" in place of WHOIS-database contact information;[255]

---

tent on Respondent's web site and Complainant's mark," *see* Kenneth Calvert v. Domain Strategy, Inc., Case No. FA0306000162075 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/162075.htm>; (6) Imitating a mark holder, *see, e.g.*, Bill Sizemore v. DIS, Inc., Case No. FA0312000221173 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/221173.htm>; (7) Providing false contact information to the WHOIS database; *see, e.g.*, Convergencia Democratica de Catalunya v. ar mas, Case No. DTV2003-0005 (WIPO Arb. and Mediation Center 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>; (8) Neglecting to conduct a trademark search before registering a domain name, *see* Kate Spade LLC v. Darmstadter Designs, Case No. D2001-1384 (WIPO Arbitration and Mediation Center 2001), <http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-1384.html>; (9) Copying portions of a complainant's web site, *see* U.S. Office of Pers. Mgmt. v. MS Tech. Inc., Case No. FA0310000198898 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/198898.htm>; (10) Failing to put forward a logical explanation for use of another's mark in a domain name, *zss* Am. Red Cross v. Habersham, Case No. FA103926 (Nat'l Arb. F. 2002), <http://domains.adrforum.com/domains/decisions/103926.htm>. Complainants may freely use unique fact patterns that arise to show evidence of bad faith, as the list above is not exclusive.

[244] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(b)(i) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[245] *See, e.g.*, The Salvation Army v. Info-Bahn, Inc., Case No. D2001-0463 (WIPO Arb. and Mediation Center 2001), <http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0463.html>.

[246] For an in-depth discussion on this topic, *see* Geissler, *For Sale Signs in Cyberspace*, *supra* note 173.

[247] Fed. R. Evid. 408(a)(1) (2007).

[248] Netvault Ltd. v. SV Computers and Sunil Walia, Case No. D2000-0095 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0095.html> (DeCicco dissenting).

[249] LifePlan v. Life Plan, Case No. FA0005000094826 (Nat'l Arb. F. 2000), <http://domains.adrforum.com/domains/decisions/94826.htm>.

[250] *See, e.g.*, CBS Broadcasting, Inc. v. Saidi, Case No. D2000-0243 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0243.html>.

[252] Penguin Books, Ltd. v. Katz Family, Case No. D2000-0204 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0204.html>.

[252] Geissler, *supra* note 173.

[253] Mark Warner 2001 v. Mike Larson, Case No. FA0009000095746 (Nat'l Arb. F. 2000), <http://domains.adrforum.com/domains/decisions/95746.htm>.

[254] *See, e.g.*, Federated Western Properties, Inc. v. Mr. Faton Brezica, Case No. D2002-0083 (WIPO Arb. and Mediation Center 2002), <http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0083.html>.

[255] *See, e.g.*, America Online, Inc. v. QTR Corp., Case No. FA0001000092016 (Nat'l Arb. F. 2000), <http://domains.adrforum.com/domains/decisions/92016.htm>.

- Placing a web-traffic counter on an otherwise blank web site;[256] and
- Listing a domain name with an auction service.[257]

The "valuable consideration" sought by respondents need not be monetary. A panel found bad faith, for example, when a cybersquatter offered Metallica.org in return for dinner with members of the heavy-metal band Metallica.[258] This precedent may be particularly useful to combat cybersquatters who try to parlay their small domain-name investment into an opportunity to gain access to a political candidate.

(2). Pattern of cybersquatting

Complainants may show a respondent's bad faith by pointing to a pattern of registering domain names "in order to prevent the owner of [a] trademark or service mark from reflecting the mark in a corresponding domain name."[259] This may be simple if the respondent is an infamous and active cybersquatter.[260] A pattern may be less visible with little-known cybersquatters, but commercial services like Mark Monitor provide complainants with a method to catalogue respondents' domain-name portfolios.[261] Some panels "have not taken the 'pattern' requirement very seriously."[262] One panel, for example, found a "pattern" existed where a respondent with no cybersquatting history simultaneously registered MethodistUrology.com, MethodistUrology.net, and MethodistUrology.org.[263]

(3). Disrupting competitor's business

Complainants may prove a respondent's bad faith by showing that a domain name was registered "primarily for the purpose of disrupting" a competitor's business.[264] One panel held that a cybersquatter's registration of DieboldElections.com and DieboldVote.com showed bad faith because the cybersquatter was an engineer at Sequoia Voting Systems, a competitor to voting-machine manufacturer Diebold.[265] At least one panel has interpreted "competitor" to include all "who act[] in opposition to another," even outside of the commercial context.[266] This may open the door for political candidates who wish to take back a domain name from their cybersquatting opponents.

(4). Using confusion to intentionally attract users for commercial gain

Complainants may establish bad faith by showing that respondents created a likelihood of confusion with the complainant's mark in an intentional effort to attract Internet users for commercial gain.[267] Typosquatting is usually conclusive proof.[268] Web sites that expose users

---

[256] *See, e.g.*, Home Interiors & Gifts, Inc. v. Home Interiors, Case No. D2000-0010 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0010.html>.

[257] *See, e.g.*, AT&T Corp. v. rnetworld, Case No. D2006-0569 (WIPO Arb. and Mediation Center 2006), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0569.html>.

[258] Metallica v. Schneider, Case No. FA0009000095636 (Nat'l Arb. F. 2000), <http://domains.adrforum.com/domains/decisions/95636.htm>.

[259] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(b)(ii) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[260] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>.

[261] MarkMonitor, *Intellectual Property and Trademark Protection*, <http://www.markmonitor.com/solutions/brand protection/> (last visited Nov. 18, 2007).

[262] Anne Gilson LaLonde, *Litigation Alternatives: UDRP and Trademark Office Proceedings*, 904 PLI/PAT 561, 576 (2007).

[263] Methodist Urology LLC v. Urology of Indiana, Case No. FA0008000095609 (Nat'l Arb. F. 2000), <http://domains.adrforum.com/domains/decisions/95609.htm>.

[264] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(b)(iii) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[265] Diebold, Inc. v. Paul Terwilliger, Case No. D2003-0416 (WIPO Arb. and Mediation Center 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0416.html>.

[266] Mission KwaSizabantu v. Benjamin Rost, Case No. D2000-0279 (WIPO Arb. and Mediation Center 2000), <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0279.html>.

[267] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(b)(iv) (1999), *available at* <http://www.icann.org/dndr/udrp/policy.htm>.

[268] *See, e.g.*, Amazon.com, Inc. v. Newman, Case No. D2006-0517 (WIPO Arb. and Mediation Center 2006), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0517.html>. <http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0582.html>.

to pay-per-click search engines,[269] pop-up ads,[270] commercial hyperlinks,[271] and purchase opportunities[272] are all sufficiently "commercial" to indicate bad faith.

IV. ICANN SHOULD CREATE ".POL" AS A NEW TLD TO MITIGATE THE HARMS OF POLITICAL CYBERSQUATTING

Political candidates are uniquely damaged by cybersquatting for several reasons.[273] First, the Internet is singularly important to modern outreach-intensive operations like election campaigns. Second, the time-sensitive and divisive nature of elections means that candidates are attractive cybersquatting targets. Third, candidates cannot rely on standard preventive and remedial measures like UDRP to avoid and solve their cybersquatting problems. Because political cybersquatting is a distinct problem, it demands a distinct solution. This section briefly reviews past reform proposals and suggests the creation of ".pol," a new special-use TLD, as a measure to mitigate harms that result from political cybersquatting.[274]

A. Past proposals

Past proposals for solving political cybersquatting problems include those that favor national legislation and those that prefer UDRP reforms.

Some reformers favor national laws based on ACPA that specifically prohibit political cybersquatting in both commercial and non-commercial instances.[275] Others point to California's "Political Cyberfraud" law as an attractive model for nationwide legislation because it broadly prohibits the denial of access to a political web site.[276] However, jurisdictional limitations prevent national laws from addressing political-cybersquatting problems that originate from outside of national borders.[277] Cybersquatters and cybersquatting targets are spread across the world. A global problem needs a global solution.

Many prefer changes to UDRP that would protect personal names, including political candidates' names. These proposals avoid national laws' jurisdictional problems, but leave other challenges for political candidates. Tamarah Belcyzk, for example, has suggested that UDRP panelists simply "develop flexible guidelines that can adequately address the diverse interests at issue when personal names are involved in domain-name disputes."[278] This ad hoc method is attractive and is already occurring to some extent, but, as we have seen, a case-by-case UDRP system cannot offer a process to which political candidates can dependably turn to solve their cybersquatting problems. It could also muddy trademark law's application to non-political UDRP claims. Jacqueline Lipton, on the other hand, would revise UDRP to formally protect political candidates' names.[279] But this too may suffer from considerable uncertainty because, unlike trademark law, there is little global consensus on personal names' protection.[280] And to the extent that this formal change causes panels to consistently favor

---

[269] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>.

[270] Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com, Case No. FA0502000414641 (Nat'l Arb. F. 2005), <http://domains.adrforum.com/domains/decisions/414641.htm>.

[271] Disney Enters., Inc. v. Dot Stop, Case No. FA0302000145227 (Nat'l Arb. F. 2003), <http://domains.adrforum.com/domains/decisions/145227.htm>.

[272] G.D. Searle & Co. v. Celebrex Drugstore, Case No. FA0208000123933 (Nat'l Arb. F. 2002), <http://domains.adrforum.com/domains/decisions/123933.htm>.

[273] More precisely, political campaigns are uniquely harmed. Although this article has discussed candidates, much if not all of what has been said is equally applicable to ballot measure campaigns, which would be eligible for the proposed ".pol" TLD.

[274] A ".pol" TLD should not be confused with Poland's country-coded TLD, ".pl."

[275] Coleman, *Domain Name Piracy and Privacy*, *supra* note 72, at 257–262.

[276] Denise Pereira, *Chapter 277: California's Solution to Cyberfraud in the Political Arena*, 35 McGeorge L. Rev. 399 (2004).

[277] Magier, *Tick, Tock, Time is Running Out to Nab Cybersquatters*, *supra* note 5, at 420–421.

[278] Belczyk, *Domain Names*, *supra* note 9, at 506.

[279] Lipton, *Who Owns Hillary.Com? supra* note 2.

[280] Second WIPO Internet Domain Name Process, The Recognition of Rights and the Use of Names in the Internet Domain Name System ¶ 201 (2001), *available at* <http://www.wipo.int/amc/en/processes/process2/report/html/report.html>.

candidates, it is not apparent they *should* favor candidates when domain conflicts arise with those who are not cybersquatters.[281] Tinkering with UDRP's substantive elements will not adequately solve the political cybersquatting problem.

B. New ".pol" TLD for political candidates and entities

ICANN recently introduced several special-use generic TLDs, including ".aero" for the aerospace industry, ".museum" for museums, and ".pro" for professionals.[282] It should create another special-use generic TLD, ".pol," for candidates and other political entities.[283] Only current and prospective political candidates and entities would register ".pol" domains, just as ".gov" is only available to U.S. government agencies and ".edu" is only offered to educational institutions.[284] Following ICANN's existing model for special-use TLDs, a designated private international organization[285] that represents political candidates and entities would communicate with potential stakeholders to formulate ".pol" policies and registration requirements.[286] It would ensure that ".pol" sites are both used primarily for political activities and registered only by political groups with credible claims to particular domains. It would also establish and administer a ".pol"-specific process similar to UDRP for resolving disputes between competing claims in the same ".pol" domain.[287]

A ".pol" TLD would not stop political cybersquatting altogether. But a TLD reserved exclusively for political candidates and entities is needed for several reasons. First, it would mitigate the most serious problems caused by political cybersquatting. Cybersquatters could not register ".pol" domains to exploit candidates' public reputations. Candidates could timely and dependably access and control at least one domain from which to reach voters. Internet users could easily locate candidate domains because ".pol" provides a reliable shortcut for finding and identifying official web sites. So even if, as was the case in 2008, imitator sites house official-looking contribution web pages on ".com" sites, informed Internet donors can visit ".pol" sites for assurances that their money will go to an intended campaign recipient.

Second, it would reduce cybersquatters' economic incentive to purchase candidates' domains under ".com," ".net," ".org," ".mobi," and other TLDs outside of ".pol." Candidates' easy access to ".pol" domains will undermine the price for which cybersquatters can ransom non-".pol" domains to candidates. Decreased web traffic to non-".pol" candidate domains will also reduce non-".pol" sites' value to commercial and non-commercial cybersquatters hoping to divert Internet users.

Third, designating a specific and separate TLD for political candidates and entities would improve the Internet's functionality and organization. Past candidate web sites hosted under ".com," ".net," and ".org" TLDs have left Internet users to guess the correct TLD and

---

[281] Lipton's solution in such cases is to temporarily cede the contested domain to the political candidate. Although this remedy would be less harsh than permanent transfer, there seems to be little justification for favoring candidates over other legitimate domain holders, even temporarily. *See* Lipton, *Beyond Cybersquatting*, *supra* note 55, at 1433–1434.

[282] ICANN, *Top-Level Domains (TLDs)*, <http://www.icann.org/tlds/>.

[283] This ".pol" proposal is based on a previous U.S. congressional proposal to create a new second-level domain under the ".us" country-coded TLD for official federal, state, and local campaign sites. Its application is much broader than the ".us" plan, however, because political candidates and entities around the world could register a ".pol" domain name. *See* Trademark Cyberpiracy Prevention Act § 6 (1999) (H.R. 3028).

[284] A registrant would, for example, certify that she is a political officeholder, candidate, or prospective candidate, or that it is a political party, committee, or other political organization. To avoid abuse of the "prospective candidate" category, the ".pol" sponsoring organization could require that certain preparatory benchmarks are met before registration (i.e., potential candidacy mentioned in a news report, etc.).

[285] Perhaps ICANN's Government Advisory Committee could directly administer the ".pol" TLD or spin off a group to do so.

[286] *See* ICANN, *sTLD Information Page*, <http://www.icann.org/tlds/stld-apps-19mar04/> (last visited Nov. 19, 2007).

[287] Commenters on WIPO's 2001 Report on domain names suggested a similar reform for personal names generally. *See* SECOND WIPO INTERNET DOMAIN NAME PROCESS, THE RECOGNITION OF RIGHTS AND THE USE OF NAMES IN THE INTERNET DOMAIN NAME SYSTEM ¶ 198(iii) (2001), *available at* <http://www.wipo.int/amc/en/processes/process2/report/html/report.html>.

have required candidates to purchase domains under all possible TLDs.[288] A ".pol" TLD will eliminate Internet-user uncertainty about a web address' TLD portion and allow candidates to purchase only ".pol" domains. Moreover, political-candidate sites do not squarely fit within existing TLD categories like ".com" and ".org."[289] Educational institutions, air carriers, and museums may all register specialized TLDs. Political organizations are just as distinctive as these entities and are deserving of their own specialized TLD.

Fourth, as a bonus, the ".pol" TLD would provide an amicable solution for politically related domain conflicts that are not caused by cybersquatters. Brewers of Samuel Adams beer and Samuel Adams the mayoral candidate, for example, would no longer need to fight over ".com" domains. The brewers could use SamuelAdams.com and the candidate could take SamuelAdams.pol.[290]

The proposed ".pol" TLD will avoid the past reform proposals' problems described above. It is unhampered by the jurisdictional shortcomings of national legislation. Unlike formally altering UDRP to protect political names, arbitration panels could develop a coherent and consistent policy that protects political names in the limited ".pol" context, without causing confusion over trademark law's application in non-political UDRP cases or running roughshod over other interests.

Some may object to a ".pol" TLD. Cybersquatters would undoubtedly complain that ".pol" prevents them from exercising their commercial and free-speech rights. This is true to an extent, but the countervailing interests of preventing confusion, fraud, and reputation exploitation in the political context demand *some* reform measure that combats political cybersquatting. Blocking political cybersquatters from only one TLD is a relatively non-invasive way of solving an important problem, especially since that TLD is not currently available anyway. Cybersquatters will not lose anything but the opportunity to exploit bona fide political campaigns in an entirely new area of the Internet. A ".pol" TLD would infringe less upon whatever rights cybersquatters hold than proposed alternatives like national legislation and UDRP revisions, because it preserves all other TLDs for unrestricted free-speech use. And ".pol" would not violate cybersquatters' rights any more than other newly created TLDs, such as ".aero" and ".museum." Others may say that identifying legitimate political candidates and entities would be too difficult, particularly given the world's wide variety of governmental systems. This would undoubtedly be a difficult task, requiring the ".pol" sponsoring organization to both exercise due care in formulating and maintaining ".pol" registration criteria and consult a wide constituency of governments, NGOs, and other political actors. There is a risk of some legitimate political candidates and entities being excluded from ".pol" registration. Arbitrary exclusion is an inherent problem with "line drawing." But even if a small minority of politicians is left out, ".pol" makes domain names accessible to a vast number of candidates and entities; hence, ".pol" would be a significant step forward in combating political cybersquatting regardless of the particular eligibility criteria settled upon by the sponsoring organization and the relevant stakeholders.

A specialized ".pol" TLD is thus a workable solution to political-cybersquatting problems and other political domain-name conflicts that can avoid past proposals' shortcomings. Political leaders—particularly American officials, who have special leverage because of the United States's historically close relationship with ICANN—should pressure ICANN to create a ".pol" TLD as soon as possible.

V. CONCLUSION

Political cybersquatting is a problem for candidates worldwide as they run for offices at all levels of government. It hinders candidates' ability to perform essential campaign functions. It occurs often, precisely because candi-

---

[288] *See* Levinthal, *Master of Your Domain? supra* note 99, at 8A.

[289] *See* Oram, *Will the Real Candidate Please Stand Up?, supra* note 107, at 472.

[290] KPTV Blog, *Brewer, Ore. Candidate Bump Heads Over Campaign Site* (Oct. 26, 2007, 9:34 PDT), *available at* <http://www.kptv.com/news/14431394/detail.html?taf=ptl1>.

dates are easy targets operating in a contentious environment. But despite candidates' sustained damage and unique vulnerabilities, current measures have failed to prevent or remedy political cybersquatting. ACPA and various nationwide solutions, for example, are hampered by jurisdictional and other problems. UDRP too heavily emphasizes trademark possession to offer a reliable remedy for candidates. Rather than revised national legislation or UDRP processes, a desirable solution is a TLD reserved exclusively for political candidates and entities. Problems associated with political cybersquatting—confusion, fraud, and reputation exploitation, to name a few—can be mitigated if candidates and voters have a guaranteed space to raise funds, organize, and communicate. ICANN should immediately introduce ".pol" to mitigate political cybersquatting's harms and preserve the Internet as a useful medium for real-world democracy.

Address reprint requests to:
Matthew T. Sanderson
Capin & Drysdale, Chartered
One Thomas Circle, NW
Suite 1100
Washington, D.C. 2005–5802

E-mail: MTS@Capdale.com