Domain Name Piracy and Privacy: Do Federal Election Regulations Offer a Solution?

Matthew Coleman†

No one cares if you plant an election poster in your front yard. But if you do the same on your Web site, you might be required to file financial disclosure forms with the Federal Election Commission.1

INTRODUCTION

From e-commerce to online games to live streaming video, the Internet has arrived. A global audience has access to an “indescribable wealth of information,” all available via a telephone line and a personal computer.2 Like many other activities once conducted exclusively in the offline world, political campaigns are beginning to make use of the Net.3 Given that nearly half of the adults in the United States have access to the Internet,4 it is not surprising that political candidates have developed campaign technologies and methods to exploit this new medium.

However, the candidates themselves are not the only politically active citizens to make use of the World Wide Web. Like their counterparts in the commercial realm, political “cybersquatters” and “domain name pirates”5 have been quick to purchase potentially valuable domain names6 that are intuitively linked to candidates and their campaigns. These online squatters and pirates then either offer to sell the Internet address at a substantial premium above cost, or they post embarrassing material on the site. Such material may consist

† Associate, Cravath, Swaine & Moore, New York. B.A., Wake Forest University, 1997; J.D., Yale Law School, 2000. I would like to thank Ian Ayres for his invaluable guidance and mentoring. Monica Coleman provided helpful comments and suggestions.

3. See Howard Fineman, Pressing the Flesh Online, NEWSWEEK, Sept. 20, 1999, at 50 (“In the ever-accelerating world of the Internet, e-campaigning has gone from a novelty to a necessity in less than a year.”).
5. Throughout this Note, I will use the term “cybersquatter” to refer to someone who purchases a potentially valuable Internet address in the hope of selling it for an inflated price. I will use “domain name pirate” to denote a group or individual who purchases a domain name for the purpose of posting a parody of the candidate or company to which the site is intuitively linked.
6. A domain name is simply a World Wide Web address, such as www.yale.edu or www.ibm.com.
of a parody of the candidate and his positions, or it may involve more extreme content, such as pornographic images.\footnote{In the commercial context, Gateway Computer Co. paid $100,000 to a person who bought the rights to www.gateway2000.com and posted pornography on the site. Jessica Lee, \textit{Bill Would Protect Trademarks, Names from Cybersquatters}, USA TODAY, Aug. 3, 1999, at 8A.} These postings, at a minimum, disparage the candidate and his campaign,\footnote{A Web site parodying the George W. Bush presidential campaign includes a mock initiative dubbed "Amnesty 2000," which suggests that if elected president, Bush would pardon those convicted of drug offenses if they have "grown up." See Wayne Slater, \textit{Bush Criticizes Web Site As Malicious; Owner Calls It a Parody of White House Bid}, DALLAS MORNING NEWS, May 22, 1999, at A29.} and they may act to induce the candidate to purchase the address for an exorbitant price. However, even in the absence of damaging content, a candidate may still be willing to pay big money for sites logically linked to his or her name. For instance, Chris Hayden, an enterprising Californian, purchased www.hillary2000.com and www.clinton2000.com and listed them with an online broker for the steep price of $15,000 each. Hayden himself paid $70 for each of the sites.\footnote{Andrew J. Glass, \textit{Internet Domain Names Become a Pain for Public Figures}, ATLANTA JOURNAL-CONSTITUTION, Aug. 22, 1999, at A11. Glass also reports that Zack Exley offered to sell www.gwbush.com for the handsome sum of $380,000 and that www.presidenthatch.com had an asking price of $45,000. \textit{Id.}}

The George W. Bush presidential campaign experienced even greater problems in dealing with twenty-something graduate student Zack Exley, who purchased sites such as www.gwbush.com and www.gbush.org. Exley vexed the Bush camp with his anti-Bush postings and the vast amount of press he received, prompting Bush officials to file a complaint with the Federal Election Commission (FEC).\footnote{The Bush complaint was filed with the Federal Election Commission on May 3, 1999. See Paul Kedrosky, \textit{Bush-League Cybersquatters Threaten the Web: Hijacking of G.W. Bush Web Domains Shows Downside of Net Freedom, NAT'L POST, May 31, 1999, at C5.} In April 2000, more than eleven months after the filing, FEC commissioners determined that the Bush complaint did not warrant consideration and dismissed it without considering the merits. Exley was thus left free to continue his activities without fear of running afoul of federal election regulations.\footnote{See Will Rodger, \textit{Election Officials Weigh Legality of Net Campaigning}, INTERACTIVE WEEK FROM ZD WIRE, June 30, 2000 ("[T]he commission waited more than 11 months before delivering the nonverdict: The Bush complaint was too far down on the commission's list of priorities to address.").} Nevertheless, the Exley controversy has raised difficult issues that are likely to resurface as cyber-politics become more prevalent and more necessary for electoral success.

In the complaint, Bush lawyers first argued that Exley should have had to register as a political action committee (PAC) because he expended more than $1,000 in connection with a federal election.\footnote{[A]ny committee, club, association, or other group of persons which ... makes expenditures aggregating in excess of $1,000 during a calendar year is a political committee." 11 C.F.R. § 100.3(a) (2000).} Classification as a PAC would have required Exley to adhere to the extensive disclosure and reporting requirements of the political committee regulatory regime. Alternatively, Bush officials contended that Exley should have been required to file reports with
the FEC because he is an individual who makes yearly independent expenditures of more than $250 in connection with a federal election.13 A point of contention involved the set expenditure amounts that trigger both the PAC rules and the independent expenditure regulations. Exley maintained that his Web sites are virtually cost free, while Bush lawyers argued that the cost of the computer hardware used in the Web page production should be included in the cost of the sites, thus pushing Exley over the respective thresholds.14

Filing a formal complaint with the federal government was not the only combative action the Bush campaign was forced to take against Exley. Like many other candidates and corporations who have fallen victim to cyber-piracy, Bush officials found it prudent to make preemptive purchases of Bush-related domain names in an effort to preserve the integrity of the campaign's online presence. After the Exley escapade was well under way, the Bush campaign bought up over 260 domain names, including www.bushblows.com and www.bushsux.org.15 Needless to say, such purchases made good material for the anti-Bush crowd, adding yet another incentive for the likes of Zack Exley to continue their cyber-harassment.16 Furthermore, Bush was forced to think ahead to who his potential vice-presidential running mate might be and purchase those domain names as well. According to newspaper reports, months before the nomination was his, Bush purchased www.bushwhitman.com and www.bushwhitman.net, among other sites,17 thereby publicly tipping his hand with regard to at least some of his vice presidential possibilities.

Although preemptive purchasing entails many inconveniences, its most damaging consequence results from the fact that the domain name registry is public. Anyone can determine the owner of a particular address by going to the online directory maintained by Network Solutions, Inc. and using their free search engine.18 A consequence of this system is that cyber-piracy can lead to serious cyber-privacy issues, particularly for political candidates who need to
be able to ponder strategic moves outside of the public view. Unfortunately, for candidates seeking protection on the privacy front, federal election law has nothing to say on the issue.

This Note will examine whether federal election regulations address any of the problems raised when forward-looking and unscrupulous individuals purchase the rights to potentially valuable Internet addresses. Part I will provide context for the problem by exploring the role of the Internet in the modern political campaign. It will set forth empirical data from the 1998 congressional elections and will examine the future of online campaigning.

Part II will focus on the problem of domain name piracy by considering problems that have arisen in both the political and commercial spheres as a result of the first-come, first-served method of domain name registration. This section will explore the history of domain name registration, as well as the dispute resolution procedures that have evolved to address the problem of competing claims to a common Internet address. Additionally, it will analyze the Anticybersquatting Consumer Protection Act, which was passed by Congress as part of the year 2000 budget bill and applies intellectual property principles in an effort to stop domain name hijacking in the commercial context.

Part III of the paper will evaluate the claims raised in the Bush complaint and explore whether federal election regulations might offer a solution to the problem of domain name theft. It concludes that a person who posts a campaign parody at a potentially misleading Internet address is unlikely to fall within the definition of a political committee and is subject at most to the reporting requirements for persons making large independent expenditures. An "independent expenditure," by definition, is an expenditure for communication expressly advocating the election or defeat of a candidate. Therefore, this disclosure regime may be inadequate to stop domain name piracy, given that parodists can easily craft their sites to avoid express advocacy. Additionally, even if persons such as Zack Exley fall within the federal disclosure regime because of computer hardware cost allocation, mere disclosure offers no real solution to the underlying problem of the fraudulent use of misleading domain names.

Part IV concludes that a statutory measure analogous to the Anticybersquatting Consumer Protection Act is a superior solution and that federal law should (1) target "cybersquatters" who, with a bad-faith intent, either register, use, or sell domain names identical to or confusingly similar to the names of viable political candidates; and (2) ensure that domain name purchasers remain anonymous up until the point when materials are posted on their sites or until certain bad-faith motives can be proven. Such a measure would not only address cyber-piracy, but would also protect cyber-privacy by allowing the

---

19. See discussion infra Parts III.A.2, III.B.
I. THE ROLE OF THE INTERNET IN THE MODERN POLITICAL CAMPAIGN

In the world of politics, there may never be a substitute for a candidate getting out among the electorate and pressing the flesh. Indeed, in many respects, cyber-campaigning seems to be the antithesis of politics as we know it. Mass e-mails, on-line solicitations for donations, and professionally produced Web pages are hardly the equivalent of a candidate making an appearance at a local charity event, speaking at a college or university, or staging a town meeting. Nevertheless, empirical data suggest that politicians are beginning to make extensive use of the Internet. From online disclosure of donors, to policy statements, to transcripts of speeches, many campaigns have begun to make their mark in cyberspace. Although online activities in the political realm will probably never be a substitute for more traditional campaigning, there can be little doubt that politicians are ready to make as much use of the information superhighway as electoral success will permit.

In addition to the benefits that Internet campaigning offers to candidates, new technology also holds exciting possibilities for the citizenry. As Bruce Bimber of the University of California at Santa Barbara explains, “[t]his technology offers new opportunities for citizens to engage in various political actions, such as attempting to persuade others how to vote, learning about issues or candidates, or attempting to coordinate or organize political action.”22 The hope is that the electorate will become more politically active because of the Internet and that American democracy will reach participation levels that were previously technologically impossible.23 Additionally, electronic dissemination of political information at a relatively low cost means that citizens will have the opportunity to access campaign materials that were previously too ex-
Nevertheless, early studies suggest that while "technology does have effects on the aggregate political behavior of the public, . . . this effect is very small—much smaller than is implied in much of the literature on the Internet as a political phenomenon."24 Despite this, candidates are jumping on the electronic bandwagon, and online campaigning is becoming increasingly common and increasingly sophisticated.

It was not until the 1996 election cycle that candidates for public office began to use the Internet as a campaign tool.25 At that time, the Pew Research Center . . . reported that . . . "about 21 million Americans (12% of the voting-age population) obtained political or policy news from online sources." As many as 10% of the sample polled stated that they received at least some election information from the Net. In addition, 8% visited sites sponsored by candidates or political parties, and 3% said that the Internet was their principal source of campaign information (citations omitted).26

The more recent Bimber study reports that under 9% of people in 1998 used the Internet to express political views, to learn about political issues, or to get in contact with elected officials or candidates.27 Many observers attribute the low participation rates to the fact that the Internet has not matured enough to be an effective political medium. Online service is not universally available—presently less than half of all American adults have Internet access; and second, online information reaches only those World Wide Web users who intentionally seek it out.28

Although potential voters may not be using the Internet at very high rates, that is not because of a lack of politically oriented content. Many candidates now see a Web page as an obligatory part of campaigning. An American University study reports that 75% of U.S. Senate candidates and 64% of U.S. House candidates had Web sites for the 1998 election.29 Because most of the sites did not have a public counter, it is difficult to determine how much activity actually took place on the Web. Available data indicate that campaign sites for Senate candidates received hits in a range from 3,000 to 6,000 over the en-

---

27. See Bimber, supra note 24, at 10.
28. See Raney, supra note 21 ("On TV, you decide to watch "Seinfeld," and you get our ad," said Mark Mellman, a Washington political consultant. . . . "The problem is, not many people want political information. When you go to the Web, you have to want to go to a political site.").
29. See Dulio et al., supra note 25, at 2.
Domain Name Piracy and Privacy
tire campaign period and that House sites were substantially less active.\(^\text{30}\)

Even so, at least one political consultant believes that 1998 represented the "first election year in which the Net [could] be considered a mass medium."\(^\text{31}\) Not only did candidates make increased use of Web sites in 1998, but the sites became more technologically sophisticated. In the past, candidates’ presence in cyberspace had been likened to little more than digital yard signs containing only static content, such as candidates’ biographies, appearance schedules, and speeches.\(^\text{32}\) However, by 1998, more interactive Web sites appeared, inviting people to register online as volunteers and donors.\(^\text{33}\) Dulio, Goff, and Thurber found that nearly 73% of the candidates with Web sites in 1998 solicited contributions from visitors in some way. Methods of online fundraising ranged from inviting potential contributors to send money by mail to more advanced secure transaction technology allowing collection of online contributions made with a credit card.\(^\text{34}\)

The experience in 1998 suggests that the Internet is fast becoming a viable campaign tool with unprecedented uses. And given that candidates now take cyber-campaigning seriously,\(^\text{35}\) so too must Internet governance bodies take seriously political cybersquatting and domain name piracy. Campaigns invest money and time in professional Web page production, and they know that a least a small percentage of voters look to the Web for news and information. Both of these factors provide background for the growing problem of political domain name piracy, and they indicate the need for a solution to the problems of misleading political parodies and the ransoming of valuable Internet addresses.

II. DOMAIN NAME PIRACY AND THE CONGRESSIONAL RESPONSE

A. The Problem of Domain Name Piracy in the Political and Commercial Realms

The phenomenon of domain name appropriation is a consequence of the

\(^{30}\) See id. at 11 ("One campaign manager lamented that his candidate’s site had been accessed only 26 times—13 of them by the candidate looking to see how many hits there were.").

\(^{31}\) Raney, supra note 21 (quoting Phil Noble, president of Politics Online).


\(^{35}\) A recent search using the AltaVista search engine www.altavista.com confirmed that all presidential hopefuls for the 2000 election had an official campaign site.
general structure of the World Wide Web. Although many Web sites utilize "hyperlinks" allowing a user to jump from site to site via a simple "point and click" system, the address of the first site accessed must be typed in. "Because there is no infallible index of Web sites, users continue to use trial and error to find a Web site. This creates a strong incentive for companies to register domain names that are short, simple, and logically related to their company name or product trademarks." Thus, the site addresses themselves become valuable Internet "property" for which some companies are willing to pay large sums in order to establish a meaningful online presence.

Cybersquatters are aided in their pursuit for valuable domain names by the first-come, first-served system that governs domain name registration. Until very recently, a consortium of organizations called the InterNIC, operating under a franchise from the National Science Foundation (NSF), held a monopoly on all " .com," " .net," " .edu," and " .gov" domains. Distribution of the names was administered exclusively by Network Solutions, Inc. (NSI), a for-profit Virginia corporation.

Originally, NSI followed a strict first-in-time rule, awarding each particular address to the first applicant to request it and allowing individual parties to work out any trademark or intellectual property disputes on their own. However, in response to the growing problem of "domain name hijacking," NSI adopted a new domain name dispute policy in September of 1996. Under the new policy, NSI maintained that it would not determine the legality of domain name registration or otherwise evaluate whether registration of an Internet address infringed on the rights of a third party. Rather, upon proof that a domain name was identical to a valid foreign or domestic trademark owned by another entity, NSI would place the domain name on "hold," precluding use by both the applicant and the trademark holder. If the issue was then litigated, NSI would agree to abide by any court orders.

As the Internet expanded and became more commercialized, individuals and businesses began to complain about the system of domain name allocation.

36. Adrian Wolff, Pursuing Domain Name Pirates into Uncharted Waters: Internet Domain Names that Conflict with Corporate Trademarks, 34 SAN DIEGO L. REV. 1463, 1469 (1997).
38. "InterNIC" stands for Internet Network Information Center. The consortium includes the National Science Foundation, General Atomics, AT&T, and Network Solutions, Inc. See generally, DANIEL P. DERN, THE INTERNET GUIDE FOR NEW USERS 412-16 (1994).
39. See William A. Tanenbaum, Rights and Remedies for Three Common Trademark-Domain Name Disputes: (1) Domain Name vs. Trademark, (2) Shared Trademarks and (3) Domain Name Hijacking, 505 PLU/PAT 253, 257 (1998).
41. See id.
42. See id.
Domain Name Piracy and Privacy

Businesses that were “staking their future on the successful growth of the Internet” wanted a more “formal and robust management structure.” Moreover, leaving the domain name system in the hands of NSI proved to be a sub-optimal situation, because it offered users no alternative places in which to register and prevented new registrars from entering the lucrative domain name business. Thus, when NSI’s contract with the NSF expired in March 1998, many groups, including the United States government, began to advocate the privatization of domain name registration.

Although not yet fully implemented, the anticipated solution will create a new non-profit corporation called the Internet Corporation for Assigned Names and Numbers (ICANN) that will serve as the governing body for the domain name registration system and accredit companies seeking to compete with NSI. According to its governance structure, ICANN is to operate in “an open and transparent manner” in order to “ensure fairness.” However, because of the time needed to implement the ICANN solution, the NSF extended its contract with NSI until September 2000 on the condition that NSI would begin to develop a system to support new registrars, create a searchable domain name database, and provide technical assistance to ICANN.

Under a deal worked out between NSI and ICANN in September 1999, NSI will retain long-term control of all “.com” addresses. In return, NSI has agreed to give $1.25 million to ICANN and to reduce the wholesale price it charges competing registrars for entering domain names into the main database, or “telephone book for the Internet.” Additionally, under the agreement, NSI announced that it would give the public access to the directory, although it would charge companies for such access. As of the summer of 2000, ICANN had not yet announced the procedure through which it will resolve domain name disputes, thereby leaving NSI’s domain name dispute policy in place for the immediate future.

B. Political Cybersquatting and its Consequences

Because NSI’s dispute resolution mechanism applies only to domain names that are identical to a valid registered trademark, it provides no protection to
political candidates. Candidates, like businesses, want simple, easy-to-
remember and easy-to-guess domain names. However, because political can-
didates are, by definition, engaged in political rather than commercial endeav-
ors, they are precluded from seeking trademark protection for their personal
names.

"Trademarks concern commercial origin identifications (they are marks of
trade)." Thus, the Trademark Act of 1946 (the Lanham Act) provides for
federal registration of a "trademark used in commerce." It is possible to
trademark a personal name so long as it has "attain[ed] secondary meaning" or
"the requisite degree of notoriety," but only so long as it is used in a com-
mercial setting. The idea behind these requirements is that names are not con-
sidered inherently distinctive unless they are associated with some degree of
notoriety, and only then will courts be likely to award relief against an in-
fringer who adopts the same or a confusingly similar personal name of another
as his own trademark or trade name.

For example, under the Lanham Act, Kareem Abdul-Jabbar would have
federally protected trademark rights in the commercial use of his given name,
Lew Alcindor, but Al Gore would have no protectable right in the political
use of his name. On the other hand, Gore would have a cause of action if a
manufacturer promoted its product through a "false endorsement claim based
on the unauthorized use of [Gore's] identity." In other words, trademark
protection of personal names turns on whether the alleged infringing use is
commercial in nature. Because political campaigning is not a commercial or
profit-seeking activity, a political candidate does not have the ability to trade-
mark his name for campaign purposes. Therefore, as George W. Bush recently
discovered, candidates are denied the protection of NSI dispute resolution pro-
cedures, making the online political world fertile ground for cyber-pirates.

In late 1998, Zack Exley, a Boston computer consultant and graduate stu-
dent, realized that the George W. Bush presidential campaign had not regis-
tered various permutations of Bush's name. Seizing on this opportunity,
Exley purchased Internet addresses at www.GWBush.com, www.GWBush.org,
and www.GBush.org. He then posted anti-Bush materials on each of the sites.

51. JANE C. GINSBURG ET AL., TRADEMARK AND UNFAIR COMPETITION LAW 27 (1991) (emphasis
added).
53. JEROME GILSON, TRADEMARK PROTECTION AND PRACTICE I § 2.08 (1974).
54. See Abdul-Jabbar v. General Motors Corp., 85 F.3d 407 (9th Cir. 1996).
55. Waits v. Frito-Lay, Inc., 978 F.2d 1093, 1110 (9th Cir. 1992). This result obtains regardless of
whether a public figure, such as Al Gore, has registered his name as a trademark or not. "You need not
register a trademark to have protectable exclusive rights in it. . . . By simply using a mark on or in con-
nection with goods, or by displaying the mark in the sale or advertising of services, you can automati-
cally acquire trademark rights in the geographic area of use." GINSBURG ET AL., supra note 51, at 27.
56. For a general description of the Exley escapade, see Kedrosky, supra note 10.
57. Exley's postings center on allegations of drug use in Bush's younger days and include a fake
Domain Name Piracy and Privacy

hoping to extort money from the Bush campaign. Initially, Exley posted look-alike pages that closely resembled the official Bush campaign Web page, using the same graphics and page layout. However, after Bush officials sent Exley a letter threatening to bring suit for copyright infringement, he amended the sites, while still preserving their basic anti-Bush sentiment.

The Bush camp, recognizing they had been beaten to the mark, then registered up to 260 Bush-related domain names, including such negative addresses as www.bushsux.org and www.bushblows.com. Additionally, the campaign sent Exley a cease-and-desist order. Shortly thereafter, Bush lawyers filed a complaint with the Federal Election Commission, requesting that Exley be required to file certain disclosure documents with the Commission. The candidate himself would later call Exley a “garbage man” and demand that “there ought to be limits to freedom.”

Meanwhile, as Bush made potentially damaging remarks, Exley was flourishing. He received vast amounts of press, and as a result, his sites received more than six million hits in May 1999 alone, while the official Bush site was visited only 30,000 times in the same period.

Although some might argue that the heavy traffic at Exley’s sites is a fine example of the robust debate and citizen participation toward which the American political process should strive, there can be little doubt that the Exley sites are also potentially misleading and deceptive—characteristics that have important ramifications for the development of the Internet into a viable political medium. As one observer has noted, “[t]he problem [of misleading domain names] becomes especially damaging when Net users may fail to recognize that the parody is not really the official campaign site.” Simply by duplicating an official campaign’s Web page layout or by using professional quality pictures, he could defraud Net users.

other sections of the site, such as the following, poke fun of Bush’s claim to be a “compassionate conservative”:

G.W. Bush’s politics derive from his own life experience. Although he made serious mistakes as a youth, the Bible says, “Do unto others. . . .” And G.W. Bush has indeed been forgiven again and again by others.
First there was his rambunctious youth, in which he doesn’t deny there was use of cocaine and other drugs. Then, as an unsuccessful Texas businessman, he was bailed out with millions of dollars from friends of his powerful father. As President, G.W. Bush wants to create an America in which everyone gets as much forgiveness, and as many chances to grow up, as he had.


58. The Bush campaign engaged in some cyber-trickery of its own, automatically linking anyone who reaches www.bushblows.com or www.bushsux.com to the official Bush campaign site.
59. See infra Part III for a more detailed examination of the allegations set forth in the Bush complaint.
60. Kedrosky, supra note 10.
61. Zremski, supra note 33. Although traffic at Exley’s Web pages continues to be extremely high, there is no evidence that Exley has tried to sell advertising space on the sites. The only revenues that Exley collects for his efforts are from the sales of T-shirts and bumper stickers calling for “Unlimited Freedom.”
62. Oram, supra note 26, at 489.
graphics and design, a sophisticated political parodist can easily dupe the unsuspecting Net surfer. For instance, during the 1996 presidential campaign, software developers Brooks Talley and Mark Pace established sites at www.dole96.org, www.clinton96.org, www.forbes96.org, and www.buchanan96.org, with the result that nearly 20% of the e-mail inquiries they received were "sincere campaign questions or comments."  

Not only do candidates themselves have a vested interest in making sure that potential Internet addresses are not appropriated by cybersquatters or parodists, but voters too need assurance that the information they receive is accurate. At least one commentator has argued that fraudulent political messages should be restricted in furtherance of the integrity of democratic processes.  

From a candidate's perspective, the use of a confusing domain name can be the difference between a humorous but harmless attempt to poke fun and an act of political sabotage. By appropriating an official-sounding name, the parodist can draw Internet traffic away from the real candidate's home page. This in turn will diminish the size of the candidate's audience, thereby hindering his ability to recruit supporters, communicate with the press, and disseminate his message to the undecided voters. Furthermore, by diverting potential visitors, a parody site can also impede Internet fund-raising.  

Fraudulent and misleading online parodies inhibit the development of the Internet as an effective political medium. They not only make the cost of speech on the Web more expensive as potential candidates make preemptive purchases of numerous domain names, but they also dilute the public's confidence in the reliability and authenticity of online materials. As the next section demonstrates, Congress has considered the commercial implications of this problem serious enough to enact a legislative solution.

C. The Anticybersquatting Consumer Protection Act

Cybersquatting and domain name piracy are phenomena that have a commercial origin. As one industry commentator has noted, "[w]ith dollar signs in their eyes, World Wide Web surfers have busily registered what they hope

---


64. The First Amendment debate surrounding domain name piracy is beyond the scope of this Note. For a general discussion of the constitutional implications of restricting online political parody, see Oram, supra note 26, at 518-21 ("[S]ome restrictions on political expression can be justified. For example, an individual's free speech rights do not entitle him to infringe a candidate's intellectual property rights.").

65. Id. at 489.

will become lucrative domain names—as either popular Web sites or high-priced items to auction." Congress has not been oblivious to the problem, recently passing the Anticybersquatting Consumer Protection Act, which promises to cut into the profits of cybersquatters and domain name hijackers. The law, sponsored by Senators Orrin Hatch (Republican-Utah), Patrick Leahy (Democrat-Vermont), and Spencer Abraham (Republican-Michigan), was introduced in the summer of 1999 and quickly gained broad bipartisan support. Beginning with the basic premise that a commercial, and indeed political, presence on the Internet is dependent on having a memorable domain name, the core of the Act provides that:

[a] person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section

(ii) registers, traffics in, or uses a domain name that—

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark; [or]

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark.

Because the bill requires the plaintiff to prove "bad-faith intent" on the part of the cybersquatter, it does not extend to innocent domain name registrations by those who are unaware of another's claim to the name. Nor does it cover someone who is aware of the trademark status of the name but registers a domain name without a bad faith intent to profit. In considering whether a bad-faith intention exists, a court may consider the following eight factors, the first four of which suggest the absence of bad-faith, and the last four of which indicate the presence of a bad-faith intent to profit:

- the trademark or other intellectual property rights of the registrant in the Internet address;

69. See Lee, supra note 7.
70. See Steve Higgins, What's in an Internet Name? To On-Line Marketers, Lots, INVESTOR'S BUS. DAILY, Oct. 17, 1995, at A10 ("Catchy addresses are as important to on-line merchants as prime retail space is to conventional merchants, cybernauts say. It's easier to order jewelry from a business that can be reached by typing 'gold.com,' for example, than it is to buy it from another vendor with a forgettable address.").
71. § 3002(a), 113 Stat. at 1501A-545 to -546.
the extent to which the domain name consists of the legal name of the registrant or a name that person commonly uses;

- the person’s legitimate noncommercial use of the mark in a site located at the domain name;

- the person’s bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

- the registrant’s intent to divert consumers from the mark owner’s Web site to the site registered either for commercial gain or with the intent to disparage the mark by creating a “likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;”

- the registrant’s offer to sell the domain name for substantial consideration;

- the registrant’s provision of misleading contact information when applying for the domain name; and

- the registration of multiple domain names which are identical to, confusingly similar to, or dilutive of trademarks without regard to the goods or services of such persons.73

Once a court determines that a bad-faith intent to profit exists, a domain name pirate may be held liable for a variety of activities, from mere registration, to actual use, to resale of the Internet address.

Damages available under the bill consist of the traditional trademark remedies—injunctive relief and damages. Specifically, statutory damages are available in an amount not less than $1,000 and not more than $100,000 per domain name.74 Finally, the Act encourages domain name registrars to act to prevent cybersquatting by providing them with limited liability when they suspend, cancel, or transfer domain names pursuant to a court order or in the implementation of a policy prohibiting cybersquatting.75 Additionally, a trademark owner who knowingly and materially misrepresents that a domain name is in violation shall be liable to the original domain name registrant for any damages resulting from the suspension, cancellation, or transfer of the domain name.76

Although the Anticybersquatting Consumer Protection Act has the potential to address serious problems in the commercial realm, it is limited in application by virtue of the fact that it applies only to domain names identical to or confusingly similar to valid trade- and service marks. As indicated above, politicians are precluded from seeking trademark protection for their names, leaving them vulnerable to domain name hijacking even under the new law. Therefore, unless some existing regulatory regime offers relief, there is a need for a new statute to address the problem of domain name piracy in the political

73. See § 3002(a), 113 Stat. at 1501A-546.
74. See § 3003(b), 113 Stat. at 1501A-549.
75. See § 3004, 113 Stat. at 1501A-549 to -550.
76. See id.
Domain Name Piracy and Privacy

context.

III. THE FAILURE OF FEDERAL ELECTION REGULATIONS TO ADDRESS THE PROBLEM OF DOMAIN NAME PIRACY

As discussed above, the Bush campaign reacted to the Exley sites by filing a complaint with the FEC. Because such complaints are not public documents, it is impossible to know the theories upon which Bush lawyers hoped to bring Exley within the federal election regulations. However, according to newspaper reports, the complaint requested that Exley either be regulated as a political action committee or that he make the disclosures required of persons making large independent expenditures.77 This section will examine the merits of each of these claims in turn and explore the ramifications that each would have for the future of online politics.

A. Online Political Parodists Are Probably Not Political Committees

The term "political action committee" is an informal one that is found neither in federal statutes nor in the Code of Federal Regulations.78 However, the regulations do define a "political committee," and it is this set of definitions that delineates what is known in common parlance as a PAC.79 Additionally, the regulations impose filing and disclosure requirements on political committees—rules that the Bush campaign had hoped would reign in Exley and other cyber-pirates.

Under FEC rules, all political committees must file a Statement of Organization with the Commission.80 Thereafter, as a general matter, the committee must file periodic reports detailing (1) receipts, (2) disbursements, (3) contributions and operating expenditures, and (4) debts and obligations.81 The reports must include the names of any persons who either made contributions in excess of $200 or to whom expenditures totaling more than $200 were made.82 More important for present purposes, every communication by a political

---

77. See Glass, supra note 9; Slater, supra note 10; Wallack, supra note 1; Zremski, supra note 33.
79. The definition appears at 11 C.F.R. § 100.5 (2000). As the Supreme Court has noted, [t]he Act's use of the word "political committee" calls to mind the term "political action committee," or "PAC," a term that normally refers to organizations that corporations or trade unions might establish for the purpose of making contributions or expenditures that the Act would otherwise prohibit. See §§ 431(4)(B), 441b. But, in fact, the Act's term "political committee" has a much broader scope. The Act states that a "political committee" includes "any committee, club, association or other group of persons which receives" more than $1,000 in "contributions" or "which makes" more than $1,000 in "expenditures" in any given year.
80. See 11 C.F.R. § 102.1.
81. See id. § 104.3.
82. See id.
committee soliciting any contribution or *expressly advocating* the election or defeat of a clearly identified candidate through any broadcasting station, newspaper, magazine, or other type of general public political advertising must "clearly state" that the communication is not authorized by a candidate, authorized committee, or agent, and that it is paid for by such other person.\(^8\)

It is this rule, Bush lawyers argued, which mandates that Exley include a disclaimer on his Web pages stating that the sites are his own and are unconnected with the Bush campaign. However, before Exley and other cybersquatters and pirates fall within the political committee regulations, it is necessary to determine whether they meet the definition of a political committee.

Federal Election Commission rules identify four types of political committees. The three definitions set forth below are clearly inapplicable to online parodists:

1. a separate segregated corporate fund;\(^8\)\(^4\)

2. "any local committee of a political party" which "receives contributions aggregating in excess of $5,000 during a calendar year, . . . makes payments exempted from the definition of contribution . . . in excess of $5,000 during a calendar year, . . . or makes expenditure aggregating in excess of $1,000 during a calendar year,"\(^8\)\(^5\) and

3. "an individual's principal campaign committee or authorized committee(s)."\(^8\)\(^6\)

Instead, Bush lawyers likely argued that Exley falls under the political committee regime because he qualifies as a "committee, club, association, or other group of persons which receives contributions aggregating in excess of $1,000 or which makes expenditures aggregating in excess of $1,000 during a calendar year."\(^8\)\(^7\)

As a threshold definitional matter, most political cybersquatters and parodists might argue that they are individuals rather than a "committee, club, association, or other group of persons." Although that might be true in a large number of cases and enough to exempt many online parodists from PAC regulations, this argument does little to help Exley. It turns out that the Exley sites are run by him in connection with a "corporate sabotage collective" called *®Mark* (pronounced "art-mark"), thereby precluding the potential defense that the parody sites are not the work of a "committee, club, association, or other group of persons."

Additionally, it is necessary to note that the broad definition of a "political

\(^8\)\(^{3}\) See *id*. § 110.11. This Note will address the mass communication rule in more detail at *infra* Part III.A.2.

\(^8\)\(^{4}\) The separate segregated fund is defined at 11 C.F.R. § 100.5(b).

\(^8\)\(^{5}\) See *id*. § 100.5(c).

\(^8\)\(^{6}\) See *id*. § 100.5(d).

\(^8\)\(^{7}\) *Id*. § 100.5(a).
committee" set forth above is subject to further definitional limits. First, the regulations define the key terms “contribution” and “expenditure” to include only those contributions and expenditures made “for the purpose of influencing any election for Federal office.” And even within this narrowed category of election-related disbursements, there are certain exclusions, such as “payments made solely for the purpose of determining whether an individual should become a candidate” and costs incurred by a membership organization for communications to its members, among others.

Second, the FEC has interpreted the term “political committee” to require that the “major purpose” of the organization, not just the contribution or expenditure, be political in nature for the organization to be deemed a political committee. In Federal Election Comm’n v. GOPAC, Inc., a federal district court held that this limitation was constitutionally necessary and that under it the FEC was unable to prove that the major purpose of an organization whose aim was to end the Democratic Party’s control of Congress was the election of particular federal candidates. However, in a subsequent case, the D.C. Circuit held that the “major purpose” limitation was unwarranted and that, accordingly, the FEC acted improperly in dismissing a complaint that a lobbying organization supporting U.S.-Israel relations was a political committee. On appeal, the Supreme Court declined to decisively address the “major purpose” question, preferring instead to permit the FEC to “develop a more precise rule that may dispose of this case, or at a minimum, . . . aid the Court in reaching a more informed conclusion.” For the present, the “major purpose” test remains a constitutionally necessary requirement for determining whether an organization is a political committee.

89. 11 C.F.R. § 100.7(a)(1), § 100.8(a)(1) (2000).
90. Id. § 100.8(b)(1)(i).
91. Id. § 100.8(b)(4).
   The general requirement that “political committees” and candidates disclose their expenditures could raise similar vagueness problems, for “political committee” is defined only in terms of amount of annual “contributions” and “expenditures,” and could be interpreted to reach groups engaged purely in issue discussion. The lower courts have construed the words “political committee” more narrowly. To fulfill the purposes of the Act they need only encompass organizations that are under the control of a candidate or the major purpose of which is the nomination or election of a candidate.
93. The Court reiterated this position in Federal Election Comm’n v. Massachusetts Citizens for Life, Inc., 479 U.S. 238, 252 n.6 (1986), holding that “an entity subject to regulation as a ‘political committee’ under the Act is one that is either ‘under the control of a candidate or the major purpose of which is the nomination or election of a candidate.’” (quoting Buckley v. Valeo, 424 U.S. 1, 79 (1976))
1. Application of the Political Committee Definition to Exley

To qualify as a political committee, Exley—in conjunction with $TM^c$Mark, the corporate sabotage group that helps him maintain the sites—must (1) meet the $1,000 expenditure or contribution threshold and (2) have as his “major purpose” the election or defeat of a candidate.

First, although the contribution issue is a simple question of fact and recordkeeping, the issue of expenditures raises a more complicated set of problems. Bush lawyers argued that “[the FEC should] factor... in everything from the cost of the computer equipment used to the market value of the Net address” when evaluating whether the $1,000 threshold has been met. Conversely, Exley argued that his Web pages are virtually cost-free, save for the $70 domain name registration fee.

In a perfect accounting world, some version of the Bush position is probably the correct one. An accurate measure of expenditures should include a portion of the cost of the computer hardware used to create the site at issue, although determining an appropriate allocation method presents serious practical problems. First, there is the problem of valuing the hardware. As anyone who has ever purchased a computer knows, rapid depreciation necessitates a more sophisticated metric than purchase price to accurately gauge hardware value. However, deciding on a depreciation schedule or other computational basis for determining an accurate value is likely to subject the FEC to a far more difficult administrative problem than it cares to become involved in. Additionally, even if an appropriate method can be divined, the valuation question would undoubtedly lead to endless litigation for the Commission.

Furthermore, Bush lawyers argued that the FEC should factor in the market value of the Internet site itself when determining whether a cybersquatter has exceeded the $1,000 expenditure threshold. However, not only is a domain name a potentially even more troublesome asset to value than computer hardware, but the suggestion that the market value of the site, as opposed to the price actually paid, be considered as an expenditure is unconvincing. The regulations define a political committee in terms of “expenditures,” not value of assets held or value of assets purchased. Thus, the focus on fair market value is irrelevant for current purposes.

A further difficulty raised by the Bush proposal is that it would require the FEC to develop a fair and accurate allocation method. That is, once the FEC has determined the appropriate value of the computer hardware, there must be some mechanism by which a portion of the value is assigned to the Web site at

96. Wallack, supra note 1.
97. See id.
98. Although it is true that an online market for domain names has developed, the market is often so thin that accurate valuation may be next to impossible.
issue and treated as an expenditure for purposes of the political committee
definition. Should the allocation be based simply on the proportion of time
spent creating and maintaining the site at issue as compared to all other com-
puter activities; should it depend on the computing power necessary to create a
certain site; should it be a combination of the two; or are there other more ac-
curate methods? Any of these possibilities is likely to lead to complicated
factual disputes that the FEC may find that it lacks the expertise to resolve.
Additionally, they are likely to subject the Commission to vexatious litigation
that has the potential to consume large amounts of time, effort, and money. In
the end, although an allocation method may be possible in theory, it raises
practical concerns that may be fatal in practice, and absent some such method,
Exley does not meet the $1,000 expenditure requirement.

As for the second prong of the political committee definition, it is likely
that Exley satisfies the FEC's "major purpose" test. Briefly stated, the relevant
inquiry is whether the Exley group's "major purpose" is issue advocacy or the
election or nomination of a candidate. If the purpose is mere issue advocacy
and a desire to educate the public with regard to certain issues, then the group
would not qualify as a political committee even if it satisfied the expenditure or
contribution test. Although the line between issue advocacy and a more ex-
plicit electoral purpose is muddy, the fact that Exley's Web pages focus on
a single candidate as opposed to a specific topic, suggest that they might satisfy
the "major purpose" test. Additionally, there is little doubt that they are closely
connected with a particular election and the fate of a particular candidate in
that election. Nevertheless, officials of @Mark are quick to point out, "[w]e're
not affiliated with any . . . campaign. In fact, we see ourselves as completely
nonpartisan." Even so, there is at least a plausible argument that Exley and
company satisfy the "major purpose" prong of the political committee defini-

99. These are but two possible allocation methods. Undoubtedly, there are many others—each pre-
senting the opportunity for dispute and litigation over whether the $1,000 expenditure threshold was
reached.

100. See Akins, 118 S. Ct. at 1782 (distinguishing between election-related expenditures and issue
advocacy).

101. In distinguishing issue advocacy and explicit electoral statements, the Buckley Court noted
that
the distinction between discussion of issues and candidates and advocacy of election or defeat
of candidates may often dissolve in practical application. Candidates, especially incumbents,
are intimately tied to public issues involving legislative proposals and governmental actions.
Not only do candidates campaign on the basis of their positions on various public issues, but
campaigns themselves generate issues of public interest.


Similarly, the D.C. Circuit observed in the same case that
[p]ublic discussion of public issues which also are campaign issues readily and often unavoid-
ably draws in candidates and their positions, their voting records and other official conduct.
Discussions of those issues, and as well more positive efforts to influence public opinion on
them, tend naturally and inexorably to exert some influence on voting at elections.

Buckley v. Valeo, 519 F.2d 821, 875 (D.C. Cir. 1975).

102. Slater, supra note 10 (quoting Frank Guerrero).
2. Express Advocacy

Even assuming that some domain name pirates meet the expenditure requirement and the "major purpose" test and are brought under the political committee regulatory regime, the only consequences that they face are reporting requirements and the possibility that they will be required to disclose their identity in certain mass communications. Not only are these relatively insignificant burdens, but the mass communications disclosure rule is easily avoided. According to the regulations, a disclaimer is required only if the mass communication "expressly advocates" the election or defeat of a clearly identified candidate. "Express advocacy" is defined in the regulations to mean using any communication that

> uses phrases such as "vote for the President," "re-elect your Congressman,"... "Bill McKay in '94,"... or communications of campaign slogan(s) or individual word(s), which in context can have no other reasonable meaning than to urge the election or defeat of one or more clearly identified candidate(s), such as posters, bumper stickers, advertisements, etc. which say "Nixon's the One," "Carter '76," "Regan/Bush" or "Mondale!"; or

> when taken as a whole and with limited reference to external events, such as the proximity to the election, could only be interpreted by a reasonable person as containing advocacy of the election or defeat of one or more clearly identified candidate(s).\(^{103}\)

The express advocacy standard was first adopted by the Supreme Court in *Buckley v. Valeo*, when the Court held that the FEC can regulate speech as an independent expenditure only if it represents "communications that in express terms advocate the election or defeat of a clearly identified candidate for federal office."\(^{104}\) The Court went on to explain, in a footnote, that express advocacy would include communications containing certain magic words, such as "'vote for,' 'elect,' 'support,' 'cast your ballot for,' 'Smith for Congress,' 'vote against,' 'defeat,' [or] 'reject.'"\(^{105}\) Ten years later, in *FEC v. Massachusetts Citizens for Life*,\(^{106}\) the Court expanded the standard somewhat by holding that express advocacy could be "less direct" than the examples suggested in *Buckley* so long as the essential nature of the communication goes "beyond issue discussion to express electoral advocacy."\(^{107}\)

The FEC definition of "express advocacy" quoted above is very much in the spirit of *Massachusetts Citizens for Life*. "[T]he FEC does not halt the

---

103. 11 C.F.R. § 100.22(a, b) (2000).
104. *Buckley*, 424 U.S. at 44.
105. *Id. at 44 n.52.
107. *Id. at 249.*
search for express advocacy after looking for magic words. . . . [T]he FEC, or the court, also examines the communication as a whole and considers such factors as when and where the communication takes place."  

However, at least some federal courts have continued to adhere to the more restrictive "magic words" approach taken in Buckley, casting constitutional doubt on the FEC definition. In fact, the First Circuit has gone so far as to hold that subsection (b) of the FEC definition, which mandates consideration of the "communication as a whole," is unconstitutional under Buckley. 

The narrow construction of "express advocacy" as "magic words" alone is a definition that is easily avoided. A Web page which is strongly critical of a candidate but avoids the use of certain incriminating phrases is exempt from federal election regulation. Therefore, even if a cyber-pirate happens to be classified as a PAC, careful site design may defuse the mass communications identity disclosure rule—the rule that has the greatest potential to provide some measure of protection for candidates. Additionally, depending on the nature of various parody sites, it is quite conceivable that they might escape regulation even under a more expansive definition of express advocacy. Many of these sites are posted far in advance of elections and could be interpreted by a reasonable person to be directed at a goal other than "the election or defeat of one or more clearly identified candidates."

3. Shortcomings of the Political Committee Argument

There are strong reasons to think that the PAC argument is a weak way to stop cyber-pirates. First, as a definitional matter, it is questionable whether most parodists will have the election or defeat of a particular candidate as their "main purpose;" second, it unlikely that many cybersquatters would satisfy the $1,000 contribution or expenditure requirement, particularly those who purchase sites with a view toward resale rather than posting materials; and third, Web page designers will find it easy to evade the mass communications rule by


109. See, e.g., Faucher v. Fed. Election Comm'n, 928 F.2d 468, 470-72 (1st Cir. 1991) (citing Massachusetts Citizens for Life solely for the proposition that the Supreme Court requires the express advocacy standard to be met). But see FEC v. Furgatch, 807 F.2d 857 (9th Cir. 1987) (rejecting the "magic words" approach to express advocacy).


111. See Scott E. Thomas & Jeffrey H. Bowman, Is Soft Money Here To Stay Under the "Magic Words" Doctrine?, 10 Stan. L. & Pol'y Rev. 33, 43 (1998) (arguing that a "magic words test . . . would reach 'only those who lacked the minimal wherewithal to choose some words other than 'vote for' or the like'" (quoting 63 Fed. Reg. 8363, 8364 (1998)).
avoiding express advocacy. However, even if one overcomes the definitional problems and the express advocacy hurdle, the PAC argument does nothing to stop true cybersquatters who simply purchase a potentially valuable domain name with the hope of reselling it. These individuals spend little or no money to maintain content on the site, nor do they post material that might be construed as express advocacy. Therefore, it seems unlikely that this set of election regulations offers much hope of combating the political domain name hijacking problem.

B. Independent Expenditures

As an alternative to classifying Exley as a PAC, Bush lawyers also suggested that he should be required to comply with the independent expenditure regulation. Under this rule, "[e]very person other than a political committee, who makes independent expenditures aggregating in excess of $250 during a calendar year shall file a signed statement or report... with the Commission."112

According to the regulations, an "independent expenditure" is defined as an "expenditure... for a communication expressly advocating the election or defeat of a clearly identified candidate which is not made with the cooperation... of, a candidate... or authorized committee of such candidate."113 A person making an expenditure which meets these requirements must file a report with the FEC including such information as to whom the expenditure was paid, whether the expenditure was in support of or in opposition to a candidate, and the identity of each person who made a contribution in excess of $200 to the person filing the report.114

Unfortunately for candidates trying to protect their virtual turf, the independent expenditure regulation suffers from the same weaknesses as the rules governing political committees. Again, domain name hijackers are likely to argue that their activities are costless,115 and even if they meet the $250 expenditure requirement, they can carefully word their Internet postings to avoid express advocacy, however defined. A further limitation of subjecting parodists to the independent expenditure regime is that even if the independent expenditure is used to fund mass communications containing express advocacy,

113. Id. § 109.1(a) (emphasis added). "Independent expenditures are funds spent by interested individuals or groups—usually in the form of television or radio advertisements or mass mailings—to support or defeat a particular candidate, but are not coordinated in any way with the candidate or her campaign organization." Leffel, supra note 108, at 686.
115. Here again, Bush lawyers relied on an allocation argument to bring Exley up to the $250 threshold. As for the validity of this approach, "Trevor Potter, a Washington lawyer and former FEC chairman, said the rules could be read either way. But Potter said he's convinced the FEC doesn't want to force every individual to file." Wallack, supra note 1.
there is no requirement that the communication include a disclaimer stating who paid for it. Thus, independent expenditure regulations fail to address the problem of misleading parodies that may be confused with a candidate’s official campaign site.

As a general matter, federal election law offers little relief for the increasingly severe problem of political domain name theft. As one commentator has noted, current election regulations operate on the presumption that communications to the general public cost money. However, the rise of the Internet as a communications medium creates problems for the current regime because there is usually no incremental cost to keystrokes, and thus to e-mail, speech on Web sites, and hyperlinks . . . Without a cost to communication, current law has nothing to measure . . . the entire mechanism for disclosing political expenditures and requiring adequate information about the identity of the speaker is thrown into question.\footnote{Trevor Potter, \textit{Recent Developments in Campaign Finance Regulation} (visited June 29, 1999) http://www.brook.edu/gs/campaign/updates/Internet.htm.}

Given these problems, the most promising solution is a new federal statute analogous to the Anticybersquatting Consumer Protection Act, which would specifically address the problem of political domain name hijackers.

**IV. CONGRESS SHOULD ADOPT A STATUTE THAT ADDRESSES POLITICAL DOMAIN NAME HIJACKING**

Because federal election regulations offer little hope, if any, of combating the problems brought about by political cybersquatters, Congress should adopt a statute to provide protection for candidates—call it the Candidate Domain Name Protection Act (“the Act”). More specifically, the Act should have two provisions: the first targeting cybersquatters and domain name pirates who, with a bad-faith intent, either register, use, or sell domain names identical to or confusingly similar to the names of viable political candidates; and the second ensuring that domain name purchasers remain anonymous until materials are posted on their sites. Such provisions would address both the problems of cyber-piracy and cyber-privacy.

**A. Bad Faith Provisions**

Following the model of the Anticybersquatting Consumer Protection Act, the Candidate Domain Name Protection Act should provide that:

- any person who, with a bad-faith intent to:
  - (1) fraudulently misrepresent that a World Wide Web page is the official site of a viable political candidate,
  - (2) profit from the resale of a domain name logically linked to the name of a viable political candidate,
(3) hold a domain name logically linked to the name of a viable political candidate for the purpose of preventing that candidate from using the site as his own, registers, traffics in, or uses a domain name that is identical to or confusingly similar to the viable political candidate's name, shall be liable in a civil action by that candidate.

Whereas the intent required by the Anticybersquatting Consumer Protection Act is exclusively a bad-faith intent to profit, the Candidate Domain Name Protection Act would also apply to individuals with a bad-faith intent to either fraudulently misrepresent that the Web page is an official page of the candidate or to preempt the candidate from using certain sites intuitively linked to his or her name. Thus, the Act would address both the problem of posting material that could be falsely attributable to a candidate and the problem of holding an unutilized site with the aim of either (1) selling it for an exorbitant price or (2) preventing its use by a viable candidate.

1. Intent To Deceive

Proof of a bad-faith intent to misrepresent the parody page as an official campaign site would require extrinsic evidence of an intent to commit political sabotage. For this purpose, the very use of a domain name logically related to a legitimate candidate would be necessary but not sufficient evidence of such intent. Additionally, other factors, such as the ones listed below could provide evidence of an intent to mislead.

- Failure to disclose the identity of the owner and/or webmaster of the site;
- appropriation of site layout or graphics from the candidate's official Web page;
- an explicit statement that the parody page is an official publication of the campaign; or
- mass e-mails sent by the parodist "on behalf of the official campaign" referring recipients to the parody site.

In practice, a bad-faith provision would directly and forcefully mandate that a parodist clearly disclose his site as such if he hoped to escape liability under the Act. Note that this is exactly the result that the Bush campaign hoped to achieve in the Exley case by the circuitous route of (1) classifying Exley as a PAC and (2) alleging that he had promulgated a mass communication containing express advocacy. Under the proposed Act, the definitional problem of classifying a parodist as a political committee as well as the need to prove express advocacy would drop out of the equation. Rather than using federal election regulations in a situation to which they were probably never intended to apply, the Act would straight-forwardly and directly impose liability on those who intentionally deceive the online electorate.
Domain Name Piracy and Privacy

2. Intent To Profit

The second bad-faith intent alternative would target cybersquatters who purchase valuable political domain names and hold them ransom for large sums of money. Tracking the guidelines set forth in the Anticybersquatting Consumer Protection Act, intent to profit could be shown by:

- the registrant's intent to divert Internet traffic from the candidate's official site to the site registered;
- the registrant's offer to sell the domain name for substantial consideration;
- the registrant's provision of misleading contact information when applying for the domain name; or
- the registration of multiple domain names which are identical to or confusingly similar to the names of viable political candidates.

Because the Act would apply to registration, use, and trafficking, there would be no need for a bad-faith intent to profit to exist at the time of registration. If someone who happened to be named George W. Bush bought www.gwbush.com long before he had ever heard of the candidate, yet later threatened to post anti-Bush materials unless the Bush campaign was willing to pay him thousands of dollars for the site, he would be liable under the Act regardless of the fact that he purchased without a bad-faith intent to profit. On the other hand, if the hypothetical George W. Bush purchased www.gwbush.com in ignorance of the candidate and used the site for his own purposes—even certain political purposes—he would not be liable under the Act.

3. Intent To Preempt

The third, and final, bad-faith intent alternative is the intent to preempt, which is characterized by the intent to purchase and hold domain names intuitively linked to a viable political candidate so that the candidate cannot use the sites for himself. For example, if Steve Forbes wanted to diminish the effectiveness of John McCain's online campaigning, he might preemptively purchase sites such as www.McCain2000.org and www.McCain.com, among others, solely for the purpose of preventing McCain from using those potentially valuable addresses. Forbes might then either post nothing on the sites and merely hold them, or he might post non-deceptive content on the sites, such as a hyperlink to the official Forbes campaign Web site. In either of these scenarios, Forbes would have neither an intent to profit nor an intent to deceive, yet he would still be engaged in a type of political cyber-piracy for which candidates need a remedy. The Candidate Domain Name Protection Act would address this problem by making either the registration or use of a domain name actionable when it could be proved (1) that the registrant had an intent to pre-
vent the candidate from using the site for his own campaign and (2) the domain name registered is the same or confusingly similar to the name of the candidate bringing the action.

Because the aim of the statute is to protect candidates and their use of World Wide Web addresses intuitively linked to their names, the statute would not prevent a candidate from preemptively purchasing negative domain names logically associated with his or her own name. For example, the Bush purchases of www.bushsux.org and www.bushblows.com would not subject the candidate to liability under the proposed Act. Although Bush might have an intent to preempt in this circumstance, the cause of action granted by the statute would lie with himself, not the parodist who was actually preempted from using the site. Therefore, as a technical matter, Bush could escape liability.

This limitation on liability is not simply an accidental case that slips through the Act’s language. Rather, it is consistent with the Act’s purpose of protecting candidates’ legitimate uses of politically valuable domain names and protecting them from cyber-pirates. Although, the statute would not reach preemptive purchases of negative sites by candidates, it also would not disallow the use of negative sites by cyber-pirates. So long as www.bushsux.org was not purchased with the intent to profit, a parodist would be free to post parodies and criticisms of Bush on the site. However, the parodist would bear the burden of being the first in time to register the site, because the Candidate Domain Name Protection Statute would not extend so far as to protect parodists from preemptive purchases.

4. Defining a “Viable Political Candidate”

Finally, in addition to one of three bad-faith intents, the Act would require the registration, use, or trafficking in a domain name that is identical to or confusingly similar to the name of a viable political candidate. Admittedly, the concept of a “viable political candidate” raises difficult definitional problems that ultimately may be dependent on a facts and circumstances test. Factors to be considered might include:

- whether the potential candidate already holds elected office,
- whether the potential candidate has begun making public appearances in anticipation of running for office,
- whether the potential candidate has formed an exploratory committee,
- whether the potential candidate is engaged in fundraising,
- whether the potential candidate has put together a preliminary campaign staff,

117. I am assuming, for obvious reasons, that www.bushsux.org could never be purchased with an intent to misrepresent that it is the official Bush campaign site.
Domain Name Piracy and Privacy

and

• whether the press has begun to suggest that the potential candidate might be considering elective office.

Under the terms of the Act, once both the bad-faith element and the viable candidate element have been satisfied, either registration, use, or trafficking in the domain name would be sufficient to establish liability.

Because of the stringent bad-faith requirements in the proposed statute, the Act would protect the legitimate interests candidates have in their own names, while at the same time preserving other Internet users' freedom. In other words, anyone who wanted to purchase www.gwbush.com would be free to do so without fear of liability, so long as the site was purchased without an intent to mislead the electorate or to resell at an exorbitant price. Furthermore, the owner could also post materials on the site—even explicitly political materials—so long as there was no bad faith intent to mislead. Thus, the Act attempts to balance the freedom that has long been a hallmark of the online world with the rights of political candidates to protect the "goodwill" associated with their names.

B. Anonymity Provision

A second provision of the Candidate Domain Name Protection Act would provide that purchasers of domain names have the right to remain anonymous so long as no materials are posted on the purchased site and so long as a candidate seeking to require disclosure of ownership could not make a colorable claim that the registrant had an intent to preempt. This provision would directly address the problem that the Bush campaign ran into when it registered sites such as www.bushwhitman.com prior to the presidential primary season. The Bush camp received much unwanted press after it bought domain names containing permutations of possible presidential tickets, purchases it made to beat domain name pirates to the punch. Additionally, Bush would undoubtedly have appreciated some measure of privacy when he purchased www.bushblows.com and www.bushsux.org in an attempt to buy negative sites before they fell in the hands of Zack Exley or another political saboteur.

It seems to be a relatively uncontroversial proposition that a presidential campaign should not be forced into breaching its own privacy in order to outmaneuver unscrupulous cybersquatters. A statutory provision allowing anonymous purchasing would allow a candidate to buy strategic sites intrinsically linked to his or her name without anyone other than the domain name registrar being aware of the purchase.

118. See supra note 17 and accompanying text.
However, the period of anonymity could not extend beyond the time that materials are posted on the site without rendering the bad-faith provisions set forth above ineffective. If a domain name holder were allowed to post information, such as a misleading or deceptive political parody anonymously, then the candidate would have no means of finding out against whom to bring suit. Presumably too, a political candidate would not be concerned about protecting his own anonymity once his campaign had decided to post materials on a purchased site. That is, if Bush had selected Governor Whitman as his running mate and decided to use www.bushwhitman.com as the official site, he would have no interest in anonymous ownership. Conversely, for sites such as www.bushblows.com and other sites that the Bush campaign would merely prefer to own and not actually use, an indefinite period of anonymous ownership is desirable.

Additionally, anonymity would have to be terminated, even in the case where no materials were posted on a site, as soon as a candidate could make a colorable claim that an anonymous registrant had an intent to preempt. Because preemption may be carried out by simply buying a number of sites and holding them without content, the posting of content cannot be the sole triggering mechanism for ending anonymity. As soon as a candidate could prove to a court that he had reasonable cause to believe that a registrant had purchased sites intuitively linked to the candidate’s name, the candidate would be able to compel disclosure of the site owner’s identity and bring suit against him. By using posting and the requirement of a colorable claim of an intent to preempt as the triggering mechanisms for ending anonymity, the Act ensures cyber-privacy in those times when it is desirable, and forces disclosure when there is an increased risk of cyber-piracy.

CONCLUSION

The Internet is revolutionizing business, health care, education, science, and politics. E-campaigning is but a small facet of the momentous changes that have been brought about by the digitalization of society. Nevertheless, given the vast number of Internet users and the increasing reliance on online information sources, candidates who invest time, energy, and money into cyber-campaigning deserve protection against fraud and profiteering. Unfortunately, federal election regulations, which were drafted in era when the rise of the Internet was unforeseeable, offer little hope of a solution to the problems of cybersquatting and cyber-piracy. Therefore, it is up to Congress to recognize that e-politics deserve as much protection as e-commerce and to draft federal legislation that will help ensure the viability of the Internet as an

Domain Name Piracy and Privacy

effective political medium. Although universal Internet access is a distant and long-term goal, widespread use of a new and inexpensive communications medium has the potential to lead to unprecedented citizen participation in politics—but only if candidates and the electorate are given the statutory protections necessary to ensure the validity and integrity of this new resource.