What’s in a Name?: Predictably Regulating Cyberfraud to Protect the Democratic Political Process

ABSTRACT

In recent elections, political candidates have capitalized on the Internet as a central organizing resource. As a result of the low-cost, high-reward nature of campaign websites, some candidates have begun to register Web addresses—or domains—in opponents’ names in order to disrupt the democratic political process. Engaging in a practice known as cyberfraud, these individuals register for domains containing the candidate’s name, such as “firstnamelastname.com.” Then, instead of finding themselves on the candidate’s official campaign website, voters access a website operated by the candidate’s opponent that contains misleading or outright false information. Unfortunately, most political candidates have little recourse for such subversion of an informed voting process.

This Note analyzes the existing law’s failure to regulate cyberfraud in federal elections. Candidates may file trademark lawsuits or submit to the arbitration of the Internet Corporation for Assigned Names and Numbers (ICANN)—the body responsible for regulating Internet-related tasks, such as authorizing domain use. However, this Note explains why trademark law and its commerciality requirements are inadequate to protect against cyberfraud. While the US Congress could enact legislation specifically aimed at preventing cyberfraud, this Note argues that First Amendment concerns make this remedy unlikely. Finally, while California has provided a model for lessening the impact cyberfraud has on elections, the possibility of each state sufficiently and uniformly regulating cyberfraud is also unlikely. This Note proposes that, because of the obstacles presented by legislative remedies, the Federal Election Commission (FEC) should submit an application to ICANN’s new program expanding top-level domains (the “.com” or “.net” portion of the web address) to match the domain holder’s interests. With this system, the FEC may distribute official campaign websites to federal candidates in the form of “firstnamelastname.fec” and opponents may criticize candidates on
other websites that the public would know are not official sites of those candidates.

TABLE OF CONTENTS

I. BACKGROUND .................................................................................................................. 134
   A. Registering a Domain Name ......................................................................................... 135
   B. Federal Law and International Arbitration ................................................................. 136
      1. ICANN’s Uniform Domain-Name and Dispute-Resolution Policy ............................. 136
      2. Lanham Act ................................................................................................................ 139
      3. Cyberpiracy Protections for Individuals ................................................................. 142
   C. State Law ....................................................................................................................... 143
      1. California’s Experiments ............................................................................................ 143
         a. Political Cyberfraud Abatement Act ........................................................................ 144
         b. California Business and Professional Code ........................................................... 144
      2. Defamation .................................................................................................................. 145
   D. First Amendment Considerations ................................................................................. 146

II. ANALYSIS: FROM EXPANSION OF EXISTING LEGISLATION TO AGENCY DISTRIBUTION OF CAMPAIGN WEBSITES THROUGH NEW TECHNOLOGY ........................................... 147
   A. Expand Existing International and Federal Legislation to Cover Political Cyberfraud ................................................................................................................................. 147
   B. Enact Cyberfraud Legislation on the Federal and State Levels ..................................... 149
      1. The Political Cyberfraud Abatement Act as a Model: Expand to “firstname.lastname.com” ................................................................. 149
      2. The California Business and Professional Code as a Model ....................................... 151
      3. Problems with Enacting Legislation ........................................................................... 151
   C. Federal Government Application for the Creation of a New Top-Level Domain .......... 152

III. SOLUTION: WHERE LEGISLATIVE AND JUDICIAL REMEDIES FAIL, AGENCY DISTRIBUTION OF DOMAINS PROTECTS BOTH THE DEMOCRATIC POLITICAL PROCESS AND FREE SPEECH ............................................................... 156

IV. CONCLUSION .................................................................................................................. 158

Leading up to the last presidential election in 2008, millions of registered voters accessed “barackobama.com,” then-Senator Barack Obama’s campaign website, and “johnmccain.com,” Senator John
McCain’s campaign website. Republican candidates in the upcoming 2012 presidential election have largely followed suit, with four of the seven major candidates, including the two frontrunners, owning web addresses containing their full names. But it is not always easy for candidates to secure sites like these, which feature easy-to-remember web addresses based on each candidate’s first and last names. A survey by the Coalition Against Domain Name Abuse (CADNA) found that only 25 percent of domains that Congressional candidates used for their campaigns were owned by corresponding members of the House of Representatives or the Senate. CADNA studied three variations of politicians’ names that are most commonly associated with running for office with both “.com” and “.org” extensions. The highest rate of ownership was for “lastnameforsenate.com,” yet only 46 percent of Senators actually owned the domain corresponding to their names. CADNA contacted each US Congressman after the study, informing each about the use of the domain names he did not own. Presumably realizing that they may more effectively reach
donors and voters every two to six years with accessible websites within their own control, thirty-three Congressmen then registered eighty-two of the domain names that were still available.9

An accessible website is crucial to a presidential campaign.10 President Obama raised millions of dollars in small contributions through his campaign website with its memorable domain, “barackobama.com.”11 Most importantly, his website successfully energized those registered voters who normally lack enough interest in the political process to participate.12 While President Obama’s most fervent and tech-savvy supporters would likely be able to find campaign information—both organizational and ideological—no matter the name of the domain, a successful website aims itself at the undecided or less interested voters. Additionally, as voters become increasingly accustomed to campaign websites, even politicians in elections confined to a single state will utilize the Internet as an organizing resource.13 For instance, Senator Scott Brown, a Republican from Massachusetts, received nearly $14 million in last-minute contributions, most of which came from out-of-state donors.14 A website’s ability to reach millions of people across the nation simultaneously makes it a valuable resource for any campaign.

9. Id.
12. See David Carr, How Obama Tapped Into Social Networks’ Power, N.Y. TIMES, Nov. 9, 2008, http://www.nytimes.com/2008/11/10/business/media/10carr.html (“But Senator Barack Obama understood that you could use the Web to lower the cost of building a political brand, create a sense of connection and engagement, and dispense with the command and control method of governing to allow people to self-organize to do the work.”) (citations omitted).
13. See THE COAL. AGAINST DOMAIN NAME ABUSE, supra note 5 (noting that Congressmen who did not own the studied domain names that were still available registered for them after being informed of the study and its results).
Political candidates must capitalize on the Internet as a resource; but, in order to do so, their campaigns must first own domains that are both relevant to the candidate and memorable for the average citizen. This makes a domain containing the candidate’s full name, such as “barackobama.com,” a popular choice. Considering the number of years since the advent of the Internet, and the current, widespread use of it, registering a full-name domain could prove difficult. For instance, someone else may have already registered the particular domain a candidate wishes to use. Occasionally, the owner of the domain is not using the website, but reserving the name for profit—registering the name and hoping a politician will eventually be willing to purchase the domain from him for a hefty price. Known as “cybersquatting,” this action is partly regulated through trademark law by both the Lanham Act and the Internet Corporation for Assigned Names and Numbers’ (ICANN) Uniform Domain-Name and by Dispute-Resolution Policy (UDRP).

Unfortunately, because existing protections against cybersquatting contain a commerciality requirement, there are mixed results for politicians who file disputes. Only those politicians found to have a sufficiently commercial interest in a particular domain have secured the transfer of a web address from the cybersquatter to the campaign.

15. See Steve Friess, As Candidates Mull ’08, Web Sites Are Already Running, N.Y. TIMES, Nov. 18, 2006, http://www.nytimes.com/2006/11/18/us/politics/18domain.html (“[T]he more a domain name differs from a candidate’s name, the weaker the candidate’s case might be.”). But see Lipton, Hillary, supra note 10, at 64-65 (discussing Senator John Kerry’s campaign arbitration attempting to secure the domain name “kerryedwards.com” from an individual named “Kerry Edwards”).


18. Friess, supra note 15 (“But Mr. Treftz, who lives in Aurora, Ill., owns the domain name obama2008.org, and he thinks he will make a tidy profit if Mr. Obama’s campaign gets around to wanting it.”); see Lipton, Hillary, supra note 10, at 57-58.

19. Lanham Act, 15 U.S.C. §§ 1051-1141 (2006); Uniform Domain Name and Dispute Resolution Policy, INTERNET CORP. FOR ASSIGNED NAMES AND NOS., http://www.icann.org/en/udrp/udrp-policy-24oct99.htm (last visited Sept. 4, 2011); see Lipton, Hillary, supra note 10, at 57-59 (labeling “political cybersquatting” as the practice of “a registrant with no personal connection to a relevant name . . . register[ing] it in order to sell it for profit to the relevant politician or another person”).


However, a political opponent may register the domain to publicize information either harmful to a politician or supportive of himself. This action falls under the term “cyberfraud” because, despite any disclaimers on the website, a voter may believe the candidate bearing its domain name operates the site, rather than an opponent. Unlike cybersquatting, cyberfraud focuses on purely political gain rather than economic gain. While cybersquatting has been a problem in past elections, cyberfraud is the newest concern for politicians and their campaign websites. New Jersey Senator Robert Menendez and Jack Conway, former candidate for a Kentucky US Senate seat, had both seen websites in their names misappropriated in the 2010 midterm elections.

Because trademark law is tailored to regulate commercial disputes over domain names, it cannot provide relief for candidates who find themselves victims of political cyberfraud. Instead, candidates are left to pursue their complaints through state tort law, most commonly defamation, in their local courts. However, most defamation laws require burdens of proof too high for political cyberfraud victims because of their status as public figures, and jurisdictional restrictions may also prevent relief. Ownership of domain names thus becomes a race to the registrar; so candidates with unusual names, candidates who declare their intention to run
early on, and career politicians tend to have the advantage.\textsuperscript{31} Yet, a candidate should not gain an advantage by using a low-cost, high-reward political resource merely because his name is unique or because he has been in politics the longest—both Senator Daniel Inouye and Senator Mike Lee should have equal opportunity to utilize a full-name domain.\textsuperscript{32} Campaign website domains should be systematically regulated to allow voters easy access to non-misleading information while preventing a race to register a domain.\textsuperscript{33} Although such regulation raises a host of problems—particularly run-ins with the First Amendment—the Federal Election Committee (FEC) can take steps to protect the integrity of the democratic vote while preserving freedom of speech.\textsuperscript{34}

This Note will discuss a fictional scenario in which the reader will be asked to imagine that President Obama does not have access to “barackobama.com.” Instead of the Obama campaign registering the website, either a future opponent in the 2012 presidential campaign or a political detractor of President Obama controls the site. The site would contain information that is either misleading about, or detrimental to President Obama or that directly supports his opponent. Thus, during the course of the 2012 presidential election, President Obama’s official campaign website would be a variation of his full name—be it “obamaforpresident.com,” “barackobama.net,” or “barackobama2012.com.” No matter what he will choose for his official website, “barackobama.com” will still lead voters to information that is antithetical to President Obama’s goal to win the 2012 election. Although it is likely that incumbents will have access to their own full-name domains, this Note will nevertheless use the fraudulent registration of “barackobama.com” as an example of cyberfraud because of the website’s familiarity.

Part I of this Note provides background information on the process of registering a domain. It examines the international,
federal, and state regulations of cybersquatting, including where political cyberfraud is overlooked. Part II analyzes the possible solutions to balance three interests—voters’ access to accurate and non-misleading information, citizens’ First Amendment rights, and administrators’ ease of implementation. Part III proposes a solution to cyberfraud in the political context: creating a new top-level domain for federal election candidates.

I. BACKGROUND

International, federal, and state laws fail to provide an adequate or practical remedy for cyberfraud. If a potential voter in the 2012 presidential election visits “barackobama.com,” he will reasonably expect to find himself on a page regulated by President Obama’s political staff that contains information relevant to his candidacy, such as his platform, donation bank, and campaign stops. If that voter instead finds content about the Republican nominee’s candidacy or content critical of President Obama, whether truthful or not, the democratic political process would be impaired. Such impairment happens particularly if that voter believes the Obama campaign operates the misleading website or if the misleading website prevents the voter from taking additional steps to find the Obama campaign’s actual website. In either case, the Obama campaign may lose a donor or a volunteer. Most importantly, though, if the voter does not take further steps to find President Obama’s official website, the cyberfrauder has prevented open access to his opponent’s ideas. Consequently, the democratic political process may lose an informed vote.

In this scenario, if the Obama campaign wants to dispute the rights to “barackobama.com,” traditionally, it would file a complaint with one of ICANN’s trademark-regulating arbitrators under the UDRP. However, if the Obama campaign’s complaint with the unauthorized website was instead content based, the campaign would file a defamation action in a local court. Yet neither situation would

35. See discussion infra Part I.B-C.
36. Lipton notes that the assumption that the Obama campaign controls “barackobama.com” parallels an assumption in trademark law that Target controls “target.com.” See Lipton, Hillary, supra note 10, at 93 (discussing developments in commercial trademark law that assumes “trademark.com” belongs to the relevant trademark holder). This Note, nonetheless, argues that the overarching objectives of trademark law, with its concern for monetary value, are incompatible to effectively regulate political cyberfraud.
37. See Lipton, Hillary, supra note 10, at 62-63.
38. See id. at 75.
provide complete and predictable regulation of a full-name domain in
the political context.\textsuperscript{39}

A. Registering a Domain Name

ICANN administers the registration process for domain
names.\textsuperscript{40} ICANN is a global, private entity created by a partnership
agreement with the US Department of Commerce, which, in turn,
accredits and oversees particular registrars located in various
countries.\textsuperscript{41} All of these registrars act as middlemen and operate on a
first-come, first-served basis.\textsuperscript{42} Because of the need for unique and
individual domains, once a user registers a name, it is deemed taken.\textsuperscript{43}
The registrar prohibits the next would-be registrant from using that
particular domain.\textsuperscript{44} Because the fee to register the domain is
moderately low, a would-be registrant’s only obstacle is the required
uniqueness.\textsuperscript{45} The registrars do not perform inquiries into the
registrant’s right to use a specific character combination,\textsuperscript{46} but ICANN
itself has set up a procedure for the mandatory arbitration of disputes
that the registration agreement requires.\textsuperscript{47}

The first aspect of a domain is the top-level domain, the “.com
component of “barackobama.com.”\textsuperscript{48} The most common are “.com,”
“.org,” and “.net.”\textsuperscript{49} ICANN is responsible for maintaining the current
top-level domains and issuing new ones.\textsuperscript{50} The other component of the
domain is the second-level domain, which is the “barackobama”
portion of “barackobama.com.”\textsuperscript{51} Both the top- and second-levels are
equally important in the political context this Note examines. For
instance, if “barackobama.com” had been taken when the Obama

\begin{thebibliography}{9}
\bibitem{39} See discussion \textit{infra} Part I.B-C.
\bibitem{40} \textit{Factsheet, supra} note 17.
\bibitem{41} Id.
\bibitem{42} Id.
\bibitem{43} Id.
\bibitem{44} Tamarah Belczyk, \textit{Note, Domain Names: The Special Case of Personal Names}, 82 B.U. L. REV. 485, 492 ("There are few qualifications other than uniqueness.").
\bibitem{45} Id.; \textit{Friess, supra} note 15 ("Registering a domain name is simple and costs about $10
a year.").
\bibitem{46} Belczyk, \textit{supra} note 44.
\bibitem{47} Lipton, \textit{Hillary, supra} note 10, at 61-62.
\bibitem{48} Jacqueline D. Lipton, \textit{Beyond Cybersquatting: Taking Domain Name Disputes Past
Trademark Policy}, 40 WAKE FOREST L. REV. 1361, 1367-68 (2005) [hereinafter Lipton,
Cybersquatting].
\bibitem{49} Id. None of these top-level domains are tied to any particular geographical location,
as opposed to “.uk” for the United Kingdom, “.ca” for Canada, and “.fr” for France. Other top-level
domains include “.edu” and “.gov.” \textit{See id.} at 1368.
\bibitem{50} \textit{See id.}
\bibitem{51} \textit{See Belczyk, supra} note 44, at 489.
\end{thebibliography}
campaign undertook to register its website, the campaign then could have attempted to register not only “obamabiden.com” or “obama.com,” but also “barackobama.net.” But, because “.com” is the most well-known of the top-level domains, a politician will more likely want access to “firstname.lastname.com,” rather than “firstname.lastname.net.” Moreover, depending on the content provided on the already-registered site, the politician may not want the “.net” version in order to avoid confusion with the “.com” site. That is, if President Obama’s political opponent used “barackobama.com” to put forth information that the Obama campaign deems detrimental, the Obama campaign may be reluctant to register “barackobama.net,” as potential voters may confuse the two due to the popularity of “.com” websites.

B. Federal Law and International Arbitration

Both federal legislators and ICANN have implemented measures to regulate disputes affecting the registration of a domain. The federal Lanham Act defines a trademark and sets out the factors for the judicial system to weigh when a plaintiff claims his trademark rights have been violated. Moreover, ICANN requires those who register for a domain to settle trademark disputes through arbitration. Both the federal and international effort to resolve these disputes are grounded in trademark law, which emphasizes a commercial interest in a domain.

1. ICANN’s Uniform Domain-Name and Dispute-Resolution Policy

ICANN’s Internet regulation is significant because every party wishing to own a domain must apply through a registrar and sign a contract that mandates the use of the UDRP arbitration policy whenever there is a dispute over the domain ownership. ICANN’s jurisdiction is international, despite existing alongside federal trademark legislation and despite the organization being created through a joint agreement with the US Department of Commerce. Because of these factors, the UDRP has overshadowed the Lanham Act, making the UDRP the most recognizable—not to mention most

52. Factsheet, supra note 17.
53. See id.
55. Lipton, Hillary, supra note 10, at 61-63.
56. Id.
57. Id.
efficient and cost-effective—way to resolve a domain dispute. All of these arbitrations take place between a current trademark holder and a non-trademark holder, with the non-trademark holder having access to the domain instead of the trademark owner. A successful plaintiff in a UDRP arbitration must show (1) that the non-trademark holder’s mark is identical or misleadingly similar to its own trademark, (2) that the non-trademark holder has no legitimate rights or interests in the trademark it is using, and (3) that the non-trademark holder is acting in bad faith.

ICANN’s UDRP suffers from several flaws when considered in the political cyberfraud context. Most importantly, the UDRP has no explicit provision for individual names. While individuals have seen the successful transfer of their personal name domains, most of these cases have involved celebrities, whose commercial interests lie in the public recognizing their names as brands. In one of the few cases involving politicians, Kathleen Kennedy Townsend’s name was unprotected under the UDRP because her name had not been infringed upon commercially. In fact, it did not matter that she had been a candidate in the gubernatorial election in Maryland; a politician’s name is outside the scope of the UDRP if it is not connected with commercial exploitation. Thus, the fact that President Obama is a widely recognized political figure will have no bearing on a trademark infringement analysis under the UDRP if there is no threat to commerciality.

Nevertheless, in 2005, then-Senator Hillary Clinton was successful in securing the transfer of the domain “hillaryclinton.com” for use in her political campaign. Senator Clinton was able to establish a trademark interest in her name because of her book sales;

58. \textit{Id.}
59. \textit{Id.}
60. \textit{Uniform Domain Name and Dispute Resolution Policy, supra note 19.}
61. \textit{Lipton, supra note 10, at 61-63.}
62. \textit{Id.}
63. \textit{Id.}
65. \textit{Id.}
66. \textit{See id. The case, nonetheless, does not close the door to political parties filing complaints under the UDRP. See id. (“Here, the claim for the domain names is brought by the individual politician, and not by the political action committee actively engaged in the raising of funds and promotion of Complainant’s possible campaign. Had the claim been brought in the name of the Friends of Kathleen Kennedy Townsend, the result might well have been different. But it was not.”).}
she had written four best-sellers at that time.\textsuperscript{68} In the same respect, the UDRP may find that President Obama’s name is a trademark because of his success as an author.\textsuperscript{69} Given potential presidential candidates’ tendencies to author autobiographies,\textsuperscript{70} reliance on such a scheme will tilt the system in favor of incumbents and career politicians.

Moreover, although the UDRP arbitrators have been willing to recognize unregistered names as trademarks, they are less likely to do so where the name has only a regional impact.\textsuperscript{71} For example, when Bruce Springsteen, a popular American singer in the 1970s and 1980s, sought to secure the transfer of “springsteen.com,” the arbitrators suggested—before deciding the case on other grounds—that his name was not well-known enough to support a trademark interest.\textsuperscript{72} So even if President Obama’s book deals moved his case past the commerciality obstacle, he still would not secure the transfer of “barackobama.com” if an arbitrator found that he was not famous enough.\textsuperscript{73} While this is inconceivable as applied to President Obama, it could be the case for a politician like Christine O’Donnell, who ran in and lost the election for Vice President Joe Biden’s old Senate seat in Delaware.\textsuperscript{74} Although running in an election with a relatively small voter pool,\textsuperscript{75} O’Donnell became well-known for past comments that resurfaced during the election, and she has since signed a book deal.\textsuperscript{76}

\textsuperscript{68} Id.
\textsuperscript{69} See id.
\textsuperscript{70} See Gail Collins, \textit{Presidential Primary Book Club}, N.Y. TIMES, Jan. 14, 2011, http://www.nytimes.com/2011/01/15/opinion/15collins.html (“This is the time when presidential candidates start poking their little noses up through the snow, and making soft, trilling noises. I know you think it’s too soon, even though Mitt Romney made his intentions clear on the family Christmas card. But as a public service, I am going to start providing summaries of the latest books from the potential Republican nominees so we’ll all be well educated by the time the debates begin.”).
\textsuperscript{76} Book Deal, supra note 74 (“Backed by Sarah Palin, O’Donnell was a surprise winner in the GOP primary, but was widely ridiculed for lack of experience and for past comments,
O'Donnell is not as well-known as President Obama, and it would be difficult to determine where an arbitration panel would draw the line when weighing regional impact with book deals.\(^77\)

Recognition of unregistered trademarks would have an important impact not only in congressional elections, but also in presidential elections. Lesser-known candidates seeking the Republican nomination in 2012, such as Rick Santorum, former Pennsylvania senator, or Jon Huntsman, former Utah governor and President Obama’s former ambassador to China, may not be famous enough for protection under the UDRP.\(^78\) Moreover, although these candidates have been heavily involved in politics, UDRP arbitration may still make an unfair distinction between these lesser known candidates and political forces such as Mitt Romney, governor of Massachusetts, and Rick Perry, governor of Texas.\(^79\)

2. Lanham Act

Congress enacted the Lanham Act in 1946 to demarcate federal regulation of US trademarks and to specify remedies for trademark infringement or dilution.\(^80\) A 1999 amendment added the Anticybersquatting Consumer Protection Act (ACPA).\(^81\) The ACPA provides that a defendant infringes a trademark if the plaintiff can show that the defendant used the plaintiff’s trademarked domain name, or one confusingly similar, in bad faith to profit from it.\(^82\) Alternatively, a plaintiff can prove a defendant diluted his trademark.\(^83\) Dilution does not require confusion, but the doctrine is limited in scope and protects only famous marks.\(^84\) Courts may look to the following factors to determine whether the mark is famous: (1) the duration and extent of use of the trademark, (2) the duration and


\(^82\) Id.

\(^83\) Id.

\(^84\) Id.; see Jacqueline D. Lipton, Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property, and Restitution, 23 HARV. J.L. & TECH. 447, 451 (2010) [hereinafter Lipton, Bad Faith].
extent of advertising for the trademark, (3) the geographic area where the trademark has been used, (4) the distinctiveness of the trademark (either through the trademark itself or through acquired distinctiveness), (5) the recognition of the trademark, (6) the distribution and marketing method of the trademark’s product, (7) third parties’ use of the trademark, and (8) whether the trademark was federally registered.\(^8\) Further, the act of dilution consists of either blurring or tarnishment.\(^8\) Blurring arises when there is a similar mark that “impairs the distinctiveness of the famous mark,”\(^8\) whereas tarnishment hinges on the similarity of the two marks “harm[ing] the reputation of the famous mark.”\(^8\) While its jurisdiction is limited to bad faith infringers—a determination made by consulting the Act’s nine bad faith factors\(^9\)—the Act does provide civil liability for the misuse of some individual names.\(^9\)

However, the Act’s most significant restriction is a commercial one.\(^9\) The infringer of the trademark must have been seeking to profit monetarily from its use.\(^9\) While this restriction might still render the Act applicable to cybersquatting, it actually excludes cyberfraud.\(^9\) With cyberfraud, the only profit in an electoral context...
is political capital, rather than monetary gain.\textsuperscript{94} If the wrongful owner of “barackobama.com” were using the website to gather campaign donations (donations for President Obama’s political opponent, presumably), President Obama might argue that this is sufficient to show intent to profit from the site.\textsuperscript{95} However, a court will likely construe the manner and intention of profiting narrowly pursuant to Congress’ intent in drafting the statute—that is, “profit” must be the end game, not the means to an end, as in the Obama example.\textsuperscript{96} Even if President Obama were successful in this argument, not all courts would be willing to apply it as such.\textsuperscript{97} Additionally, the Act still would not cover those political opponents who seek to gain purely political points against President Obama.\textsuperscript{98} Nor would it cover President Obama’s political detractors, who may “profit” only by having their candidate—one other than President Obama—win the election.\textsuperscript{99}

Assuming President Obama, or any other political candidate plaintiff, were able to surpass the profit hurdle, the requirement that the infringed-upon name be a famous mark poses difficulties for most plaintiffs that are similar to those of ICANN’s UDRP.\textsuperscript{100}

distract the voter from a candidate’s actual website entirely, the bad faith requirement is not as substantial an obstacle as it is in political cybersquatting. See id. at 64 (citing the “kerryedwards.com” case, where the name was not initially registered in order to profit and was the defendant’s actual name, as opposed to an amalgamation of the Presidential and Vice Presidential candidates’ names).

\textsuperscript{94} See id. at 92-93.

\textsuperscript{95} See 15 U.S.C. § 1125(d) (requiring the owner of the mark to prove the person wrongfully using the mark has a “bad faith intent to profit” from that mark).

\textsuperscript{96} H.R. REP. NO. 109-23, at 3 (2006), reprinted in 2006 U.S.C.C.A.N. 1091, 1092 (“Trademark law ‘identifies’ goods and services. When an individual encounters a mark (e.g., a word or symbol) in a store or watching a commercial, he or she can develop an association between a product or service and its corresponding quality, brand reputation, or origin. Generally, a trademark consists of the name or logo of a product. For example, the restaurant chain McDonald’s has trademarks in its name, its golden arches logo, and other marks associated with its business. In addition, trademark law also may protect the distinctive features of a product’s packaging. Examples of famous and distinctive packaging include the shape of Coca-Cola’s bottle or Tiffany’s little blue jewelry box.”).

\textsuperscript{97} See Lipton, Hillary, supra note 10, at 95-96.


\textsuperscript{99} See id.

\textsuperscript{100} See discussion infra Part II.B.3 (noting that many political candidates are only well known in a small, regional area which is insufficient for the celebrity requirement).
3. Cyberpiracy Protections for Individuals

The US Code does protect some non-trademarked names from infringement in 15 U.S.C. § 8131, but the statute is geared primarily toward cybersquatting.\textsuperscript{101} Such coverage of non-trademarked names may indicate a regulatory rationale based on more than the commerciality concerns of trademark law;\textsuperscript{102} nonetheless, the law aims only to prevent the infringers from profiting financially.\textsuperscript{103} Like ICANN’s UDRP, though, it does include a provision for the transfer of the domain to the plaintiff upon successful suit—the remedy the Obama campaign seeks against the wrongful owner of “barackobama.com.”\textsuperscript{104}

In order to be liable under § 8131, the infringer must intend to sell the plaintiff’s full-name domain (or a similarly confusing one) for financial gain without the consent of the owner.\textsuperscript{105} This provision involves commerciality similar to the Lanham Act and ACPA, but here the profit is specifically confined to selling the domain.\textsuperscript{106} In this Note’s fictional Obama campaign scenario, as the wrongful owners of the site that intentionally posted misleading information about Obama, cyberfrauders would not be liable. On the other hand, any individual who bought the domain name intending to subsequently sell it to President Obama’s detractors might be found culpable for cybersquatting.\textsuperscript{107} Meanwhile, the cybersquatter has committed an inherently different violation than the cyberfrauder. The cybersquatter intends to impair the political process solely for monetary profit; any effect on the political process is an unintentional byproduct.\textsuperscript{108} The cyberfrauder, on the other hand, intends to throw a wrench in the political process—his goal is to sway voters.\textsuperscript{109}

Under the Lanham Act, a plaintiff may want to argue that the offender is profiting through campaign donations or profiting in a

\textsuperscript{101} 15 U.S.C. § 8131.

\textsuperscript{102} See Lipton, Bad Faith, supra note 84 (suggesting a restitutionary, unjust enrichment rationale as the driving force of the ACPA).

\textsuperscript{103} See Lipton, Hillary, supra note 10, at 106 (arguing that the infringer must have had the bad faith intent to sell the domain name).

\textsuperscript{104} 15 U.S.C. § 8131(2).

\textsuperscript{105} See Ficker v. Tuohy, 305 F. Supp. 2d 569, 572 (D. Md. 2004) (“The Court is not convinced, at this point, that the ACPA provides coverage for personal names that are not trademarked, where the websites have no commercial use.”).

\textsuperscript{106} Lipton, Hillary, supra note 10, at 106.

\textsuperscript{107} See id.

\textsuperscript{108} See Lipton, Hillary, supra note 10, at 85 (“Unlike a person engaging in political cyberfraud, by definition, a political cybersquatter is trying to make a profit from the registration of the name without actually disseminating any particular message to voters.”).

\textsuperscript{109} See sources cited supra note 25.
political sense. But this argument will fail because political, rather than monetary, profit is inconsistent with Congress’s statutory intention and with the definition of cybersquatting: selling domains for profit. For instance, the Fourth Circuit rejected an ACPA claim where the defendants had posted a message on a domain based on the plaintiff’s name, “bernardjcarl.com,” and then alleged that the plaintiff owed them money for services performed. The court held that “while the defendants may have been attempting to profit, they did not do so in the means specified in the statute.” The defendants here hoped to profit by receiving money the plaintiff owed them, rather than by selling the domain for a profit, as the statute requires.

C. State Law

Because both federal law and international arbitration schemes are concerned primarily with commerciality, resulting in more successful adjudication for corporations and celebrities, politicians seeking recourse in a domain dispute may turn to state law. On the whole, however, such a patchwork scheme may prove unsatisfactory to a plaintiff due to jurisdictional issues.

1. California’s Experiments

California, taking the lead position among states, has recognized the need for cyberfraud regulation. Enacting the Political Cyberfraud Abatement Act (PCAA) and amending its Business and Professional Code, California provided means for individuals to protect an interest in their names on the Internet. However, personal jurisdiction concerns restrict the availability of this remedy across the nation.

111. Id. at 630.
112. Id.
113. Id.
114. See Lipton, Hillary, supra note 10, at 93.
115. See discussion infra I.C.1.a.
116. See Lipton, Hillary, supra note 10, at 98.
117. CAL. BUS. & PROF. CODE § 17525 (West 2010); CAL. ELEC. CODE § 18320(c)(1) (West 2010).
118. See discussion infra I.C.1.a.
a. Political Cyberfraud Abatement Act

The PCAA prohibits three types of conduct concerning a political website. One may be liable for political cyberfraud if he (1) intends “to deny a person access to a political Web site,” (2) denies “a person the opportunity to register a domain name for a political Web site,” or (3) causes “a person reasonably to believe that a political Web site has been posted by a person other than” the person who posted it. However, the Act currently applies only to websites dealing with state ballot measures. Politicians seeking access to their full-name domain for campaign purposes will likely be unsuccessful in this route. Moreover, because of personal jurisdiction restrictions, the Act’s applicability would seemingly be limited to those politicians with constituents in the state of California; that is, those politicians the California legislature contemplated when authoring this provision. Even so, courts applying the Act may find the PCAA was not meant to regulate registrars and registrants outside California, even if the politician and constituents are in state. Thus, even if this provision applied to general campaign websites, a California court may find that President Obama, an out-of-state defendant who registered the domain on an out-of-state registrar, does not have sufficient contacts with the state of California.

b. California Business and Professional Code

Soon after the enactment of the ACPA, California also amended its Business and Professional Code. Similar to the ACPA, the Code prohibits bad faith registration and use of another person’s name—or one confusingly similar—in a domain name. The Code seems broader than the ACPA with regard to the misuse of personal names in two ways: (1) it applies both to living and deceased

119. CAL. ELEC. CODE § 18320(c)(1) (West 2010).
120. Id.
121. Id.
122. See Lipton, Hillary, supra note 10, at 99-101.
123. Id.
124. Id.
125. See id. at 73-74 (noting caselaw that holds that merely maintaining a website, without directing it toward the state, is insufficient to constitute minimum contacts that comport with fair play and substantial justice).
127. CAL. BUS. & PROF. CODE § 17525 (West 2010).
128. See 4 J. THOMAS McCArTHY, McCArTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:81, at n.2 (2011) (citing the author of the bill, Senator Burton, in stating that the Act protected all personal names, rather than only famous names, as with the federal law).
persons and (2) it offers more than one way for a person to qualify as a bad actor.\textsuperscript{129} Obviously, the Code’s application to deceased persons is not helpful in the political context. However, the broader definition of “bad faith actor” includes one who intended “to mislead, deceive, or defraud voters.”\textsuperscript{130} Thus, a plaintiff suing under this code need not prove intent to profit as he would if he were suing under the Lanham Act.\textsuperscript{131} Like the state’s PCAA, though, personal jurisdiction restrictions will arise for those seeking redress under this statute.\textsuperscript{132}

2. Defamation

Another state-law route for a politician who is a cyberfraud victim is to sue for defamation.\textsuperscript{133} The tort of defamation operates on a theory that false statements “interfere with the truth-seeking function of the marketplace of ideas.”\textsuperscript{134} Nevertheless, a plaintiff who is a public figure will not prevail unless he can show the defendant acted with “actual malice”; that is, that the content on the website was made “with knowledge that it was false or with reckless disregard of whether it was false or not.”\textsuperscript{135} First Amendment protections of speech criticizing public figures make this standard more difficult to prove than the bad faith actor standard of California’s Business and

\begin{footnotesize}
\textsuperscript{129} CAL BUS. \& PROF. CODE § 17526 (West 2010) (‘‘[A] court may consider factors, including, but not limited to, the following: (a) The trademark or other intellectual property rights of the person alleged to be in violation . . . in the domain name. (b) The extent to which the domain name consists of the legal name of the person alleged to be in violation . . . . (c) The prior use . . . by the person alleged to be in violation . . . in connection with the bona fide offering of any goods or services. (d) The legitimate noncommercial or fair use of the person’s . . . name . . . in an Internet Web site accessible under the domain name by the person alleged to be in violation . . . . (e) The intent of a person alleged to be in violation . . . to divert consumers . . . to a site accessible under the domain name that could harm the goodwill represented by the person’s . . . name either for commercial gain or with the intent to tarnish or disparage . . . the person’s . . . name . . . by creating a likelihood of confusion as to the source . . . of the site. (f) The offer by a person alleged to be in violation . . . to transfer, sell, or otherwise assign the domain name to the rightful owner . . . for substantial consideration without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services. (g) The intentional provision by the person alleged to be in violation . . . of material and misleading false contact information when applying for the registration of the domain name. (h) The registration or acquisition by the person alleged to be in violation . . . of multiple domain names that are identical or confusingly similar to names of other . . . personalities. (i) Whether the person alleged to be in violation . . . sought or obtained consent from the rightful owner to register, traffic in, or use the domain name. (j) The intent of a person alleged to be in violation . . . to mislead, deceive, or defraud voters.’’).

\textsuperscript{130} See id.

\textsuperscript{131} MCCARTHY, supra note 128.

\textsuperscript{132} Lipton, Hillary, supra note 10, at 73-74.

\textsuperscript{133} Id. at 75.


\textsuperscript{135} Id. (citing N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964)).
\end{footnotesize}
Professional Code. Although protecting the truth-seeking function would be important as voters pursue factual information about a candidate, politicians, being public figures, will nevertheless have to prove that the offender met the “actual malice standard.” Even if a politician were able to meet this standard, the remedy will likely consist of damages or an injunction against posting the defamatory content, and would not include turning over the domain to the politician. Thus, even if President Obama made a successful defamation claim against the wrongful owner of “barackobama.com,” the court would not require the wrongful owner to hand over the website, allowing the owner to continue to deprive the Obama campaign of his full-name domain.

D. First Amendment Considerations

Because of the protection that political speech enjoys under the First Amendment of the Constitution, legislative enforcement mechanisms are unlikely to be enacted successfully. Legislators will be unwilling to pass laws that seemingly violate the First Amendment, and, even if they did, close scrutiny of such laws may result in the court striking them down. Speech in the political sphere enjoys the highest form of protection “in order to assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people.” Candidates campaigning in the public sphere necessarily invite criticism; it is essential in maintaining “the spirit of healthy democracy in this country.” The First Amendment protects, even encourages, political speech that criticizes public officials. Thus, critics of cyberfraud regulation will

---

139. See id.
140. See Buckley v. Valeo, 424 U.S. 1, 14 (1976).
143. Ficker v. Tuohy, 305 F. Supp. 2d 569, 572 (D. Md. 2004) (weighing the public’s interest in “maintaining the fairness and integrity of the electoral process” with the defendant’s First Amendment rights and, in the end, denying the injunction to prohibit the defendant’s use of a domain name).
144. Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 51 (1988) (“The sort of robust political debate encouraged by the First Amendment is bound to produce speech that is critical of
argue against it based on First Amendment concerns. They may say that prohibiting cyberfraud promotes some forms of political speech over others; that is, the content of the Obama campaign’s website over that of the wrongful owner’s website.

II. ANALYSIS: FROM EXPANSION OF EXISTING LEGISLATION TO AGENCY DISTRIBUTION OF CAMPAIGN WEBSITES THROUGH NEW TECHNOLOGY

Several possible solutions exist to regulate cyberfraud in order to promote active and informed voting in federal elections, but agency action would be the most effective. First, the US Congress could expand existing trademark law to prevent cyberfraud or enact a new cyberfraud provision outright. In the alternative, states could be encouraged to follow California’s lead and enact their own cyberfraud laws. However, these legislative solutions are unlikely to be successful. First Amendment concerns provide a substantial hurdle to any federal legislation; politicians will be unwilling to risk earning a reputation as anti-free speech in order to expand existing trademark law, much less to enact a highly publicized new law against cyberfraud. State action faces an additional issue: securing each state’s participation in the campaign against cyberfraud to implement a nationally uniform system. In light of these obstacles, agency action by the FEC emerges as the most effective route. Under ICANN’s new application procedure, the FEC, acting as a registrar, may ask ICANN to issue a new top-level domain so that the FEC may distribute domains to federal political candidates. This Note will first examine other solutions and show why they are inadequate before demonstrating why agency action by the FEC is the best solution.

A. Expand Existing International and Federal Legislation to Cover Political Cyberfraud

One way to remedy the current state of the law would be to expand the UDRP, the Lanham Act, and § 8131 to cover all instances of political cyberfraud. Yet, Congress would have to excise the commerciality requirement from these statutes so that more names that hold public office or those public figures who are ‘intimately involved in the resolution of important public questions . . . ”) (citations omitted).

145. See Freiss, supra note 15 (“Political speech is really tough to make improper. . . . Well, this is a great name, and I’m going to put up a pro-Republican Web site on barackobama2008.com. ‘It’s political speech. Is that inappropriate?’”).

146. See id. (“Christine Jones, a lawyer for GoDaddy.com, one of the largest domain registration services, noted that some uses of domain names could be legitimate free speech.”).

147. See discussion infra Part II.B.3.
could qualify for unregistered trademark status. But without such a requirement, UDRP arbitration panels and local courts would be left only with trademark law’s most arbitrary and subjective standard: whether the plaintiff is “famous” enough.\textsuperscript{148}

If left with the celebrity requirement alone, candidates running for president are the most likely individuals to be able to obtain an unregistered trademarked name because they are usually nationally known politicians. Whether this would apply to all presidential candidates or merely to the two nominees of the major parties is a tougher question. Moreover, the applicability to candidates who have yet to win the party nomination, or have yet declared a formal intention to run despite the general public’s familiarity with the potential primary candidate, is also unclear. Hillary Clinton, who saw the successful transfer of her full-name domain,\textsuperscript{149} was, at the time of the Democratic primary elections, arguably more well known than then-Senator Obama. His website was certainly as instrumental in securing his primary election victory as it was in the general election.\textsuperscript{150} The Republican candidates’ websites may play similar key roles in the 2012 presidential election. Godfather’s Pizza CEO Herman Cain’s rise to fame has occurred only recently.\textsuperscript{151} Cain’s ability to host a campaign website as equally accessible as that of Mitt Romney and Rick Perry—long-standing party leaders—should not depend upon when he starts to realize success within the party.

In any event, drawing a line at presidential candidates seems arbitrary. Former House Speaker Nancy Pelosi and Senate Majority Leader Harry Reid are both well known, and, for that reason, opponents targeted them specifically during the 2010 midterm elections.\textsuperscript{152} Would the test for whether a politician’s name qualifies

\begin{references}
\item 150. See Alexovich, \textit{supra} note 11 (noting that “barackobama.com” boasted over 1 million contributors as of 12:34 p.m. on Feb. 27, while Hillary Clinton’s campaign did not have as many); Carr, \textit{supra} note 12 (“Instead, by bolting together social networking applications under the banner of a movement, they created an unforeseen force to raise money, organize locally, fight smear campaigns and get out the vote that helped them topple the Clinton machine . . . .”).
\item 152. See Lacey, \textit{supra} note 4. While Nancy Pelosi was not a victim of cyberfraud, “more than $65 million was spent on 161,203 ads that targeted Pelosi.” Paul Steinhauser and Abby
as an unregistered trademark put more emphasis on whether the election is local or national? Or would the test be one of reputation on a national scale? The uncertainty in applying the celebrity standard for unregistered trademarks in the political context shows that trademark law as it now stands is a poor way to regulate political trademarks and would give an unfair advantage to incumbents and career politicians.

The UDRP, however, is more uniform than the Lanham Act and § 8131, which would have varying interpretations of the law among jurisdictions. Nevertheless, the global scale of the UDRP makes it an undesirable way to resolve political domain disputes. The United States alone has an interest in the effectiveness of our democratic process, and international UDRP arbitrators may not fully appreciate the necessity for equal footing for all candidates when it comes to registering a domain name.

**B. Enact Cyberfraud Legislation on the Federal and State Levels**

While California has made significant strides in preventing political cyberfraud, remedies in California alone are insufficient to regulate the widespread nature of the political cyberfraud problem. Congress could model federal legislation after California’s statutes, or the federal government and voters could encourage states to adopt measures similar to the ones California has implemented. If the PCAA or the Business and Professional Code were to serve as a model for legislation, modifications will be necessary to ensure that politicians have access to “firstnamelastname.com” and that the Supreme Court will not overturn the provision for First Amendment violations.

1. The Political Cyberfraud Abatement Act as a Model: Expand to “firstnamelastname.com”

First, if federal or state governments were to use the PCAA as a model, their legislatures would need to expand the Act to include “firstnamelastname.com” domains. Assuming the subsequent legislation would contain similar subsections, subsection (A), which

153. See generally Lipton, Hillary, supra note 10.
154. See generally id.
155. See id.
156. See CAL. BUS. & PROF. CODE § 17525-17527 (West 2010); CAL. ELEC. CODE § 18320(c)(1) (West 2010).
prohibits anyone from denying a person—here, the politician—access to a political website, is useful to ensure a politician’s access to his full-name domain. However, the strictness with which the courts construe this provision depends on which part of the domain they find more important both to politicians and the voters. Because this Note is primarily concerned with each politician having access to his full-name domain to use as a website, the author promotes a statute that would protect President Obama’s interest in the “barackobama” portion of the domain rather than ensuring he had access to a “.com” website containing a variation of his name. But it is conceivable that a court would find that “obama.com,” “obama2012.com,” or “obamabiden.com” is just as useful for campaigning as “barackobama.com.” Without clarification, the law would fail to ensure that each jurisdiction—either various states or federal districts—equally protects President Obama’s interest in his full name, thus leaving uniformity lacking. If left to the courts, the Obama campaign may have a successful suit in New York but not in Texas. Besides leading to forum shopping, an unclear statute poorly protects all politicians: Candidates unable to sue in New York, or those states willing to protect a full name, will be at a disadvantage.

Yet the inquiry does not end there. Would a court still find that President Obama was denied access to a political website if, although he could not register “barackobama.com,” “barackobama.net” were still available? “Barackobama.net” might still be undesirable, both because of the popularity of “.com” websites and because potential voters might confuse that site with “barackobama.com,” still being run fraudulently by Obama opponents.

Subsection (C) of the PCAA is the most useful of the three subsections in regulating cyberfraud, as it prohibits the registration and use of a website including a politician’s name in order to mislead the voting public about him and his platform. This approach has the potential to serve as a model for other state legislatures, but the judiciary may face subjective difficulties in determining whether the defendant intended to mislead the website’s viewers. Because the speech is political in nature, the subjective regulation of it may prove untenable, as is the case with regulating protected political speech.

158. See Lipton, Hillary, supra note 10, at 100-01.
159. See id.
160. See discussion supra Part I.A.
161. See Lipton, Hillary, supra note 10, at 99-100.
162. See id.
163. See id.
While it is possible to raise the standard of proof to one like the actual malice standard in defamation cases, this burden would not find liable those cyberfrauders who maintain websites with sufficiently truthful, but still detrimental, content in a candidate’s name.\footnote{164}{See Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 52 (1988) (citing N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964)).}

Moreover, a law modeled after subsection (C) will not necessarily result in President Obama’s access to “barackobama.com.” His political detractors may still register the domain and simply refrain from posting information on it. Seeing the value in holding the domain so that President Obama may not use it, his political opponents effectively block the Obama campaign from utilizing an easily accessible political resource, one in which the campaign could maximize its visibility. This is different from traditional cybersquatting because President Obama’s opponents will not attempt to sell the domain for a monetary profit. Thus, a law modeled after the PCAA will need to include a provision for the transfer of the domain.

2. The California Business and Professional Code as a Model

Rather than expanding the PCAA to cover “firstnamelastname.com” domains, federal and state legislatures could enact a statute like the California Business and Professional Code. Yet, judges will face particular difficulty in determining bad faith violations. Such a subjective inquiry could result in the US Supreme Court overturning the legislation for content regulation of free, political speech.\footnote{165}{See Mills v. Alabama, 384 U.S. 214, 218 (1966); Ficker v. Tuohy, 305 F. Supp. 2d 569, 572 (D. Md. 2004).} Again, legislatures could raise the burden of proof to one resembling the actual malice standard, but such a standard leaves a loophole in cyberfraud law, allowing infringers who do not knowingly publish false information to evade regulation.\footnote{166}{See Hustler, 485 U.S. at 52 (citing N.Y. Times Co., 376 U.S. at 279-80).}

3. Problems with Enacting Legislation

Federal legislation seems to be the easiest choice, as it would provide a uniform system for the entire nation. One benefit of state action is that it ensures that the resolutions of political domain disputes are locally contained, which weigh the candidates’ specific interests most accurately; however, there is no guarantee that each state would be willing to enact such legislation. This would leave some candidates protected against cyberfraud and others not. But
even relying on the US Congress to regulate political cyberfraud risks lengthy delays or that the regulation may never occur. With such a hot-button issue like the First Amendment on the line for politicians, legislation may be interminably delayed in the lawmaking process. The political capital that either US Congressmen or the executive branch (assuming support of the legislation) must expend when the legislation’s critics complain of interference with elections and hindrance of First Amendment rights will make this remedy unlikely.

Moreover, federal legislators may face difficulties in tailoring the law to avoid First Amendment complications and eventual invalidation of the legislation by the judicial branch. The Supreme Court issued several opinions recently that greatly expand the use of funds in elections due to the First Amendment.\footnote{167} Corporations may now donate unlimited contributions to independent political broadcasts,\footnote{168} while state programs that provide matching funds to candidates who do not accept private contributions were held unconstitutional.\footnote{169} If the First Amendment prohibits such limitations on monetary expenditures in elections—that is, considers “money as speech”—it is more likely to prohibit regulation of actual speech. Thus, First Amendment concerns likely will prevent Congress from enacting any political cyberfraud regulation, and, even if such regulation occurs, the courts probably will strike down the law as unconstitutional.

**C. Federal Government Application for the Creation of a New Top-Level Domain**

In place of regulation or expanded arbitration, the government could push for ICANN to institute a new top-level domain specifically designed for the use of political candidates. ICANN has a Joint Project Agreement with the US Department of Commerce, stating: “ICANN shall maintain and build on processes to ensure that competition, consumer interests, and Internet DNS stability and security issues are identified and considered in [top-level domain] management decisions, including the considerations and implementation of new [top-level domains].”\footnote{170}

Whenever the variety of unique domain names has previously become scarce, ICANN has responded by developing and regulating

---


\footnote{168. Citizens United, 130 S. Ct. at 876.}

\footnote{169. Bennett, 131 S. Ct. at 2806.}

\footnote{170. Factsheet, supra note 17.}
new top-level domains. Included in these past top-level domains was “.name,” which was intended for use by registering individuals, rather than corporations and organizations. ICANN introduces new top-level domains in a fair and transparent process and assigns them “to organizations that can effectively manage them on behalf of Internet users.” The organizations that manage the top-level domains are registrars—either operators or sponsors—and these must meet ICANN’s technical requirements and comply with its applicable policies, as per ICANN’s agreement.

ICANN recently began a new top-level domain program, opening up the first application period from January 12 to April 12, 2012, for an organization to apply for a new top-level domain. Applying for a new top-level domain is not the same as registering for a domain name. Whereas both organizations and individuals register for domains (and pay the attendant annual fees) in order to put content on that particular website, organizations applying for new top-level domains are instead “applying to create and operate a registry business.” Essentially, these organizations intend to serve as the middlemen acting between individual domain registrants and ICANN. The application fee is estimated at $185,000, with an additional $100 user registration fee to obtain access to the electronic system on which potential registrants submit applications. The application and approval process may take anywhere from eight months for a straightforward application with no objections and no dispute for the same top-level domain, to nineteen months for highly complex applications.

---

171. See Belczyk, supra note 44 (noting that ICANN released seven new top-level domains in November 2000).
172. See Lipton, Cybersquatting, supra note 48, at 1368 (“The new [top-level domains, issued in 2000.] are: ’.aero,’ for the aviation community; ’.biz,’ for business purposes; ’.coop,’ for cooperatives; ’.info,’ for general, unrestricted use; ’.museum,’ for museums; ’.name,’ for personal names; and ’.pro,’ for professionals.”); Belczyk, supra note 44; New gTLDs: Frequently Asked Questions, INTERNET CORP. FOR ASSIGNED NAMES AND NOS., http://www.icann.org/en/topics/new-gtlds/strategy-faq.htm (last updated June 10, 2011) [hereinafter gTLDs: FAQ] (noting that in 2004 six new top-level domains were issued, including “.asia,” “.cat,” “.jobs,” “.mobi,” “.tel,” and “.travel”).
173. Factsheet, supra note 17.
174. Id.
176. gTLDs: FAQ, supra note 172.
177. Factsheet, supra note 17.
178. Id.
179. gTLD Applicant Guidebook, INTERNET CORP. FOR ASSIGNED NAMES AND NOS., 1-40 (Sept. 19, 2011), http://www.icann.org/en/topics/new-gtlds/rfp-clean-19sep11-en.pdf [hereinafter gTLD Guidebook] (noting additional fees or deposits in the case of dispute resolution or other review procedures); gTLDs: FAQ, supra note 172.
complex and contested applications. Throughout the application process, ICANN will comply with all US laws.

The application process is available to all public and private organizations, so long as they can show, through a detailed plan, that they can operate and finance such a technical system. ICANN requires, apart from ongoing registrar operating fees, a quarterly fixed fee of $6,250 for domain renewals. Besides providing financial statements and documented proof of legal establishment, applicants who would be designated “community-based” must also submit endorsement comments from the community. Community-based applications are for those top-level domains that would be operated for the purpose of a “clearly delineated community.” While the decision to submit an application as community-based is within the applicant’s discretion, ICANN intends community-based applications to be a narrow category. An applicant submitting under this designation will have to substantiate itself as a representative of the community, and its proposed top-level domain will have to “strongly and specifically” relate to the community that the applicant represents. In considering whether an applicant represents a clearly delineated community, ICANN balances four factors: (1) the ability to participate in activities, membership, and leadership, (2) the institutional purpose and benefit to the asserted community, (3) the performance of regular and beneficial activities within the asserted community, and (4) the level of formal boundaries of the asserted community. An applicant need not satisfy each and every factor. The benefit of an applicant designating itself as community based would be that it may then restrict potential second-level domain registrants to community members. Otherwise, a standard, non-community-based applicant

180.  *gTLD Guidebook*, supra note 179, at 1-14 to 1-15.
181.  *Id.* at 1-23.
182.  *See id.* at 2-19, 2-21 to 2-22; *see also id.* at 2-22 to 2-23 (discussing how application review is centralized around the questions of security and stability in the registration and maintenance of second-level domain names for the newly-created top-level domain).
183.  *gTLDs: FAQ*, supra note 172; *see also The Best Internet Addresses Will Cost a Cool Million*, N.Y. TIMES (July 14, 2009, 11:53 AM), http://bits.blogs.nytimes.com/2009/07/14/the-best-internet-addresses-will-cost-a-cool-million (estimating that it will cost approximately $1 million to apply for and begin to operate a newly created top-level domain name).
184.  *gTLD Guidebook*, supra note 179, at 1-23.
185.  *Id.* at 1-23 to 1-24; *see also id.* at 4-10 to 11 (discussing characteristics of a community for the purposes of a community-based application, including delineation, pre-existing, organization, extension, size, and longevity).
186.  *gTLD Guidebook*, supra note 179, at 1-27.
187.  *Id.* at 1-25.
188.  *Id.* at 3-7 to 3-8.
189.  *Id.*
190.  *See id.* at 4-15.
may or may not operate without restricting registrants. If the FEC designates its application as community-based, then it could refuse a domain to a non-candidate and ensure federal candidates were matched with their names for official campaign websites.

With the new application process, ICANN expects changes “in the way people find information on the Internet or how businesses plan and structure their online presence.” Thus, a new top-level domain would assist both politicians planning for their campaign sites and voters searching for a particular candidate’s official website. ICANN even expects new top-level domains to eventually include “.blog,” “.brand,” and “.city.”

All registered domains will still be subject to the UDRP arbitration process and any other process that ICANN may mandate. Nevertheless, ICANN expects applicants to describe their “rights protection mechanism” designed to resolve disputes between individuals over registered domains. Thus, ICANN encourages applicants to “develop and implement additional [rights protection mechanisms] that discourage or prevent registration of domain names that violate or abuse another party’s legal rights” and that resolve disputes before the arbitration stage. Procedures would also be in effect to allow individuals to challenge whether the applicant—here, the FEC—maintains the newly created top-level domain in an appropriate fashion.

If the federal government filed an application to create a new top-level domain for political candidates, those opposed to the proposal could submit objections before ICANN made its final decisions. Objections fall under one of four categories: (1) string confusion, (2) legal rights, (3) morality and public order, and (4) community objections. String confusion objections apply when a potential new domain would assist both politicians planning for their campaign sites and voters searching for a particular candidate’s official website. ICANN even expects new top-level domains to eventually include “.blog,” “.brand,” and “.city.”

191. See id. at 1-25 to 1-26. The gTLD Guidebook states that standard applicants must abide by the registry agreement and the principles of the program, but does not elaborate further on a standard applicant’s ability to restrict registrants. Id. Assumedly, a community-based applicant would be more justified in restricting registrants because their community would be clearly defined. See id. at 1-23 to 1-24. For instance, the FEC would distribute “.fec” domains to candidates, and not FEC employees.

192. gTLDs: FAQ, supra note 172.

193. Cf. id. at 3.2.


195. gTLDs: FAQ, supra note 172.

196. New gTLD Agreement, supra note 194, at 47.

197. See id.

198. gTLDs: FAQ, supra note 172.

199. Id.
top-level domain would be overly similar to a top-level domain that already exists.\textsuperscript{200} Legal rights objectors may be trademark holders or those with rights to a particular potential top-level domain.\textsuperscript{201} Morality and public order objections may be filed by anyone, and ICANN will decide these according to the “generally accepted legal norms of morality and public order that are recognized under international principles of law.”\textsuperscript{202} These objections will, however, be subject to a brief, initial review for frivolity.\textsuperscript{203} Finally, community objections come from “established institutions associated with clearly delineated communities,” or those whom the top-level domain may be “explicitly or implicitly target[ing].”\textsuperscript{204} To succeed, community objectors must show that the challenge to the proposed top-level domain is substantial\textsuperscript{205} and that creation of that proposed top-level domain presents a likelihood of “material detriment”\textsuperscript{206} to both the asserted community and the broader Internet community.\textsuperscript{207} ICANN’s new application procedure leaves top-level domain choice to the registrant, while settling objections at the outset.

III. SOLUTION: WHERE LEGISLATIVE AND JUDICIAL REMEDIES FAIL, AGENCY DISTRIBUTION OF DOMAINS PROTECTS BOTH THE DEMOCRATIC POLITICAL PROCESS AND FREE SPEECH

Trademark law is not adequate to regulate political cyberfraud. Although both trademark and cyberfraud laws are based on assumptions that the names of domains should represent those they appear to represent,\textsuperscript{208} the bases of legal protection for a commercial mark and for a politician’s name rest on different theoretical grounds.\textsuperscript{209} Because of trademark law’s concern with commerciality

\begin{itemize}
\item \textsuperscript{200} Id.
\item \textsuperscript{201} Id.
\item \textsuperscript{202} Id.
\item \textsuperscript{203} See id.
\item \textsuperscript{204} Id.
\item \textsuperscript{205} Id. (discussing the nuances in determining whether community objection is substantial, including the percentage of expressions of opposition in the community, the authority or representative nature of those expressing opposition, community diversity among those expressing opposition, other channels through which the objectors may have to express opposition).
\item \textsuperscript{206} Id. (listing a variety of factors that could lead to a finding of material detriment).
\item \textsuperscript{207} Id. (noting that apart from these two requirements, the community objector must also show that it is a clearly delineated community and that the proposed top-level domain is strong, which are requirements that the community-based applicant will have to show regardless).
\item \textsuperscript{208} See Lipton, \textit{Hillary, supra} note 10, at 93.
\item \textsuperscript{209} See id. at 95-96 (noting the idea of democracy and free speech as the basis of protection of a politician’s name).
\end{itemize}
and monetary value, concepts of property represent trademark regulation’s origin.\textsuperscript{210} However, the protection of a politician’s name and the ability to freely use the Internet as a campaign resource are grounded in respect for the political debate.\textsuperscript{211} Politicians need avenues to cheaply and effectively reach a multitude of people who, when informed, are better participants in the political process.\textsuperscript{212} Additionally, informed participation—and not just effective campaigning—is another component that a democratic political process should protect.\textsuperscript{213}

Because of the sensitivity a legislature needs to have toward the First Amendment (for both constitutional and political reasons),\textsuperscript{214} and because of the inability of trademark law to sufficiently protect the political process,\textsuperscript{215} the US government should submit an application to ICANN to create a new top-level domain for federal election candidates. In this way, the FEC may also encourage states to apply to be registrars for state election candidates. If the United States, through the FEC, submitted a community-based application, the government could ensure the registration of a full-name domain was confined to the political candidate who is running for federal office. While the UDRP would require dispute resolution, a community-based application may protect against most of those disputes. Disputes may still exist between candidates of the same name, but rights enforcement mechanisms that the FEC implements will decrease the number that need to go through UDRP arbitration. For instance, in the rights enforcement mechanism, George W. Bush presumably would have agreed to take “georgewbush.newdomain” if “georgebush.newdomain” were already taken. In the alternative, if George H.W. Bush no longer needed his domain, he might agree to give “georgebush.newdomain” to his son. Legislative solutions that require judicial enforcement are often lengthy and a candidate with a meritorious case may not receive the transfer of his full-name domain in time to use it. Having the FEC apply for and implement a community-based registration system would utilize the efficiency of both the screening procedures and “rights enforcement mechanisms”

\textsuperscript{210} But see Lipton, \textit{Bad Faith}, supra note 84, at 451-52 (citing Ninth Circuit and Southern District of New York cases finding trademark infringement despite the lack of commercial activities).

\textsuperscript{211} Lipton, \textit{Hillary}, supra note 10, at 120 (“The electoral process is fundamental to the U.S. system of government, and the ability to disseminate and receive important information about politics and politicians in an electoral context is key to the functioning of that system.”).

\textsuperscript{212} See id. at 119-20.

\textsuperscript{213} See id. at 120.

\textsuperscript{214} See discussion supra Part II.B.3.

\textsuperscript{215} See discussion supra Parts I.B, II.A.
encouraged by ICANN, while still keeping the process as domestically contained as possible.

Because a community-based application has more specific requirements than a general one, the FEC, as an applicant, will have to propose a domain that is strongly associated with the community at issue. Thus, “.candidate” would be unacceptable because it is not so specifically associated with the FEC as to preclude its ready association with other communities, such as state election commissions. The strengths of limiting the registration of domains to a particular community would nevertheless outweigh the more limited top-level domain options. Instead, the federal government would need to pick something not too long yet specific, such as “.fec,” short for Federal Election Commission.

Although “.com” names are the most well-recognized names, the voting public would learn quickly under the new regime that each candidate’s official website had a government-approved top-level domain. The FEC would need to implement a well-publicized educational initiative to inform voters of the official campaign websites. However, the initiative, as well as the news media covering it, would aid in spreading awareness across the nation. On the other hand, leaving voters to determine website ownership for themselves is less certain to succeed. Ownership disclaimers may be hidden in small font at the bottom of a page where viewers are unlikely to look. Moreover, fraudulent ownership is less likely to be a high profile story on news outlets, especially if it concerns a local campaign. Rather than hoping that voters discover authenticity themselves, the FEC would carry the burden of creating official websites and informing the public. By creating a new top-level domain, the FEC could set an example for individual states to follow in state elections.216 At the least, all federal election campaign websites would be distributed in the same manner.

IV. CONCLUSION

With cybersquatting and cyberfraud on the rise, politicians face an increasing risk of not having access to their full-name domains for

216. Candidates in state elections should also receive official government campaign domains. However, this Note focuses solely on federal elections due to cost considerations and ease of implementation. States may not have the funds or technology to serve as a long-term registrar. Voter education may also be more difficult to achieve because state elections are lower profile than federal ones. Despite this, state boards of elections with sufficient means should apply for a community-based top-level domain. For instance, the North Carolina Board of Elections officials could assign state candidates a “firstnamelastname.ncboe” domain. Because the FEC has authority over federal elections alone, states not applying for community-based top-level domains would be left with the current system—the “barackobama.com” scenario.
their campaign websites. Thus, ease of access to readily recognizable campaign websites will be an advantage afforded primarily to incumbents—particularly those who have been in politics for a substantial amount of time—and to those who have unique names. While cybersquatting is quite common, both federal and California legislation have stepped up to combat the problem of registering for, and then selling, domains for profit. However, state, federal, and international law have yet to satisfactorily regulate the problem of cyberfraud, where one candidate registers for a domain in his opposing candidate’s name and intentionally prevents him from using it politically. Most commonly, cyberfrauders use the domain to distribute information that is false or misleading about the candidate or supporting his opponent. While the candidate could theoretically bring a claim under the federal Lanham Act—including its Anticybersquatting Consumer Protection Act—ICANN’s Uniform Dispute Resolution Policy, or even state law (depending upon one’s jurisdiction), none of these provisions will necessarily provide the candidate with the expected relief: the transfer of his full-name domain.

Federal statutes and international arbitration focus only on the commercial use of personal names, if the law even allows for the protection of a personal name at all. Most states’ laws will either provide too high of a burden for a plaintiff to meet, such as in defamation, or will be unlikely to give the remedy the candidate desires—the transfer of the domain. While California has taken a lead in attempting to prevent cyberfraud through its Political Cyberfraud Abatement Act, jurisdictional problems abound for those disputes that are not located entirely within the state. Moreover, the constitutionality of this kind of legislation has not been sufficiently tested against the First Amendment.

While it would be possible to expand the existing federal legislation and international arbitration to accommodate for cyberfraud, this is unadvisable. The existing law should be left intact to regulate what it was originally intended to regulate: commercial interests on the Internet through trademarks and cybersquatting. Moreover, Congress and the executive branch will likely be unwilling

217. See Lacey, supra note 4; The Coalition Against Domain Name Abuse, supra note 5.
218. See discussion supra Part I.A.
219. See discussion supra Part I.B-C.
220. See discussion supra Part I.B-C.
221. See discussion supra Part I.B.
222. See discussion supra Part I.C.
223. See discussion supra Part I.C.1.
224. See discussion supra Part I.D.
to expend their political capital on new federal legislation pertaining to cyberfraud, especially given the potential First Amendment concerns.\textsuperscript{225} Free speech is a political issue too high profile for legislators to want to get involved, making any non-legislative approaches more desirable. On the other hand, international arbitrators, while efficient and inexpensive, will have neither sufficient interest in the democratic political process nor enough sensitivity to the pertinent issues that national and local courts would demonstrate when dealing with federal and state elections. Finally, while each state could enact statutes similar to California’s PCAA, the interpretation of these provisions will differ widely from jurisdiction to jurisdiction.\textsuperscript{226} Additionally, jurisdictional issues concerning the location of both the registrar and the offender will remain.\textsuperscript{227} For these reasons, independent agency officials—specifically those at the FEC—are equipped to resolve the effect that cyberfraud has on our federal elections.

The FEC should apply to ICANN for a top-level domain specifically for federal political candidates. With its own top-level domain, the federal government would be able to issue campaign websites systematically to all candidates, while leaving the generic top-level domains such as “.com” and “.net”\textsuperscript{228} for the use of citizens wishing to exercise their political speech rights. All candidates should be able to capitalize on the success of “barackobama.com” by having their own “firstnamelastname.fec.”

\textit{Whitney C. Boshers\textsuperscript{*}}

---

\textsuperscript{225} \textit{See discussion supra} Parts I.D, II.B.3.
\textsuperscript{226} \textit{See discussion supra} Part II.B.1.
\textsuperscript{227} \textit{See discussion supra} Part II.B.
\textsuperscript{228} \textit{See discussion supra} Parts II.C, III.

\textsuperscript{*} J.D. Candidate, Vanderbilt University Law School, 2012; B.A., English, University of Tennessee, 2009. The author wishes to thank the \textit{VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW} Senior Editorial Board for their guidance throughout the composition of this Note.