

Hey That’s Mine: What To Do When Political Candidates Are Unable To Register Their Names as the Domain Name for Their Website

Spencer Low*

I.	OVERVIEW	136
II.	DOMAIN NAMES AND CYBERSQUATTING.....	137
III.	CYBERSQUATTING POLITICAL CAMPAIGN WEBSITES.....	138
	A. <i>Prevent Cybersquatting by Registering the Domain Names Before Anyone Else Can</i>	139
	B. <i>Paying up Can Solve the Problem if Candidates Have the Money</i>	140
	C. <i>Options in Federal Court</i>	141
	D. <i>Establishing Sufficient Trademark Rights in a Name Under the UDRP Is the Primary Challenge for Candidates</i>	143
	E. <i>California Legislation Does Not Apply Well to Cybersquatting</i>	150
IV.	POLITICAL CYBERFRAUD	151
	A. <i>The ACPA’s Applicability and First Amendment Implications Discussed in Ficker</i>	152
	B. <i>Under the UDRP, Once Candidates Establish Rights in Their Names, They Must Overcome Protections of Political Speech</i>	154
	1. Respondent’s Rights or Interests in the Domain Name.....	155
	2. The Final Requirement: Demonstrating Respondent’s Bad Faith.....	158
	C. <i>State Law Solutions</i>	160
	1. California Political Cyberfraud Abatement Act (PCAA).....	160

* © 2016 Spencer Low. Senior Business Editor, Volume 19, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2017, Tulane University; B.A. 2014 Political Science, Kansas State University. The author would like to thank his friends and family, especially his niece Rosalyn for being the shining star of the family. He would also like to thank the members of *JTIP* for all their hard work.

2.	California Business and Professional Code	
	§ 17525	161
3.	Defamation	162
D.	<i>Solutions Outside Court: Let the Press Reveal the Conduct</i>	163
V.	CONCLUSION	164

I. OVERVIEW

In today's Internet era, candidates for public office use campaign websites as tools to raise money, organize supporters, and inform voters.¹ Many candidates seek to register domain names that are composed of or incorporate their own names, which makes sense because it is another way to identify and easily find the campaign website.² However, candidates are increasingly unable to register their personal names as domain names because someone else registered it first.³ Sometimes, the domain name was registered innocently by someone else with the same name,⁴ but more often it is done by cybersquatters: people who see an opportunity to make money by registering domain names that incorporate or consist of current or future politician's names in order to sell them to that person for a profit down the road.⁵ Cybersquatting has occurred in elections on almost every imaginable level, from federal offices to local ones, and is not unique to the United States.⁶

Part III will discuss what political candidates can do if they encounter cybersquatting. Unfortunately, the legislation passed by Congress to stop this conduct applies poorly to political cybersquatting,

1. Matthew T. Sanderson, *Candidates, Squatters, and Grippers: A Primer on Political Cybersquatting and a Proposal for Reform*, 8 ELECTION L.J. 3, 10-11 (2009).

2. See Whitney C. Boshers, *What's in a Name?: Predictably Regulating Cyberfraud To Protect the Democratic Political Process*, 14 VAND. J. ENT. & TECH L. 127, 128-30 (2011).

3. See Josh Hafner, *Politicians Not Always Masters of Their Domain (Names)*, DES MOINES REG. (Mar. 27, 2015, 11:37 PM), <http://www.desmoinesregister.com/story/news/elections/presidential/caucus/2015/03/27/presidential-election-politician-domain-names/70570996/>; Sanderson, *supra* note 1, at 11-12.

4. See, e.g., Terrence Dopp, *The Time Wisconsin Chris Christie Sold Jersey Chris Christie a Web Address*, BLOOMBERGPOLITICS (July 17, 2015, 6:59 PM), <http://www.bloomberg.com/politics/articles/2015-07-17/the-time-wisconsin-chris-christie-sold-jersey-chris-christie-a-web-address>.

5. See Jacqueline D. Lipton, *Who Owns "Hillary.com"? Political Speech and the First Amendment in Cyberspace*, 49 B.C. L. REV. 55, 60 (2008) [hereinafter Lipton, *Who Owns Hillary.com*].

6. See Sanderson, *supra* note 1, at 8-9.

leading many candidates to seek help through international arbitration with mixed results.⁷

While political cybersquatting only concerns registration of domain names with the intention of turning a profit by selling them later, Part IV will discuss political cyberfraud, in which the registrant of the domain name uses it in relation to or to comment on the candidate's campaign rather than just selling it off to the highest bidder.⁸ Political cyberfraud carries First Amendment implications with it, especially since the ability to comment and criticize on public officials is highly protected and valued in the United States.⁹ While anti-cybersquatting statutes can be of some aid, international arbitration is often the preferred method to resolve this issue, as state law only offers minimal avenues of redress.¹⁰ As shown by this Comment, there are few clear-cut ways to stop political cybersquatting or cyberfraud, but some trends have emerged that can illustrate how candidates find favorable outcomes for themselves and their campaigns.

II. DOMAIN NAMES AND CYBERSQUATTING

Gone are the days when navigating the Internet required users to know the unique 32-bit number IP address of websites they wanted to visit.¹¹ That system seems complex and archaic compared to today's more "human-friendly" Domain Name System, which allows users to type in easy-to-remember addresses such as www.google.com, which their web browser automatically converts into the 32-bit IP address, taking them to the Google homepage.¹² To run the daily operations of this new system, the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation headquartered in California, was created in 1998.¹³ Those seeking to register a domain name must do so through one of many registrars that ensure the desired name is unique and not already taken.¹⁴

7. See discussion *infra* Sections III.C, III.D.

8. See discussion *infra* Part IV.

9. See discussion *infra* Part IV.

10. See discussion *infra* Sections IV.A, IV.B.

11. See Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 194 (2000).

12. Sanderson, *supra* note 1, at 4.

13. *Id.* at 5.

14. *Id.* There are a substantial number of registrars, which can be found at <https://www.internic.net/alpha.html>.

The first-come, first-serve process of registering domain names opened the door to cybersquatting: registering the names of businesses, well-known individuals, or their trademarks to which the registrants have no connection, with the intent to profit by selling the domain name.¹⁵ Although these “virtual prospectors” were quick to the draw on registering trademarks as domain names, the practice was frowned upon from the outset by courts.¹⁶ Congress responded to the problem in 1998 by passing the Anti-Cybersquatting Consumer Protection Act¹⁷ (ACPA), while ICANN created the Uniform Domain Name Dispute Resolution Policy¹⁸ (UDRP).¹⁹ While the ACPA’s effect is limited to the United States, the UDRP has a global reach because domain name registrants agree to submit to arbitration under it when they register the domain name.²⁰

III. CYBERSQUATTING POLITICAL CAMPAIGN WEBSITES

Candidates increasingly rely on their campaign websites during elections, which tend to be most effective when affiliated with desirable domain names.²¹ A website is not just a place for candidates to post a family picture, a biography and a platform; it is a way to organize support and is an exceedingly valuable fundraising tool.²² The importance of campaign websites make political candidates particularly vulnerable to cybersquatting because not having an official-looking domain name can take away the best way to reach supporters and raise funds.²³

15. *Id.* at 6.

16. Jacqueline D. Lipton, *Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property, and Restitution*, 23 HARV. J.L. & TECH. 447, 448.

17. 15 U.S.C. § 1125(d) (2012).

18. *Uniform Domain Name Dispute Resolution Policy*, ICANN, <https://www.icann.org/resources/pages/policy-2012-02-25-en> (last visited Nov. 9, 2016) [hereinafter *UDRP*].

19. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 61.

20. *Id.*

21. Sanderson, *supra* note 1, at 10.

22. *Id.* In 2006, total online fundraising in the United States eclipsed \$100 million, a number that is dwarfed by the \$525 million that Barack Obama brought in through online donations in the 2012 election. *Id.*; Byron Tau, *Obama Camp Fundraising Total: \$1.1B*, POLITICO (Jan. 19, 2013, 5:42 PM), <http://www.politico.com/story/2013/01/obama-campaign-final-fundraising-total-1-billion-086445>.

23. Sanderson, *supra* note 1, at 11.

A. *Prevent Cybersquatting by Registering the Domain Names Before Anyone Else Can*

One solution is for candidates to register their names and as many variants thereof combined with as many possible top-level domains (such as .com, .org, and .net) as possible.²⁴ Even if it were feasible to register that many permutations of a candidate's name, early registration is less useful for candidates who decide to run later in the cycle.²⁵ Moreover, doing so could signal a candidate's intention to run before the candidate was ready to announce.²⁶ Acting early may not be enough, as cybersquatters can get an early jump on candidates: Hillary2008.com was registered in 1999, while BarackObama2008.com was taken shortly after the then-Senator's speech at the 2004 Democratic National Convention.²⁷ The other side of the aisle is no less susceptible: before George W. Bush's first presidential campaign began leading into the 2000 election, thirty-nine different domain names were registered incorporating his name.²⁸ Additionally, RudyForPresident.com was registered in the days following the 9/11 attacks as New York City Mayor Rudy Giuliani entered the national spotlight.²⁹

Of course, candidates can settle for a different domain name if their personal name has already been registered; just ask 2016 presidential hopeful Ted Cruz. Internet users hoping to find his campaign website by typing in TedCruz.com during the Republican nomination process were taken to a website that simply displayed the phrase "SUPPORT PRESIDENT OBAMA. IMMIGRATION REFORM NOW!"³⁰ Cruz is not alone: JebBush.com redirected to eventual Republican nominee Donald Trump's campaign website.³¹ Instead of purchasing or fighting

24. *Id.* at 13.

25. *Id.*

26. *Id.* Any joint presidential ticket would essentially be a lost cause, as a candidate would need to register any combination of his or her name along with any potential running mate, which could lead to wild speculation by the media and public. *See id.*

27. *Id.* at 12.

28. *Id.* at 13.

29. *Id.* at 12. The Republican Party does have a buying program for potential candidate's domain names, including GeorgePBush.com for George W. Bush's nephew and 2016 presidential candidate Jeb Bush's son. *Id.* at 13.

30. Hafner, *supra* note 3; *see e.g.* TEDCRUZ.COM, www.TedCruz.com (last visited Nov. 11, 2016). As of November 2016, the website displayed a picture of Democratic nominee Hillary Clinton with the words "FIRST WOMAN PRESIDENT OF THE UNITED STATES OF AMERICA!!!" *Id.*

31. Yanan Wong, *JebBush.com Redirects to Trump, but for a Real Kick, Click on TedCruzForAmerica.com*, WASH. POST (Feb. 17, 2016), <https://www.washingtonpost.com/news/>

for the domain names, both Bush and Cruz chose different domain names for their campaign websites—TedCruz.org and Jeb2016.com.³²

B. Paying up Can Solve the Problem if Candidates Have the Money

One option for any political candidate if his or her name is already registered as a domain name is to do exactly what the cybersquatter wants—pay up. The first step would be finding out who actually owns the domain name, which can be done by searching WHOIS, a database that allows users to search for a domain name and find the contact information of the registrant.³³ Once contact is made, the owner of the domain name is in a position to ask for an inordinate price.³⁴ For example, when former Congressman and three-time presidential candidate Ron Paul contacted the owner of RonPaul.com, he was told that he could purchase it for \$848,000.³⁵ Although Paul opted for UDRP arbitration,³⁶ other candidates have chosen to buy their desired domain name, such as his son, Rand Paul.³⁷ Rather than follow his father's footsteps, the Senator purchased RandPaul.com for over \$100,000 before he announced his candidacy for President in the Spring of 2015.³⁸

Six-figure asking prices for presidential candidate websites are not confined to the Paul family tree.³⁹ Hillary Clinton's campaign committee registered HillaryClinton.com for her Senate campaigns in 2000 and 2006, but ElectHillary.com and HillaryNotPresident.com both carried an asking price of \$295,000, while ReElectHillary.com was offered at a relative discount of \$275,000.⁴⁰ Meanwhile, website domains using New Jersey Governor Chris Christie purchased PresidentChrisChristie.com and ChrisChristieForPresident.com; those are on the market for \$49,000

morning-mix/wp/2016/02/17/jebbush-com-redirects-to-trumps-site-but-wait-till-you-see-where-tedcruzforamerica-com-goes/; see www.JebBush.com (last visited Nov. 9, 2016).

32. See SENATOR TED CRUZ | CRUZ FOR PRESIDENT, www.TedCruz.org (last visited Nov. 9, 2016); JEB! 2016, www.Jeb2016.com (last visited Nov. 9, 2016).

33. Sanderson, *supra* note 1, at 13; see WHOIS LOOKUP & IP, www.whois.net (last visited Nov. 9, 2016).

34. Sanderson, *supra* note 1, at 14.

35. Paul v. Whois Privacy Servs., No. D2013-0278, 2013 WL 2390820, at *8 (WIPO May 8, 2013).

36. See generally, *id.*

37. Mario Trujillo, *Rand Paul Paid \$100,000 for Domain Name*, HILL (May 6, 2015, 2:19 PM), <http://thehill.com/policy/technology/241220-paul-paid-100000-for-domain-name>.

38. *Id.*

39. Jose Pagliery, *'Hillary' Websites Going for Up to \$295K*, CNN MONEY (Apr. 7, 2015, 9:37 AM), <http://money.cnn.com/2015/04/06/technology/hillary-clinton-website/>.

40. *Id.* Despite their conflicting messages, all three domain names shared one owner, who purchased them over ten years prior. *Id.*

each.⁴¹ But that was not all for Christie, who actually purchased ChrisChristie.com, which had been registered in 2005 by a man from Wisconsin with the same name.⁴²

As demonstrated above, people who register domain names before candidates know the value of their commodities and set the price as high as they can. Although purchasing the domain name can end the issue quickly, candidates that balk at the price tag can try their luck with a legal remedy.

C. Options in Federal Court

Candidates who fall victim to cybersquatting can turn their eyes to the courts for a remedy, but might need to squint in order to find help. Current regulations of the Domain Name System are trademark-based, which poses a problem for politicians and candidates seeking legal action against cybersquatters because most do not have or cannot establish trademark protection in their names.⁴³

The ACPA protects marks, “including a personal name which is protected as a mark” when registered by a person that “has a bad faith intent to profit from that mark,” and registers or uses a domain name that is identical or confusingly similar to that mark.⁴⁴ Several factors courts can consider in determining bad faith are listed in the statute, such as whether the domain name is used in connection with the sale of goods or services, whether it is being put to a noncommercial or fair use, or whether it was offered for sale without having been used commercially.⁴⁵ Additionally, the ACPA states that if the registrant reasonably believed that his use of the domain name was a fair use or otherwise lawful, bad faith will not be found.⁴⁶ Plaintiffs bringing a civil suit under the ACPA

41. *Id.*

42. Dopp, *supra* note 4. While Christie the politician did not disclose how much he paid for the domain name, he told people at a town hall meeting that the Wisconsin Christie “did very well.” *Id.*

43. See Lipton, *Who Owns Hillary.com*, *supra* note 5, at 57, 62; 15 U.S.C. § 1125(d) (2012) (allowing “the owner of a mark” to bring a civil suit); *UDRP*, *supra* note 18, at para. 4(a)(i) (requiring complainants to assert that the “domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.”). See also Jacqueline D. Lipton, *Celebrity in Cyberspace: A Personality Rights Paradigm for Personal Domain Name Disputes*, 65 WASH. & LEE L. REV. 1445, 1462-68 (2008).

44. 15 U.S.C. § 1125(d).

45. *Id.* § 1125(d)(1)(B)(i).

46. *Id.* § 1125(d)(1)(B)(ii).

can seek two remedies: forfeiture or cancellation of the defendant's domain name or its transfer to the plaintiff.⁴⁷

Federal case law involving politicians or candidates bringing suit under the ACPA consists of one case that is over a decade old and is less than helpful to any candidate seeking help from the courts.⁴⁸ While running for a seat in the House of Representatives, Robin Ficker found that RobinFicker.com had been registered by somebody else and was used to house summaries of disparaging news stories about him.⁴⁹ The court refused to grant Ficker's motion for a temporary restraining order on the website's use, stating that it was not "convinced, at this point, that the ACPA provides coverage for personal names that are not trademarked, where the websites have no commercial use."⁵⁰ *Ficker* is not wholly applicable to political cybersquatting because the defendant did not intend to profit by selling the domain name, but rather was using the website to criticize the candidate.⁵¹ Because of this, *Ficker* relates to cyberfraud more than cybersquatting discussed below in Part III. However, the case exemplifies the uphill battle candidates face when seeking protection for their names as used in domain names.⁵²

Another potential avenue for candidates is 15 U.S.C. § 8131, which provides:

Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.⁵³

While § 8131 could help candidates protect themselves from cybersquatters like the woman who registered multiple permutations of Hillary Clinton's name,⁵⁴ it would be of little help to Christie regarding ChrisChristie.com.⁵⁵ Not only did the other Christie appear to lack a specific intent to profit by selling the name,⁵⁶ but he was also registering

47. *Id.* § 1125(d)(1)(C).

48. *Cf.* *Ficker v. Tuohy*, 305 F. Supp. 2d 569 (D. Md. 2004).

49. *Id.* at 571.

50. *Id.* at 572. The court added that noncommercial uses of a mark are not actionable under § 43 of the Lanham Act either. *Id.*

51. *Id.*

52. *See also, infra* Section III.D.

53. 15 U.S.C. § 8131 (2012).

54. *See* Pagliery, *supra* note 39.

55. *See* Dopp, *supra* note 4.

56. *Id.*

his own name, which would not seem to be the conduct proscribed by § 8131.⁵⁷

When a candidate's name is registered as a domain name solely to earn the registrant a profit, candidates can find help in federal court under the above statutes. However, there are several limitations that can explain the lack of cases in this area. First, not all cybersquatters are in the United States, which can make it difficult for a federal court to have jurisdiction.⁵⁸ Second, demonstrating trademark rights in a name can be difficult, as discussed in the upcoming section. Third, as seen in *Ficker*, without an intent to profit, candidates might be turned away from court.⁵⁹ Lastly, federal court can be costly and time-consuming.⁶⁰ Due to these issues, candidates seem more amenable to availing themselves of the UDRP, as discussed below.

D. Establishing Sufficient Trademark Rights in a Name Under the UDRP Is the Primary Challenge for Candidates

Given that campaigns are generally short-lived, candidates may not want to wait for a federal court to weigh in.⁶¹ Because of this time-sensitivity, candidates appear to be more willing to use the UDRP than they are to seek help in court.⁶² Opting for the UDRP is understandable from both a time and price perspective: the fee for filing a case with the UDRP starts at \$1500,⁶³ while the total time from filing a complaint to final decision averages around seven weeks.⁶⁴

To initiate a UDRP proceeding, complainants file a complaint with any one of five ICANN-authorized arbitration providers, and a decision

57. See 15 U.S.C. § 8131; Lipton, *Who Owns Hillary.com*, *supra* note 5, at 65. Additionally, the ACPA envisions that a registrant whose legal name is the domain name or is otherwise commonly known by it is not acting in bad faith. 15 U.S.C. § 1125(d)(B)(i)(II) (2012).

58. See *infra* note 112 and accompanying text.

59. See *Ficker v. Tuohy*, 305 F. Supp. 2d 569 (D. Md. 2004).

60. Sanderson, *supra* note 1, at 14.

61. See *id.* at 11-12.

62. Lipton, *Who Owns Hillary.com*, *supra* note 5, at 66.

63. *WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*, WORLD INTELL. PROP. ORG., <http://www.wipo.int/amc/en/domains/guide/> (last visited Feb. 21, 2016).

64. Sanderson, *supra* note 1, at 14. The UDRP Rules state that the panel shall issue its decision within fourteen days. *Rules for Uniform Domain Name Dispute Resolution Policy*, ICANN, para. 15(b) (Sept. 28, 2013), <https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en>.

is issued without discovery or oral arguments.⁶⁵ Paragraph 4(a) of the UDRP states that complainants must prove that (1) the “domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights,” (2) the registrant has “no rights or legitimate interests in respect of the domain name,” and (3) the “domain name has been registered and is being used in bad faith.”⁶⁶ The UDRP offers two remedies: transfer of the domain name to the complainant, or cancellation of the domain name, in the rare case that the neither party can establish rightful ownership over the domain name.⁶⁷

The primary obstacle for any political candidate who chooses to use the UDRP is that under paragraph 4(a), candidates must demonstrate a trademark interest in their names.⁶⁸ While some candidates might already have established trademark protection in their names, like 2016 Republican presidential nominee Donald Trump,⁶⁹ other candidates, especially in state-level or Congressional elections, do not have that luxury.⁷⁰

Several UDRP decisions regarding politicians’ and candidates’ names being used in domain names have already occurred. Panels hearing these UDRP decisions have been split on whether the various complainants had trademark rights in their names.⁷¹ One of the earliest decisions was in 2000, when an arbitrator found that Canadian Parliament member, Minister of Justice, and Attorney General of Canada Anne McLellan had established sufficient common law trademark rights in her name to sustain her complaint.⁷² Two important things to note about this decision are that the respondent failed to submit a response and that the arbitrator only discussed McLellan’s name recognition from her political activities.⁷³ Just a couple months later, another arbitrator

65. Sanderson, *supra* note 1, at 14, 15; *List of Approved Dispute Resolution Service Providers*, ICANN, <https://www.icann.org/resources/pages/providers-6d-2012-02-25-en> (last visited Feb. 21, 2015).

66. *UDRP*, *supra* note 18, at para. 4(a).

67. *Id.* at para. 4(i); *see also* Sanderson, *supra* note 1, at 15. Cancelled domain names are then available to the public. *Id.*

68. *UDRP*, *supra* note 18, at para. 4(a); *see also* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 67-69; Sanderson, *supra* note 1, at 17-21.

69. *See* Trump v. Stevens, No. 2015-0478, 2015 WL 2357107, at *2 (WIPO May 8, 2015).

70. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 67-69; *see also* Sanderson, *supra* note 1, at 17-21.

71. *See infra* notes 73-110 and accompanying text.

72. McLellan v. Smartcanuk.com, Nos. AF-303a, AF-303b, 2000 WL 33647281, at *3 (eResolution Sept. 25, 2000).

73. *Id.*

found that former United States Senate candidate and potential Virginia gubernatorial candidate Mark Warner also established common law trademark rights in his name.⁷⁴ The arbitrator noted that actress Julia Roberts, former NFL quarterback Dan Marino, and McLellan had all established sufficient trademark rights in their names in UDRP proceedings, and while Warner was “not a movie star, an NFL quarterback, or a member of the Canadian Parliament,” his name was protected under the UDRP.⁷⁵

While *McLellan* and *Warner* seemed to have established a favorable precedent for future political candidates, a brewing storm appeared on the horizon when Kathleen Kennedy Townsend, Lieutenant Governor of Maryland, potential candidate for Governor of Maryland and daughter of former United States Attorney General Robert Kennedy, was unsuccessful in demonstrating rights in her name under the UDRP.⁷⁶ While the arbitrator stated that *McLellan* was properly decided, it noted that a recent report by the World Intellectual Property Organization (WIPO) indicated that the UDRP’s protections “should be limited to personal names that had been commercially exploited.”⁷⁷ The arbitrator continued that while political fundraising could constitute commercial exploitation of a candidate’s name, when “political candidates authorize the formation of separate legal entities to raise funds on the candidates’ behalf” only those entities would be the appropriate parties to argue that the name has been sufficiently used in commerce to gain protection.⁷⁸ The arbitrator reasoned that the “legal separation of individual candidate from fund-raising activity cannot be used as a protective cloak in certain circumstances, but shed when beneficial to do so.”⁷⁹ Despite offering a potential avenue for political complainants to demonstrate commercial exploitation of their names, the arbitrator remained skeptical of its success, concluding that “the protection of an individual politician’s name, no matter how famous, is outside the scope of the Policy since it is

74. Warner v. Larson, No. FA0009000095746, 2000 WL 33675081, at *1, *4 (Nat’l. Arb. F. Nov. 15, 2000).

75. *Id.* at *4.

76. Townsend v. B.G. Birt, No. D2002-0030, 2002 WL 827005, at *2, *5 (WIPO Apr. 11, 2002).

77. *Id.* at *4.

78. *Id.* at *5. Townsend’s fundraising entity subsequently brought suit but was found to have no standing because there was no evidence that Townsend had actually granted the entity rights to a mark, what the mark was, or when its common law rights arose. Friends of Kathleen Kennedy Townsend v. B.G. Birt, No. D2002-0451, 2002 WL 1832487, at *5 (WIPO July 31, 2002).

79. *Townsend*, 2002 WL 827005, at *5.

not connected with commercial exploitation as set out in the Second WIPO Report.”⁸⁰

Townsend's strong language against protecting politicians' names was not the start of a sweeping change, however. In 2003, an arbitrator found that United States Congressman Ken Calvert established common law rights in his name as a mark.⁸¹ Like *McLellan*, the respondent failed to submit any response, leaving the arbitrator free to “accept all reasonable allegations and inferences in the Complaint as true.”⁸² While such silence from the respondent usually bodes well for complainants, that same year an arbitrator found that a Spanish political party did not have sufficient rights in its candidate's name despite no response from the respondent.⁸³ Because the name was “used in a political context, but not in commerce to distinguish goods or services,” it had not earned sufficient protection.⁸⁴ While the result was in line with *Townsend*, that decision was not mentioned in the opinion, demonstrating the unpredictable nature of *stare decisis* as used by UDRP panels.⁸⁵ In 2004, an arbitrator found that former Oregon gubernatorial candidate Bill Sizemore established rights in his name through its use in business, hosting a radio program, and being a “public figure.”⁸⁶

The following year, an arbitrator found that then-Senator and former first lady Hillary Clinton also established common law rights in her name.⁸⁷ However, because the respondent failed to file any response, Clinton's uncontested assertion that her name became distinctive through use and exposure in the marketplace, as well as through her political activities, was taken by the arbitrator as sufficient to establish rights.⁸⁸

Clinton is not the only member of her family who has turned to the UDRP—a panel “reluctantly” found that her husband, Bill Clinton, had

80. *Id.*

81. *Calvert v. Domain Strategy, Inc.*, No. FA0306000162075, 2003 WL 24129957, at *2, (Nat'l. Arb. F. Aug. 1, 2003).

82. *Id.*

83. *Convergència Democràtica de Catalunya v. ar mas*, Case No. DTV2003-0005 (WIPO Dec. 19, 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>.

84. *Id.*

85. *See id.*; *see also Sanderson*, *supra* note 1, at 16 (discussing the role of *stare decisis* in UDRP decisions).

86. *Sizemore v. DIS, Inc.*, No. FA0312000221173, 2004 WL 3270344, at *4 (Nat'l. Arb. F. Feb. 26, 2004).

87. *Clinton v. Dinoa*, No. FA0502000414641, 2005 WL 853535, at *3 (Nat'l. Arb. F. Mar. 18, 2005).

88. *Id.*

acquired sufficient secondary meaning in his name to satisfy the UDRP.⁸⁹ The arbitrator noted that since Bill Clinton had served as President of the United States and Governor of Arkansas, participated in various philanthropic activities, and was named Time's Man of the Year in 1992, Bill Clinton was "one of the most famous and recognized people in the world," he had therefore achieved trademark protection in his name.⁹⁰

In 2007, Virginia Fields, at the time a candidate for a New York Senate seat, was unsuccessful in asserting trademark rights in her name in a UDRP proceeding.⁹¹ Fields had been the first African American woman elected to the New York City Council; she had also served as the Manhattan Borough President and had run as a candidate for Mayor of New York City.⁹² However, during the proceeding, Fields failed to point to any authorities supporting her contention that those positions gave rise to trademark rights in her name.⁹³ The respondent, on the other hand, successfully invoked *Townsend*, with the panel adding that Fields had not used her name as an indication of the source of any goods or services.⁹⁴

Lastly, in 2011, an arbitrator determined that London Mayor Boris Johnson had established rights in his name by demonstrating that he was "involved in sufficient commercial transactions."⁹⁵ Perhaps as a nod to *Townsend*, the panel stated that "[t]he fact that Complainant is a politician is not sufficient to give rise to trademark rights," but as with other well-known people such as authors, entertainers, and athletes, "the relevant inquiry is whether Complainant has used his or her personal name as a marketable commodity, for a fee to promote another's goods or services, or for direct commercial purposes in the marketing of his or her own goods and services."⁹⁶ Although his name had sufficient protection, the domain name in dispute was BackBoris.com, not simply his name.⁹⁷ The panel concluded that although he did not have trademark rights in "BACK BORIS" because it was related only to his political activity as a

89. Clinton v. Web of Deception, No. FA0904001256123, 2009 WL 1638033, at *4 (Nat'l. Arb. F. June 1, 2009).

90. *Id.* at *5.

91. Fields for Senate v. Toddles Inc., Case No. D2006-1510 (WIPO Mar. 14, 2007), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-1510.html>.

92. *Id.*

93. *Id.*

94. *Id.*

95. Johnson v. Belize Domain Whois Servs., No. D2010-1954, 2011 WL 670328, at *4 (WIPO Jan. 24, 2011).

96. *Id.* at *3, *4.

97. *Id.* at *2.

candidate for mayor, the domain name was confusingly similar to what he did have rights in, which satisfied paragraph 4(a)(i) of the UDRP.⁹⁸

As this chronological examination of UDRP decisions shows, there is no consensus on whether or how political candidates can establish sufficient rights in their name, but a few conclusions can be gleaned. First, with the exception of one case,⁹⁹ a respondent's failure to respond typically means that a complainant will be able to establish trademark protection in his or her name simply by asserting so.¹⁰⁰ Second, candidates who can highlight any commercial and non-political use of their name tend to be more successful in establishing trademark rights therein.¹⁰¹ This is especially important in the wake of *Townsend's* strong language against protection of politicians' names.¹⁰²

Moreover, although *Townsend* seemed to state a bright-line rule that politicians' names were not protected, subsequent cases show that it has not resulted in a drastic change in how arbitrators view the treatment of political cybersquatting.¹⁰³ This could be the product of a couple things. One might be that UDRP panels do not always follow *stare decisis*.¹⁰⁴ While it may be the case that former decisions are not binding precedent, panels frequently use them to bolster their positions.¹⁰⁵ That said, the more plausible reason might not be that *Townsend* has been ignored, but rather that political complainants have heeded it and emphasized any and all commercial and non-political exploitation of their names, such as Bill

98. *Id.* at *4-5.

99. *See generally*, *Convergència Democràtica de Catalunya v. ar mas*, Case No. DTV2003-0005 (WIPO Dec. 19, 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>.

100. *See, e.g.*, *McLellan v. Smartcanuk.com*, Nos. AF-303a, AF-303b, 2000 WL 33647281 (eResolution Sept. 25, 2000); *Forrester v. Hoffman*, No. FA0307000170644, 2003 WL 22700373, at *3 (Nat'l. Arb. F. Sept. 3, 2003); *Clinton v. Dinoia*, No. FA0502000414641, 2005 WL 853535, at *3 (Nat'l. Arb. F. Mar. 18, 2005); *Johnson v. Belize Domain Whois Servs.*, No. D2010-1954, 2011 WL 670328, at *2 (WIPO Arb. Ctr. Jan. 24, 2011).

101. *See, e.g.*, *Warner v. Larson*, No. FA0009000095746, 2000 WL 33675081, at *1, (Nat'l. Arb. F. Nov. 15, 2000) (involvement in local business); *Sizemore v. DIS, Inc.*, No. FA0312000221173, 2004 WL 3270344, at *4 (Nat'l. Arb. F. Feb. 26, 2004) (carpet business and radio show host); *Clinton* 2005 WL 853535, at *2-3 (best-selling author and internationally recognized); *Clinton v. Web of Deception*, No. FA0904001256123, 2009 WL 1638033, at *5 (Nat'l. Arb. F. June 1, 2009) (former U.S. President and internationally known); *Johnson*, 2011 WL 670328, at *1, *4 (journalist, author, speaker/entertainer, and had 86.5% name recognition in England).

102. *Townsend v. B.G. Birt*, No. D2002-0030, 2002 WL 827005, at *5 (WIPO Apr. 11, 2002).

103. *See supra* notes 82-98 and accompanying text.

104. *See Sanderson, supra* note 1, at 16.

105. *See, e.g.*, *Sizemore*, 2004 WL 3270344, at *5 (citing to other decisions almost exclusively as analysis).

Sizemore discussing his former carpet business and both Bill and Hillary Clinton emphasizing the non-political activities even though their name recognition originated through political activity.¹⁰⁶

Finally, while fundraising activities might qualify as commercial exploitation of a name, candidates themselves may lack standing if they have a separate fundraising entity.¹⁰⁷ Thus, if a fundraising entity has been established, it should have standing to bring a complaint and should be able to clearly demonstrate that the candidate licensed it to use the name.¹⁰⁸

After establishing trademark rights in a name and demonstrating confusing similarity, complainants have two more requirements to fulfill under the UDRP: (1) proving that the respondent has no rights or legitimate interests in the domain name, and (2) proving that the domain name was registered in bad faith.¹⁰⁹ In the case of pure cybersquatting, neither of these appear to be as difficult as proving trademark rights: cybersquatters only register domain names to sell them for a profit, which is not contemplated in paragraph 4(c)'s list of legitimate uses, while paragraph 4(b)(i) of the UDRP explicitly states that registering a domain name for the purpose of selling it constitutes bad faith.¹¹⁰

The number of complaints brought under the UDRP compared to those brought in Federal court shows which option is favored by politicians and candidates for office. Part of the disparity may be that cybersquatters are not solely located in the United States, and to take action against them, candidates must turn to international arbitration due to the jurisdictional limitations of U.S. courts.¹¹¹ Other complainants who do not face a jurisdictional issue may opt for the UDRP simply because it

106. *Id.* at *4; *Clinton*, 2005 WL 853535, at *2; *Clinton*, 2009 WL 1638033, at *2.

107. *Townsend*, 2002 WL 827005, at *5.

108. *See Townsend*, 2002 WL 827005 (finding that candidate did not have standing when fundraising was done by separate legal entity); *Friends of Kathleen Kennedy Townsend v. B.G. Birt*, No. D2002-0451, 2002 WL 1832487, at *5 (WIPO July 31, 2002) (finding that separate fundraising entity did not have standing partly because there was no evidence that the entity had been licensed to use the name); *Fields for Senate v. Toddles Inc.*, Case No. D2006-1510 (WIPO Mar. 14, 2007), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-1510.html> (stating that a candidate's political campaign committee has no standing where there was no evidence that it had any rights in a mark consisting of her name).

109. *UDRP*, *supra* note 18, at para. 4(a).

110. *Id.* at para. 4(b)-(c).

111. *See, e.g., Johnson v. Belize Domain Whois Servs.*, No. D2010-1954, 2011 WL 670328, at *1 (WIPO Jan. 24, 2011) (respondent was located in Belize while complainant was in England); *Clinton v. Dinoia*, No. FA0502000414641, 2005 WL 853535, at *1 (Nat'l. Arb. F. Mar. 18, 2005) (respondent was in Italy while complainant was in the United States).

is faster and cheaper than going to court, and thus better suited for the context of a political campaign.¹¹²

E. California Legislation Does Not Apply Well to Cybersquatting

State law in this area is limited to two California statutes, however these statutes provide little help.

First is California's Political Cyberfraud Abatement Act (PCAA), which by its name is clearly not focused on cybersquatting.¹¹³ Although the PCAA concerns acts of political cyberfraud, subsection (c)(1)(D) might have applicability to cybersquatting.¹¹⁴ This section prohibits: "[i]ntentionally preventing the use of a domain name for a political Web site by registering and holding the domain name or by reselling it to another with the intent of preventing its use, or both."¹¹⁵ While typical cybersquatting involves an intent to sell the domain name for profit,¹¹⁶ subsection (D) only pertains to holding on to the domain name in an effort to prevent others from using it.¹¹⁷ However, even if subsection (D) can be applied to a case of political cybersquatting, there is another issue: the statute defines "Political Web site" as "a Web site that urges or appears to urge the support or opposition of a ballot measure."¹¹⁸ Thus, not only is the PCAA limited by its jurisdictional reach as a state statute and its focus on cyberfraud rather than cybersquatting, it applies only to ballot measures rather than candidate's campaign websites.¹¹⁹

The other California statute is Business and Professional Code § 17525, which was amended shortly after Congress passed the ACPA and makes it unlawful "for a person, with a bad faith intent to register, traffic in, or use a domain name, that is identical or confusingly similar to the personal name of another living person or deceased personality, without regard to the goods or services of the parties."¹²⁰ To help courts, § 17526 offers a list of conduct that can constitute bad faith, but with the exception of one factor it essentially mirrors the ACPA's list in

112. See Sanderson, *supra* note 1, at 15.

113. CAL. ELEC. CODE § 18320 (West 2004).

114. *Id.* § 18320(c)(1)(D).

115. *Id.*

116. See *supra* note 9 and accompanying text.

117. See Lipton, *Who Owns Hillary.com*, *supra* note 5, at 72-73.

118. ELEC. § 18320 (c)(3).

119. *Id.* See Lipton, *Who Owns Hillary.com*, *supra* note 5, at 70.

120. CAL. BUS. & PROF. § 17525 (West 2001); see Lipton, *Who Owns Hillary.com*, *supra* note 5, at 84.

§ 1125(d)(1)(B)(i).¹²¹ The new addition in § 17526 is subsection (j), which makes it bad faith for a person “to mislead, deceive, or defraud voters.”¹²² Like the PCAA, however, this applies more to cyberfraud than cybersquatting, because a cybersquatter has no intent to “mislead, deceive, or defraud voters;” he is merely holding the domain name and offering it for sale in order to turn a profit.¹²³

California’s statutes are the only statutes of their kind thus far, although other states have unsuccessfully proposed similar bills.¹²⁴ Again though, both the PCAA and the Business and Professional Code provisions are limited because they pertain to cyberfraud more so than they do cybersquatting.¹²⁵

IV. POLITICAL CYBERFRAUD

While cybersquatting deals with registration of a domain name in order to turn a profit,¹²⁶ political cyberfraud entails conduct that starts with registration but lacks an intent to profit, instead looking beyond the domain name at what is housed there.¹²⁷ Political cyberfraud is using a website in a way that is related to the candidate, including using it to spread misleading or damaging information about a candidate or attempting to raise money under the name of that candidate.¹²⁸ However, looking at the website’s substantive content can mean serious First Amendment implications because courts fiercely protect political speech, especially the negative kind.¹²⁹ Indeed, the Supreme Court has recognized that “[t]he sort of robust political debate encouraged by the First Amendment is bound to produce speech that is critical of those who hold public office.”¹³⁰

This protection can lead to a cacophony of views and opinions from all directions, but the line between protected and unprotected speech is not and cannot be drawn at its subjective value: “[o]ne of the prerogatives of American citizenship is the right to criticize public men

121. BUS. & PROF. § 17526; *Cf.* 15 U.S.C. § 1125(d)(1)(B)(i) (2012).

122. BUS. & PROF. § 17526.

123. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 85.

124. *See* H.R. 1684, 2008 Leg. 94th Sess. (Mo. 2008); S. B. No. 1110, 57th Leg., First Reg. Sess. (Idaho 2003).

125. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 70, 84-85.

126. *See id.* at 85.

127. *See id.* at 92.

128. *Id.*

129. *See id.* at 95; *see also* N.Y. Times, *Co. v. Sullivan*, 376 U.S. 254, 269 (1964); *Ficker v. Tuohy*, 305 F. Supp. 2d 569, at 571-72 (D. Md. 2004).

130. *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 51 (1988).

and measures—and that means not only informed and responsible criticism but the freedom to speak foolishly and without moderation.”¹³¹ Those words by Justice Frankfurter ring equally as important in 2016 as they did in 1944 with new technologies such as the Internet offering more ways to comment on politicians and candidates for office.

Using a website merely to comment in support of or in opposition to a candidate is not the concern of this Comment. The issue here is commentary made under a guise of authority by housing it as a domain name confusingly similar to a politician’s or candidate’s name, which might dupe visitors into thinking that the website has more clout or truth than it does, frustrating their attempts to find the genuine campaign website.¹³² There is no question that individuals can make a myriad of statements regarding public matters and figures, and can do so as “foolishly” as they please.¹³³ When done under a false seal of authority though, the speech that the First Amendment trumpets threatens to undermine the very democratic process that sustains it.

A. *The ACPA’s Applicability and First Amendment Implications Discussed in Ficker*

While the ACPA primarily targets cybersquatting, it may still cover some instances of cyberfraud.¹³⁴ In order to pursue a remedy, any candidate would have to overcome two issues that arise under § 1125(d): establishing trademark rights in their names¹³⁵ and demonstrating the defendant’s “bad faith intent to profit.”¹³⁶ Anticipating the difficulty in demonstrating trademark rights in their names, some candidates might opt for § 8131 instead.¹³⁷ However, the personal name provision of § 8131 only applies if the domain name is registered “with the specific intent to profit . . . by selling the domain name for financial gain.”¹³⁸ While similar to § 1125(d)’s “bad faith intent to profit” standard, § 8131 requires the additional intent to sell the domain name while the former

131. *Baumgartner v. United States*, 322 U.S. 665, 673-74 (1944).

132. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 92-93.

133. *See Baumgartner*, 322 U.S. at 674.

134. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 105.

135. 15 U.S.C. § 1125(d) (2012) (allowing “the owner of a mark” to bring a civil suit); *see also supra* note 32 and accompanying text.

136. 15 U.S.C. § 1125(d)(1)(A)(i).

137. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 105-06; 15 U.S.C. § 8131 (2012); 15 U.S.C. § 1125(d).

138. 15 U.S.C. § 8131(1)(A).

could include keeping and using the website to generate a profit.¹³⁹ The advantage under § 8131, that candidates would not have to show trademark rights in their name, is therefore cancelled out by the additional intent to sell the domain name for profit.¹⁴⁰ Thus, § 8131 is better suited to address cybersquatting than cyberfraud in the political context.¹⁴¹ Differences aside, neither provision is especially applicable to political cyberfraud that lacks a profit-seeking motive, such as using the domain name solely to comment on a candidate, or to support a rival one.¹⁴²

As discussed earlier, *Ficker v. Tuohy* is the only case that has been brought under the ACPA regarding a campaign website.¹⁴³ In *Ficker*, Congressional candidate Robin Ficker's campaign website was housed at RobinFicker2004.com, but the defendant operated RobinFicker.com and used it to post negative news stories about Ficker.¹⁴⁴ Ficker's request for a temporary restraining order was denied because the harm to the defendants "clearly outweigh[ed]" the harm to him; he also failed to demonstrate a likelihood of success; and the public interest did not favor either party.¹⁴⁵

First, the court noted that because RobinFicker.com contained a disclaimer that it was not Mr. Ficker's official website and even contain a link to his actual website, visitors would not be misled.¹⁴⁶ Because there was no potential for confusion regarding Ficker's connection to the site, he could be harmed only by the information found there, which the court noted was protected by the defendant's First Amendment right to free speech.¹⁴⁷ The court emphasized that it was "particularly concerned" with the right to free speech, adding that "by entering the public arena as a candidate for political office, [Ficker had] invited comments and critique which operates in the spirit of healthy democracy in this country."¹⁴⁸

Moving on to Ficker's failure to show a likelihood of success, the court stated that it was "not convinced, at this point, that the ACPA

139. Compare 15 U.S.C. § 8131(1)(A), with 15 U.S.C. § 1125(d)(1)(A)(i).

140. *Id.*

141. See *supra* Section III.C.

142. See Lipton, *Who Owns Hillary.com*, *supra* note 5, at 106.

143. *Ficker v. Touhy*, 305 F. Supp. 2d 569 (D. Md. 2004); see *supra* Section III.C.

144. *Ficker*, 305 F. Supp. 2d at 571.

145. *Id.* at 571-72.

146. *Id.*

147. *Id.*

148. *Id.*

provides coverage for personal names that are not trademarked, where the websites have no commercial use.”¹⁴⁹ Once again, the court emphasized the importance of the First Amendment, finding it to be an overriding issue and noting that it has a “particularly important role in political campaigns.”¹⁵⁰

As the lone case in this area, *Ficker* provides the only glimpse into how the ACPA is applied to political websites. It demonstrates the unmistakable concern for protecting political speech, placing it above rights of candidates, who have “invited comments and critique.”¹⁵¹ In creating this hierarchy of rights during a campaign, *Ficker* is a clear statement that legitimate political speech is not made illegal by its location.

Apart from the court’s doubt that the ACPA protects politician’s names that are not already trademarked, an important aspect of political cyberfraud as shown in *Ficker* is the likelihood of confusion, a core precept of trademark law.¹⁵² Because the defendant’s website had a clear disclaimer that it was unofficial and even provided a link to Ficker’s official site, it was doubtful that any visitor would think RobinFicker.com was somehow official.¹⁵³

Ficker is an excellent demonstration of the issue concerning political cyberfraud: candidates highly dislike it and it can be disruptive of their campaign, but it would take a specific set of circumstances for a court to get involved, such as existing trademark protection in the name, a reasonable likelihood of confusion, and some commercial use.¹⁵⁴

B. Under the UDRP, Once Candidates Establish Rights in Their Names, They Must Overcome Protections of Political Speech

To establish a claim under the UDRP, paragraph 4(a) states that complainants must prove that the registrant of the domain name: (1) registered a domain name identical or confusingly similar to a mark

149. *Id.* at 572. The court rejected Ficker’s argument that the website had a commercial purpose and affected his law practice, finding that the website was solely political and only concerned with his congressional campaign. *Id.*

150. *Id.* The court concluded by stating that the public interest did not clearly favor either party: while fairness and integrity in the electoral process is important, there is an equal interest in preventing encroachment on free speech. *Id.*

151. *Id.*

152. See 15 U.S.C. § 1125(a)(1) (2012) (requiring likelihood of confusion for trademark infringement).

153. *Ficker*, 305 F. Supp. 2d at 571, 572.

154. See *id.*

in which the complainant has rights, (2) does not have any rights or legitimate interest in the name, and (3) registered and is using the domain name in bad faith.¹⁵⁵

As discussed above with cybersquatting, the first showing requires the complainant to demonstrate trademark rights in his name, which is not an easy hurdle to clear for candidates and politicians.¹⁵⁶ The other part of the first requirement, proving that the respondent's domain name is identical or confusingly similar to the complainant's now-protected one, is usually not difficult to prove for candidates, since their name is often used as or is a part of the domain name.¹⁵⁷ The inquiry under § 4(a)(i) is typically the same whether the alleged conduct is cybersquatting only or also includes use of the website for cyberfraud.¹⁵⁸

1. Respondent's Rights or Interests in the Domain Name

If a candidate is able to satisfy the first requirement, the next step is proving that the respondent has no rights or legitimate interests in the domain name.¹⁵⁹ The UDRP gives a list of three nonexclusive factors that can show a respondent's legitimate rights in the domain name: (1) the domain name is used "in connection with a bona fide offering of goods or services;" (2) the respondent is "commonly known by the domain name," either as a personal, business, or other organizational name; or (3) the respondent has "a legitimate noncommercial or fair use of the domain name, without intent for commercial gain" to mislead consumers or tarnish the mark at issue.¹⁶⁰

For political complainants, the first factor does not present a unique challenge compared to any other complainant.¹⁶¹ The second factor has a slight probability of arising, but it is not impossible: for example, in 2004 the Democratic Presidential ticket of John Kerry and John Edwards were unable to register "kerryedwards.com" because it had already been

155. *UDRP*, *supra* note 18, at para. 4(a); *see supra* note 47 and accompanying text.

156. *See supra* Section III.D.

157. *See* Sanderson, *supra* note 1, at 21.

158. *Compare* Clinton v. Dinoia, No. FA0502000414641, 2005 WL 853535, at *4 (Nat'l. Arb. F. Mar. 18, 2005) (domain name contained no political commentary), *with* Sizemore v. DIS, Inc., No. FA0312000221173, 2004 WL 3270344 (Nat'l. Arb. F. Feb. 26, 2004) (domain name housed information portraying the candidate in a negative light).

159. *UDRP*, *supra* note 18, at para. 4(a)(ii).

160. *Id.* at para. 4(c).

161. *See* Sanderson, *supra* note 1, at 22.

registered by a man named Kerry Edwards.¹⁶² Presumably, Mr. Kerry Edwards would satisfy the second factor because he is known by that domain name, thus leaving Kerry and Edwards with no remedy under the UDRP.¹⁶³

The third factor, however, could be the greatest burden to overcome for candidates because of the difficulty in determining whether commentary on a candidate constitutes a noncommercial or fair use.¹⁶⁴ For example, Senate candidate Doug Forrester brought a UDRP complaint because DougForrester.com was being used to redirect Internet users to an anti-abortion website.¹⁶⁵ The arbitrator found that the respondent had no legitimate rights or interests in the domain name because he was using the goodwill Forrester had created in his name to direct users to a website expressing opinions that the candidate did not endorse.¹⁶⁶

While *Forrester* did not delve into the respondent's free speech rights, the First Amendment was discussed when Congressman and Presidential candidate Ron Paul brought a complaint regarding RonPaul.com, which was being used as a fan site devoted to Paul.¹⁶⁷ Passing on the issue of whether he had trademark rights in his name, the arbitrator denied Paul's complaint because he failed to establish that the respondent violated all three requirements in paragraph 4(c).¹⁶⁸ Although RonPaul.com offered goods for sale, they were sold to promote Paul and the website's "primary purpose" was to provide news, information, and a political forum about Paul.¹⁶⁹ The respondent's legitimate interest in the site was strong because it provided "a place for political speech, which is at the heart of what the . . . First Amendment is designed to protect."¹⁷⁰

162. David McGuire, *Kerry Edwards Seeks Big Payout for Web Address*, WASH. POST (July 23, 2004, 8:50 AM), <http://www.washingtonpost.com/wp-dyn/articles/A8379-2004Jul23.html>.

163. See *UDRP*, *supra* note 18, at para. 4(c)(ii); see also *supra* note 42 and accompanying text.

164. See Sanderson, *supra* note 1, at 22.

165. *Forrester v. Hoffman*, No. FA0307000170644, 2003 WL 22700373, at *2 (Nat'l. Arb. F. Sept. 3, 2003). The site also linked the political struggle in the Middle East to the End of Times and espoused the belief that computers are instruments of Satan. *Id.*

166. *Id.* at *4. This use was neither a bona fide offering of goods or services under paragraph 4(c)(i) nor a fair use under paragraph 4(c)(iii). *Id.*

167. *Paul v. Whois Privacy Servs.*, No. D2013-0278, 2013 WL 2390820, at *4, *12 (WIPO May 8, 2013).

168. *Id.* at *12.

169. *Id.* The panel added that any money made on those sales was not sufficient to qualify as commercial use. *Id.*

170. *Id.*

Moreover, there was no clear intent to mislead visitors because the website had explicit disclaimers that it was not Paul's official site.¹⁷¹

While other panels have found that political commentary is a legitimate use, they have supported their findings with little to no reasoning.¹⁷² Bill Sizemore, a political figure in Oregon, claimed that both BillSizemore.com and BillSizemore.org were used by the respondent "on behalf of labor unions, [his] arch enemies" to spread propaganda against him.¹⁷³ The discussion of paragraph 4(a)(ii) started with the heading "FINDING FOR COMPLAINANT" and contained no substantive discussion.¹⁷⁴ The respondent conceded that he had no defense under paragraph 4(c)(i), and analysis of paragraph 4(c)(ii) and (iii) consisted of a one-sentence summary of Sizemore's argument on each factor followed by string cites to other UDRP decisions.¹⁷⁵ Thus, the findings in favor of Sizemore were made without explicitly accepting his contentions, examining the respondent's defenses, or any substantive discussion at all.¹⁷⁶ Little more reasoning was given when former Democratic President Bill Clinton brought a complaint over William Clinton.com, WilliamJClinton.com, and PresidentBillClinton.com.¹⁷⁷ The arbitrator found that using the domain names to route visitors to an official Republican Party website satisfied neither paragraph 4(c)(i) nor paragraph 4(c)(iii) and cited a handful of other decisions.¹⁷⁸

One panel has noted in dicta that using a website to comment on a candidate makes determining paragraph 4(a)(ii) difficult.¹⁷⁹ When London mayor Boris Johnson brought a complaint for the domain name BackBoris.com, the panel found that the respondent did not have a legitimate interest in the domain name because it was being used solely to generate pay-per-click advertising revenue.¹⁸⁰ However, it stated that if the website "posted only information and links about [Johnson] and his policies (whether to 'back' his positions or undermine them), the Panel

171. *Id.*

172. *See generally*, Sizemore v. DIS, Inc., No. FA0312000221173, 2004 WL 3270344 (Nat'l. Arb. F. Feb. 26, 2004); Clinton v. Web of Deception, No. FA0904001256123, 2009 WL 1638033 (Nat'l. Arb. F. June 1, 2009).

173. *Sizemore*, 2004 WL 3270344, at *2.

174. *Id.* at *4-5.

175. *See id.*

176. *Id.*

177. *Clinton*, 2009 WL 1638033, at *7.

178. *Id.*

179. *Johnson v. Belize Domain Whois Service*, No. D2010-1954, 2011 WL 670328, at *5 (WIPO Jan. 24, 2011).

180. *Id.*

would have the difficult task of determining whether that is a legitimate interest—an issue that has split UDRP panels.¹⁸¹

Given that the First Amendment implications in evaluating cyberfraud have not been clearly established by Federal courts,¹⁸² it is not surprising that UDRP panels have failed to come to a consensus on what constitutes legitimate noncommercial or fair use when political commentary is involved. UDRP panelists seem understandably wary of wading too deeply into the subject given that they are experts in commercial trademark, rather than constitutional law.¹⁸³ Indeed, the panel's statement in *Johnson* that the determination is more difficult when the website makes political commentary shows that while UDRP arbitrators consider free speech issues, there is little predictability in what decision they might reach, and even less in why they reach that decision.¹⁸⁴ Considering the lack of agreement among panelists on how a political complainant can establish trademark rights in his or her name despite the existence of what seem to be bright line rules,¹⁸⁵ it seems that the only predictable outcome for political complainants might be the lack of one.

2. The Final Requirement: Demonstrating Respondent's Bad Faith

The last of the elements that complainants must prove under the UDRP is that the respondent registered the domain name in bad faith.¹⁸⁶ The UDRP gives four nonexclusive circumstances in paragraph 4(b) that can show bad faith by respondents: (1) purchasing the domain name to sell it to the complainant “for valuable consideration in excess” of the cost to acquire it; (2) registering the domain name to prevent the owner of the mark from using that name, provided that the respondent has “engaged in a pattern of such conduct”; (3) registering the domain name to disrupt a competitor's business; and (4) using the domain name for commercial gain through attracting Internet users by creating a likelihood of confusion regarding “the source, sponsorship, affiliation, or endorsement” of the domain name.¹⁸⁷

181. *Id.*

182. *See supra* Section IV.A.

183. *See* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 108-09.

184. *See Johnson*, 2011 WL 670328, at *5.

185. *See supra* Section IV.B.1.

186. *UDRP*, *supra* note 18, at para. 4(a)(iii).

187. *Id.* at para. 4(b).

The first example listed in paragraph 4(b) can be proved by showing that the respondent offered to sell the domain name to the complainant, but some panels will not accept an offer to sell the domain name as evidence of bad faith if the complainant solicited or baited the offer.¹⁸⁸ Establishing the second circumstance hinges on showing a pattern of similar conduct by the respondent, which can be done with the help of various commercial services like Mark Monitor that allow complainants to catalogue domain name portfolios of respondents.¹⁸⁹ Complainants have also used newspaper articles to demonstrate repeated conduct.¹⁹⁰ The importance of complainants establishing strong trademark rights in their names arises again here because registering a domain name that contains the complainant's mark despite knowledge of the rights in that mark can satisfy paragraph 4(b)(iii) on its own.¹⁹¹ However, paragraph 4(b)(iii) discusses disruption of business, so a candidate would probably need to demonstrate disruption of more than just a political campaign.¹⁹²

The fourth example often relies on whether or not the respondent is using the domain name for commercial gain.¹⁹³ This can be proven by simply pointing to advertising on the website.¹⁹⁴ The intent to profit by using the candidate's name and reputation can be even clearer if advertising is accompanied by links to other political websites.¹⁹⁵ However, the arbitrator in *Warner* stated that although using a candidate's name "as a domain name will attract internet users, the attraction is

188. Sanderson, *supra* note 1, at 24. Whether or not a panel refuses to consider a baited or solicited offer to sell depends on whether it applies Federal Rule of Evidence 408, which states that attempts to compromise are not admissible. *Id.*; see FED. R. EVID. 408(a)(1)(2011). However, the panel may not explicitly reference the Rule. See, e.g., *Warner v. Larson*, No. FA0009000095746, 2000 WL 33675081, at *4 (Nat'l. Arb. F. Nov. 15, 2000) ("[S]imply considering to sell or even offering to sell a domain name is insufficient to amount to bad faith under the ICANN Policy, because the domain name must be registered *primarily* for the purpose of selling it to the owner . . . for an amount in excess of out-of-pocket expenses.").

189. Sanderson, *supra* note 1, at 25; see, e.g., *MarkMonitor Brand Protection*, MARKMONITOR, <https://www.markmonitor.com/services/brand-protection> (last visited Nov. 9, 2016).

190. *McLellan v. Smartcanuk.com*, Nos. AF-303a, AF-303b, 2000 WL 33647281, at *2 (eResolution Sept. 25, 2000).

191. *Calvert v. Domain Strategy, Inc.*, No. FA0306000162075, 2003 WL 24129957, at *4 (Nat'l. Arb. F. Aug 1, 2003).

192. See *UDRP*, *supra* note 18, at para. 4(b)(iii).

193. *Id.* at para. 4(b)(iv).

194. *McLellan*, 2000 WL 33647281, at *3; *Clinton v. Dinoia*, No. FA0502000414641, 2005 WL 853535, at *5 (Nat'l. Arb. F. Mar. 18, 2005).

195. *Johnson v. Belize Domain Whois Servs.*, No. D2010-1954, 2011 WL 670328, at *6 (WIPO Jan. 24, 2011).

arguably for *political*, not *commercial* gain,” emphasizing the importance of establishing more than a political basis for the complaint is important.¹⁹⁶ Interestingly, while resolving to an adult-oriented website constituted bad faith under paragraph 4(b)(iii) in *Calvert*, resolving to a rival political party’s website failed to show bad faith under paragraph 4(b)(iv) when Bill Clinton brought a complaint, demonstrating again the importance of commercial use to UDRP panels.¹⁹⁷

Unfortunately, UDRP panels have not clearly addressed whether a critical website constitutes bad faith: in two decisions involving such uses of the disputed domain name, the panels found that the candidate did not have rights in his or her name and ended the discussion there.¹⁹⁸ The one decision to address the issue was *Calvert*, but the respondent there failed to submit any response so the candidate’s contentions were accepted with little discussion by the panel.¹⁹⁹ While there is a dearth of discussion about whether using the domain name to criticize a candidate would constitute bad faith, it appears clear that a lack of commercial interests involved would result in no such finding. Additionally, even if a critical use was found to constitute bad faith, it is unclear how that might clash with the respondent’s legitimate rights and interests in the domain name under paragraph 4(a)(ii).²⁰⁰

C. State Law Solutions

1. California Political Cyberfraud Abatement Act (PCAA)

California has taken the lead in creating laws against political cyberfraud, starting with the PCAA.²⁰¹ The PCAA proscribes conduct regarding political websites with the intent to: (1) deny someone access to a political website; (2) deny someone the opportunity to register the domain name for a political website; or (3) cause someone to reasonably

196. Warner v. Larson, No. FA0009000095746, 2000 WL 33675081, at *4 (Nat’l. Arb. F. Nov. 15, 2000).

197. Compare *Calvert v. Domain Strategy, Inc.*, No. FA0306000162075, 2003 WL 24129957, at *4 (Nat’l. Arb. F. Aug 1, 2003) (resolving to an adult-oriented website was bad faith under ¶ 4(b)(iii)), with *Clinton v. Web of Deception*, No. FA0904001256123, 2009 WL 1638033, at *8 (Nat’l. Arb. F. June 1, 2009) (resolving to a rival political party website was not bad faith under ¶ 4(b)(iv)).

198. *Fields for Senate v. Toddles Inc.*, Case No. D2006-1510 (WIPO Mar. 14, 2007), <http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-1510.html>; *Convergència Democràtica de Catalunya v. ar mas*, Case No. DTV2003-0005 (WIPO Dec. 19, 2003), <http://www.wipo.int/amc/en/domains/decisions/html/2003/dtv2003-0005.html>.

199. *Calvert*, 2003 WL 24129957, at *4.

200. See *supra* Section IV.B.2.

201. See *supra* Section III.E.

believe that a political website was created by someone other than the person that actually created it.²⁰² There are some important limitations to the PCAA, however. The first is obvious: as a state statute its jurisdiction is limited.²⁰³ This jurisdictional issue is important because cyberfraud is not always committed by a person in one country against another in the same country, much less within the same state.²⁰⁴ The other is that the act defines a political website as a “site that urges or appears to urge the support or opposition of a ballot measure.”²⁰⁵ Since individual candidates are not a ballot measures, they might not have standing even if they can establish California jurisdiction.

2. California Business and Professional Code § 17525

As discussed above, § 17525 of California’s Business and Professional Code makes it unlawful to register a domain name identical or confusingly similar to another person’s name in bad faith.²⁰⁶ Section 17525 is followed in § 17526 by a list of circumstances that can show bad faith or a lack thereof that closely tracks the one found in the ACPA, with one exception.²⁰⁷ Subsection (j) of § 17526 adds a factor that the ACPA lacks: “The intent of a person alleged to be in violation of this article to mislead, deceive, or defraud voters.”²⁰⁸ This is more germane to cyberfraud than cybersquatting because misleading, deceiving, or defrauding voters implies that something beyond a confusingly similar domain name is at issue.²⁰⁹ A person who registers a domain name confusingly similar to a candidate’s name and attempts to pass the website off as the candidate’s would probably violate other parts of § 17526.²¹⁰ But subsection (j) could deal with sites that do not try to pass themselves off as legitimate and contain more than valid comment or criticism that might be protected under political speech.²¹¹ However, this extra layer of protection might be redundant because other factors might still deal with such conduct: for example, subsection (d) advises courts

202. CAL. ELEC. CODE § 18320(c)(1) (West 2004).

203. *See supra* note 119 and accompanying text.

204. *Id.*

205. ELEC. § 18320(c)(3).

206. *See supra* Section III.E.; CAL. BUS. & PROF. § 17525 (West 2001).

207. CAL. BUS. & PROF. § 17526 (West 2001). *Cf.* 15 U.S.C. § 1125(d)(1)(B)(i) (2012).

208. BUS. & PROF. § 17526(j).

209. *See id.*; *see also* Lipton, *Who Owns Hillary.com*, *supra* note 5, at 104.

210. *See* BUS. & PROF. § 17526(e) (discussing intent to tarnish or disparage a person’s name by creating a likelihood of confusion as to the site’s source, affiliation, or endorsement).

211. *See id.* at § 17526(j).

to consider any noncommercial or fair use of the website, and any misleading, deceiving, or fraudulent material would likely fail under that standard already.²¹²

The limited jurisdictional reach and redundancy with the ACPA might be why the statute is rarely invoked: the first case to allege violations of § 17525 in regards to political websites reached the California Court of Appeals in 2015, but discussion was focused on other issues and the violation of the Business and Professional Code was left for remand.²¹³

Due to the similarities between § 17526's bad faith factors and those found in the ACPA, this state statute is essentially a way to protect purely intrastate cybersquatting or cyberfraud that federal courts have no jurisdiction over. Given that this conduct is often international, § 17525 only offers a slight level of additional protection.²¹⁴ While its one additional factor may explicitly discuss conduct prohibited by other factors, it does serve the important role of specifically targeting voters, which many statutes regarding online activity lack.

3. Defamation

The fact that political speech is generally protected by the First Amendment “does not mean that *any* speech about a public figure is immune from sanction in the form of damages.”²¹⁵ Candidates could sue a website's operator for defamation, but public figures are subject to the heightened “actual malice” standard, requiring them to prove that the statement was made “with knowledge that it was false or with reckless disregard of whether it was false or not.”²¹⁶ Assuming actual malice is demonstrated, the available remedies would cure the defamation itself, but the domain name would remain with the defendant, which is only a short-term victory for any candidate.²¹⁷ However, defamation could still serve as an effective way to halt damaging false information from being spread during an election.

212. *See id.* at § 17526(d).

213. *See Collier v. Harris*, 192 Cal. Rptr. 3d 31, 44 (Cal. Ct. App. 2015).

214. *See supra* note 111 and accompanying text.

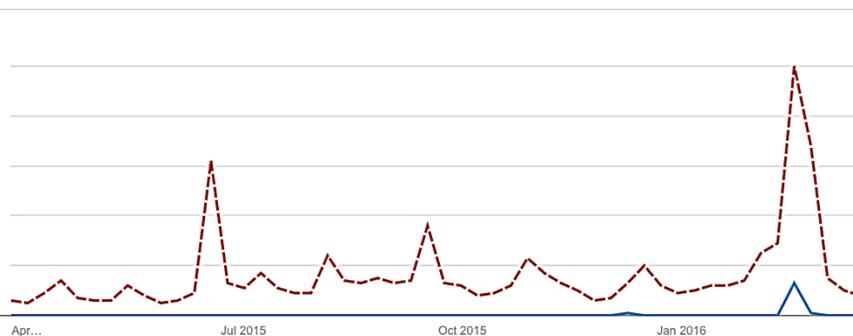
215. *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 52 (1988).

216. *N.Y. Times, Co. v. Sullivan*, 376 U.S. 254, 279-80 (1964). The “actual malice” requirement applies to candidates as well as politicians. *See Monitor Patriot Co. v. Roy*, 401 U.S. 265, 271-72 (1971).

217. *See Boshers, supra* note 2, at 146.

D. Solutions Outside Court: Let the Press Reveal the Conduct

If a legal remedy is not possible, or candidates do not want to spend the requisite time and money seeking one, they can instead appeal to the court of public opinion through the press. Media coverage of campaigns is prevalent from national to state to local races, and the media has a unique ability to shape public opinion during campaigns.²¹⁸ At the very least, media reports about potential cyberfraud or similar conduct can inform voters that the website is not official, endorsed, or supported by the candidate. In the table below, courtesy of Google Trends, the popularity of two search terms—“JebBush.com” (the solid line) and “Jeb Bush” (the dotted line)—is shown between April 2015 and March 2016, during which Bush was campaigning for President. Around January 17, 2016, it was reported that JebBush.com routed visitors straight to fellow contender Donald Trump’s website.²¹⁹ The dotted line shows that users searched for information about Bush with various levels of frequency over this time period, while the solid line’s only spike, peaking on January 17, shows that people were not informed about this issue, or uninterested in it until the media reported this rerouting issue.



While informing voters of potential cyberfraud can help the candidate by increasing awareness, a court or UDRP panel might be less inclined to find a likelihood of confusion if a legal remedy is later sought. Another potential incentive is that spreading the word through the media might result in the public getting actively involved, as Ron

218. See Jane S. Schacter, *The Pursuit of “Popular Intent”: Interpretive Dilemmas in Direct Democracy*, 105 YALE L.J. 107, 132 (1995).

219. See *supra* notes 31-32 and accompanying text.

Paul found in 2013.²²⁰ After he mentioned in a radio interview that someone else was using RonPaul.com, his supporters reached out to the registrant of the domain name urging a sale or transfer.²²¹ While their efforts were unsuccessful, they show the benefits of spreading awareness about potential cyberfraud by using the media's wide reach.²²²

Perhaps the best-case scenario of media involvement might be the activity ending all together. In *Collier v. Harris*, the defendant ceased his alleged cyberfraud activity after being contacted by a local news reporter who asked if he was behind the conduct.²²³ While stopping was not enough to save the defendant from trial in *Collier*, it might be enough for others who are not keen on a trial.

V. CONCLUSION

Neither type of conduct discussed in this Comment, cybersquatting and cyberfraud, are easily dealt with legally. The most likely reason for this is the requirement that candidates have some degree of trademark protection in their names in order to pursue either a federal remedy under the ACPA or one under the UDRP in arbitration,²²⁴ and the subsequent doubt that federal courts and UDRP panels have cast on the potential protection of individual politicians' names.²²⁵ Despite the difficulties in seeking remedies under both, candidates appear more likely to use the UDRP due to its lower price tag, quicker timeline, and perhaps its more relaxed requirements on trademark protection.²²⁶

However, courts and panels are more likely to face conduct that goes beyond pure cybersquatting, as most of the decisions above involve the domain names being put to some use. Purely commercial uses, such as generating revenue through advertising, have not been looked upon

220. Paul v. Whois Privacy Servs., No. D2013-0278, 2013 WL 2390820, at *8-9 (WIPO May 8, 2013).

221. *Id.*

222. *Id.*

223. *Collier v. Harris*, 192 Cal. Rptr. 3d 31, 36 (Cal. Ct. App. 2015).

224. See 15 U.S.C. § 1125(d) (2008) (allowing "the owner of a mark" to bring a civil suit); *UDRP*, *supra* note 18, at para. 4(a)(i) (requiring complainants to assert that the "domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.").

225. See *Ficker v. Tuohy*, 305 F. Supp. 2d 569 (D. Md. 2004); *Townsend v. B.G. Birt*, No. D2002-0030, 2002 WL 827005 (WIPO Apr. 11, 2002).

226. See *supra* notes 56-58 and accompanying text; *Townsend*, 2002 WL 827005, at *4 ("It is sufficient that the Complainant can demonstrate that she has rights in a common law trademark.").

favorably,²²⁷ but when the allegedly infringing website is used for political commentary, the First Amendment muddies up the examination by requiring political freedom to be balanced with the rights of candidates.²²⁸ Due to a lack of concrete answers, candidates' two best options for winning the domain name from its registrant is either to buy it or try their luck under the UDRP.²²⁹ However, the law is far from clear in this area, and the best option may be to register a different name and move on with the rest of their campaign.

227. *Johnson v. Belize Domain Whois Serv.*, No. D2010-1954, at *5 (WIPO Jan. 24, 2011).

228. *See id.*; *Ficker*, 305 F. Supp. 2d at 571-72.

229. *See supra* Sections III.B, III.D.