"Username Jacking" in Social Media: Should Celebrities and Brand Owners Recover from Social Networking Sites When Their Social Media Usernames are Stolen?

Dan Malachowski

Follow this and additional works at: https://via.library.depaul.edu/law-review

Recommended Citation
Dan Malachowski, "Username Jacking" in Social Media: Should Celebrities and Brand Owners Recover from Social Networking Sites When Their Social Media Usernames are Stolen?, 60 DePaul L. Rev. 223 (2010)
Available at: https://via.library.depaul.edu/law-review/vol60/iss1/7

This Comments is brought to you for free and open access by the College of Law at Via Sapientiae. It has been accepted for inclusion in DePaul Law Review by an authorized editor of Via Sapientiae. For more information, please contact wsulliv6@depaul.edu, c.mcclure@depaul.edu.
"USERNAME JACKING" IN SOCIAL MEDIA: SHOULD CELEBRITIES AND BRAND OWNERS RECOVER FROM SOCIAL NETWORKING SITES WHEN THEIR SOCIAL MEDIA USERNAMES ARE STOLEN?

INTRODUCTION

Former vice presidential candidate Sarah Palin posted a status update¹ on Facebook asking for recipe recommendations for a salmon that her husband Todd had caught.² Baseball manager Tony La Russa tweeted³ that there were no drunk-driving incidents on the St. Louis Cardinals' latest road trip.⁴ These, like many other status updates and tweets, were not really sent by Sarah Palin or Tony La Russa. Imposters had “jacked”⁵ Palin’s and La Russa’s social media usernames. After involving their lawyers, Palin and La Russa were able to recover their usernames.⁶ Given the massive growth of social networking⁷—and the high visibility that social media sites achieve on search engine

¹. A status update is a message posted by a Facebook user for that user’s friends to see.
  ³. A “tweet” is a 140-character message that is sent through Twitter, a micro-blogging social networking site. TWITTER SUPPORT: FREQUENTLY ASKED QUESTIONS, http://help.twitter.com/forums/10711/entries/13920 (last visited Jan. 25, 2011). Tweets are distributed to the author’s feed subscribers, known as “followers,” and also appear on the author’s Twitter homepage. Id.
  ⁵. The term “jacked” will be used hereinafter to refer to instances in which an imposter has stolen or squatted on a celebrity’s or brand’s social networking site username.
  ⁶. See infra notes 69, 80–86 and accompanying text.
results pages for celebrity and brand name queries—social network usernames have become extremely valuable. Thus, cybersquatters, spammers, impersonators, and celebrity and brand fans have jacked many high-profile usernames.

Username-jacking victims who seek a legal remedy can go after the individuals who jacked their profiles only if they can find them. Many times, it will be difficult to locate the perpetrator because he registered the celebrity’s or brand’s profile using a fake e-mail address or masked IP address. This—in addition to the social site’s likely ability to pay larger damages than an individual jacker—may lead the jacking victim to sue the social site itself. This Comment will analyze the potential claims that a username-jacking victim may bring against a social site and the likelihood that those claims will succeed.

Section 230 of the Communications Decency Act (the CDA) offers social networks limited immunization from many torts of their third-party users, including defamation and intentional infliction of emotional distress. But § 230(e)(2) states that Web site operators are not immune from “any law pertaining to intellectual property.” Part II of this Comment chronicles the rise of username jacking. It then discusses the potential claims a jacking victim could bring against a social networking site. Thus, Part II sets out the intellectual property claims that could apply to username-jacking situations, including cybersquatting, trademark violations, and right of publicity violations.

Part III analyzes whether a username-jacking victim should recover for any of these intellectual property claims. Part III argues that cybersquatting laws should not apply to usernames. It then argues that a jacking victim should recover for a trademark violation only when users actually believe that the fake profile is the celebrity’s or brand’s real profile. Part III then cautions against allowing celebrities to recover on right of publicity claims under § 230, an issue over

8. See infra notes 35–40 and accompanying text.
9. See infra notes 30–41 and accompanying text.
10. See infra notes 42–64 and accompanying text.
11. See infra notes 80–87 and accompanying text.
12. See infra notes 92–108 and accompanying text.
14. See infra notes 42–64 and accompanying text.
15. See infra notes 88–188 and accompanying text.
16. See infra notes 110–19 and accompanying text.
17. See infra notes 121–51 and accompanying text.
18. See infra notes 155–88 and accompanying text.
19. See infra notes 189–335 and accompanying text.
20. See infra notes 246–91 and accompanying text.
which federal courts are split.21 Part IV claims that the social sites have sufficient username dispute resolution processes in place and that it is a waste of judicial resources for celebrities and brands to sue for username jacking.22 The ultimate goals of this Comment are to show the difficulty in succeeding in a username-jacking suit and to encourage brands and celebrities to work with the social networking sites to recover jacked usernames.

II. BACKGROUND

This Part describes the value of a social network username, which has spurred the rise of username jacking.23 It discusses the resolution of specific username-jacking instances and then outlines the legal claims a jacking victim could bring against a social networking site.24 Section 230 of the CDA does not immunize Web site operators from intellectual property claims.25 Thus, this Part focuses on intellectual property claims, including cybersquatting26 and trademark violations.27 It also discusses the split in authority as to whether § 230 bars right of publicity claims.28

A. The Value of Social Media Usernames

Facebook, Twitter, MySpace, and LinkedIn enable people to claim their usernames in the URLs of their profile pages—for example, http://twitter.com/TonyLaRussa or http://www.facebook.com/cocacola. Usernames are called “vanity URLs” or, on Twitter, “handles.”29 In light of the substantial growth of social networking sites,30 it is critical for celebrities and trademark holders to own their social media usernames. Controlling a username is becoming as valuable as controlling the brand’s or celebrity’s native site.31 Usernames are valuable because social networking has changed the way in which brands and celebrities market themselves and how consumers make purchase

22. See infra notes 338–51 and accompanying text.
23. See infra notes 30–64 and accompanying text.
24. See infra notes 88–188 and accompanying text.
26. See infra notes 110–20 and accompanying text.
27. See infra notes 121–53 and accompanying text.
30. See supra note 7.
31. “Native site” will be used hereinafter to refer to a celebrity’s or brand’s traditional .com location; for example www.tonylarussa.com or www.cocacola.com.
decisions. Consumers want to interact with brands via social networking sites; forty percent of consumers have “friended” a brand on Facebook.32 These interactions can lead to direct sales—Dell Computers used its Twitter page to drive two million dollars in sales in the first half of 2009.33 Social networking sites also give brands the ability to communicate directly with consumers, solve their problems, and provide them with information.34 When a brand’s social username is jacked, someone other than the brand owner controls that brand’s message in the marketplace.

Individuals are likely to come across jacked profiles while searching for brands and celebrities within social networks and on search engines like Google. Search engines strive to provide searchers with the most relevant and helpful search results. Social media sites satisfy consumer needs in unique new ways35 and are thus increasingly being incorporated into search results.36 In determining relevancy, search engines take into account, among other factors, a page’s URL, title, and content.37 The social media username is included in the profile page’s URL (facebook.com/sarahpalin), title (“Sarah Palin — Facebook”), and content.38 Thus, search engines often rank Facebook, Twitter, and MySpace pages highly in brand and celebrity name search results. For instance, a Google search for “Sarah Palin”

34. H&R Block uses its Facebook page, facebook.com/hrblock, to interact with consumers by providing them tax advice. For instance, one user posted, My wife and I are getting ready to buy a new door to take advantage of the energy tax credit before the end of the year. I know that there were some changes made this year that make it harder to get the credit. Are there any changes coming for 2010? Mark Pannell, Posting to H&R BLOCK FACEBOOK PROFILE (Oct. 13, 2009, 9:17 AM), http://www.facebook.com/hrblock.
35. Consumer needs include connecting with friends, sharing content, talking about products, and interacting with brands.
shows facebook.com/sarahpalin as the fourth-ranked search result. If brands and celebrities do not control their social media pages, they risk losing control of how they would like their brand portrayed in the search results. A user searching for a brand on Google could easily come across a social media page that looks like an official brand page but is actually a gripe page, parody page, or page controlled by that brand’s competitor.

B. The Rise of Social Network Username Jacking

Jacking is possible because Facebook, Twitter, LinkedIn, and MySpace give out usernames on a first-come, first-serve basis. For instance, when a user registers for a Twitter account, he can pick any username as long as that name is not already taken by another user. Celebrities and politicians whose names have been jacked on social networking sites include President Barack Obama, comedians


40. Erik J. Heels, The Brand Wars Are Coming! How to Defend Your Brands on the Internet, LAW PRAC., July–Aug. 2007, at 24, 26 (commenting that, because sites like MySpace “are highly ranked by Google, you could find your brands in highly ranked search results for URLs that are not under your control”).

41. For instance, a Google search for comedian “Stephen Colbert” shows a fake Colbert Twitter page, twitter.com/stephencolbert, as the sixth-ranked search result. Google, supra note 39 (search for “Stephen Colbert”). To the average Internet searcher, there is no indication that this page is a fake one—in fact, it has over 386,000 followers as of June 2010. See Stephen Colbert on Twitter, http://twitter.com/stephencolbert (last visited Jan. 25, 2011). Colbert’s real Twitter page is twitter.com/StephenAtHome, which is a “verified account.” A verified account carries a special logo that indicates Twitter has “been in contact with the person or entity the account is representing and verified that it is approved.” Verified Account, Twitter, http://twitter.com/help/verified (last visited Jan. 25, 2011); see also infra note 344 and accompanying text.

42. See Blaise DiPersia, Coming Soon: Facebook Usernames, FACEBOOK BLOG (June 9, 2009, 2:11 PM), http://blog.facebook.com/blog.php?post=90316352130 (commenting on the launch of Facebook vanity URLs and how users will be able to choose a username starting at midnight on June 13, 2009 on a first-come, first-serve basis); Steve Patrizi, Strengthening Your Professional Brand Through LinkedIn, LINKEDIN BLOG (Sept. 26, 2007), http://blog.linkedin.com/2007/09/26/post-81 (encouraging users to claim their vanity URL on LinkedIn); see also Erik J. Heels, How to Twittersquat the Top 100 Brands, ERIK J. HEELS BLOG (Jan. 8, 2009), http://erikjheels.com/?p=1298.

43. See Create an Account, TWITTER, https://twitter.com/signup (last visited Jan. 25, 2011) (if a username types a name that is taken in the “username” box, he will be told to “pick a unique name”).

Whoopi Goldberg⁴⁵ and Tina Fey,⁴⁶ actor Christopher Walken,⁴⁷ former Secretary of State Condoleezza Rice,⁴⁸ Microsoft founder Bill Gates,⁴⁹ reporter Geraldo Rivera,⁵⁰ deceased rapper The Notorious B.I.G.,⁵¹ NFL players Peyton Manning⁵² and Ben Roethlisberger,⁵³ rapper Kanye West,⁵⁴ and actor Gary Busey.⁵⁵

In June 2009, the Facebook username “Governor Palin” was jacked by a former film executive doing a research experiment.⁵⁶ The jacker uploaded a picture and started posting earnest status updates; some users believed the updates were from the real Sarah Palin.⁵⁷ The profile gained 600 friends.⁵⁸ Fake Palin’s status updates later became more satirical and then outright offensive.⁵⁹ Facebook shut down the profile after two months.⁶⁰

The most publicized case of username jacking involved the manager of the St. Louis Cardinals, Tony La Russa. The @TonyLaRussa Twitter handle was jacked in April 2009 and used to falsely portray La

---


⁴⁶ Joshua Rhett Miller, ‘*Twitterjacking*’ — *Identity Theft in 140 Characters or Less*, FOXNEWS.COM (May 1, 2009), http://www.foxnews.com/story/0,2933,518480,00.html.

⁴⁷ Id.

⁴⁸ Id.

⁴⁹ Id.

⁵⁰ Id.

⁵¹ Id.


⁵⁵ Id.; see also infra notes 76–77 and accompanying text.

⁵⁶ Rosman, supra note 2.

⁵⁷ Most updates were about God and America, including, “Happy 4th of July and God Bless!!!” Id.

⁵⁸ Id.

⁵⁹ Updates ranged from the reasonably believable—“I need a salmon recipe for tonight. Todd just brought home a fresh one. Something spicy!” (eliciting dozens of recipe responses from her friends)—to the offensive: “GOD LOVES US ALL, no matter how black or African, or even gay or Jewish we are.” Id.
The profile, unlike the one for fake Governor Palin, was obviously a parody from day one.62

Brands are also not immune to username jacking. In January 2009, a person within the Michigan-based public relations firm Marx Layne jacked the Twitter handle of a rival firm, Tanner Friedman, and started distributing malicious tweets.63 Tanner Friedman is not alone; one legal commentator found that at the start of 2009, ninety-three of the top 100 global brands had been “Twitterjacked.”64

C. Reclaiming a Social Network Username

Social networking sites prohibit the selling of usernames and reserve the right to reclaim names when they deem appropriate.65

61. Tweets by the fake La Russa referenced the 2007 drunk-driving death of Cardinals’ pitcher Josh Hancock, as well as La Russa’s own 2007 driving under the influence charge. These tweets included, “Lost 2 out of 3, but we made it out of Chicago without one drunk driving incident or dead pitcher” and “drinking a cold Zima and wishing fucking Hancock was alive, I bet he could’ve gotten [opponent] Jack Wilson out.” Complaint, La Russa v. Twitter, Inc., No. CGC-09-488101, at Exhibit A (Cal. Super. Ct. May 6, 2009). The La Russa profile had only four followers. Id.; see also Tony La Russa Sues Twitter over Alleged Fake Page, PRESS OF ATLANTIC CITY, June 4, 2009, at B3.

62. Fake La Russa wrote in his bio, “Parodies are fun for everyone.” Complaint, LaRussa, at Exhibit A.

63. Andrew Moshirnia, Brandjacking on Social Networks: Twitter, Malicious Ghost Writing, and Corporate Sabotage, CITIZEN MEDIA LAW PROJECT (July 15, 2009), http://www.citmedia-law.org/blog/2009/brandjacking-social-networks-twitter-malicious-ghost-writing-and-corporate-sabotage (commenting that Tanner Friedman learned that the @TannerFriedman handle was created by someone within rival firm Marx Layne after Twitter provided the firm, by court order, with the IP address associated with the creation of the account).

64. Heels, supra note 42. BP was another corporate Twitter-jacking victim during the 2010 Gulf of Mexico oil spill. See Ki Mae Heussner, Fake BP Twitter Account Mocks Oil Spill PR Efforts, ABC News (May 25, 2010), http://abcnews.go.com/Technology/fake-bp-twitter-account-mocks-oil-spill-pr/story?id=10737669. The fake BP profile was used to parody BP’s response to the oil spill and has gained more than 190,000 followers as of September 2010. BP PUBLIC RELATIONS ON TWITTER, http://twitter.com/BPGlobalPR (last visited Jan. 25, 2011). Exxon Mobil was also Twitter jacked. A woman posing as an Exxon employee created the profile twitter.com/ExxonMobilCorp and began responding to questions about the company’s direction. See Jeremiah Owyang, How “Janet” Fooled the Twittersphere (and Me) She’s the Voice of Exxon Mobil, WEB STRATEGIST BLOG (Aug. 1, 2008), http://www.web-strategist.com/blog/2008/08/01/how-janet-fooled-the-twittersphere-shes-the-voice-of-exxon-mobil/.

65. Statement of Rights and Responsibilities, FACEBOOK, http://www.facebook.com/terms.php (last visited Jan. 25, 2011) (“You will not transfer your account . . . to anyone without . . . our written permission. . . . [W]e reserve the right to remove or reclaim it if we believe appropriate (such as when a trademark owner complains about a username that does not closely relate to a user’s actual name).”); User Agreement, LINKEDIN, http://www.linkedin.com/static?key= user_agreement (last visited Jan. 25, 2011) (“You agree to . . . refrain from selling, trading, or otherwise transferring your LinkedIn account to another party . . . .”); Terms & Conditions, MYSPACE, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Jan. 25, 2011) (stating that “selling or otherwise transferring your profile” is prohibited and that MySpace can “terminate your access . . . at any time, for any or no reason”); The Twitter Rules, TWITTER SUPPORT, http://help.twitter.com/forums/26257/entries/18311 (last visited Jan. 25, 2011) (“We re-
Many celebrities and brands have been able to reclaim their usernames without legal action. For example, President Barack Obama reclaimed myspace.com/barackobama in 2007.66 MySpace turned the page over to the Obama campaign at its request, commenting that Obama “had the right to the URL containing his name and to the official campaign content that was provided.”67 Twitter reclaimed singer Kanye West’s handle after he publically complained that he was being impersonated and questioned the authenticity of other celebrity Twitter accounts.68 Sarah Palin’s fake Facebook profile was removed after her attorney contacted Facebook.69

Brands often have to be careful when attempting to reclaim their usernames in instances in which a fan, called an “influencer,”70 created the social media page. A brand does not want to offend its biggest fans. Coca-Cola faced this situation when two influencers created a Coke Facebook fan page that became the second most popular page on Facebook by November 2008.71 Coke could have taken back the page using the Facebook rule mandating that only those authorized by a brand can create a page for that brand.72 Instead, it partnered with the influencers, flew them to its headquarters, and discussed strategies for jointly leveraging the page.73

Others have not succeeded in reclaiming their usernames. Senator John McCain attempted to recover his LinkedIn vanity URL during the 2008 presidential race.74 LinkedIn refused because the URL was

---

66. Rosmarin, supra note 44.
67. Id. (quoting MySpace executive Jeff Berman).
68. See generally Angwin, supra note 54.
69. Rosman, supra note 2 (quoting Palin’s spokeswoman as saying Facebook’s legal counsel “worked quickly to resolve the situation and was very responsive”).
70. An influencer is a brand’s customer who takes it upon himself to promote the brand, usually via word-of-mouth on a social site. See CHARLENE LI & JOSH BERNOFF, GROUNDSWELL: WINNING in a WORLD TRANSFORMED by SOCIAL TECHNOLOGIES 94 (2008).
72. Create a Page, FACEBOOK, http://www.facebook.com/pages/create.php (last visited Jan. 25, 2011) (stating that by clicking “Create Official Page,” the user agrees that he is “the official representative of this person, business, band or product and [has] permission to create this Page”).
73. Klaassen, supra note 71. CNN faced a similar situation when a fan created twitter.com/CNNbrk as a CNN breaking news feed and the site gained a massive following. Angwin, supra note 54. CNN was reluctant to take aggressive measures against a fan evangelizing its brand. Id. CNN arranged for the fan to train its staff on how to use Twitter in return for the fan transferring ownership of the account. Id. Twitter.com/CNNbrk has over three million followers as of June 2010. See CNN BREAKING NEWS ON TWITTER, twitter.com/CNNbrk (last visited Jan. 25, 2011).
74. Angwin, supra note 54.
validly taken by another individual named John McCain. Actor Gary Busey stopped trying to reclaim fake Gary Busey MySpace pages, including www.myspace.com/garybusey, which "portrays Mr. Busey as a hash-smoking cougar killer." Busey claimed he did not have the resources to fight the fake profiles that kept appearing.

Some disputes have resulted in legal action. In the Tanner Friedman corporate sabotage situation, Tanner filed suit to compel Twitter to provide the IP address of the user who registered the handle. Tanner did not sue Twitter, but it did sue the John Doe who created the account on the grounds of cyberpiracy, defamation, intentional interference with contractual and business relations, trademark infringement, and unfair competition.

In other cases, victims have opted to sue the social networking site because the site has more resources to pay damages than the individual who jacked the username. The victim may also sue the social network rather than the individual perpetrator because it is often difficult to identify the perpetrator; for example, the account may have been registered from an IP address that was masked or associated with many users, such as the address of a university, library, or corporation. Tony La Russa opted to sue Twitter in California state court after trying to contact Twitter for a week to have his fake profile deleted. La Russa sued Twitter for trademark infringement, false designation of origin, trademark dilution, cybersquatting, misappropriation of name, misappropriation of likeness, invasion of privacy, and intentional misrepresentation. Twitter deleted the profile within 75.

\[\text{Id. (citing LinkedIn spokeswoman Kay Luo).}\]

\[\text{Id.}\]

\[\text{Id.}\]


80. Even Tanner Friedman did not know exactly who hijacked its account, just that the person used a Marx Layne computer. Moshinia, supra note 63. The person used an anonymous e-mail address. Id.


82. Phillip Matier & Andrew Ross, Air Board Shells Out $75K for Times Columnist’s Speech, S.F. CHRON., May 10, 2009, at B1 (quoting La Russa’s attorney, “We tried to reach (Twitter) for a week, and got no response”).

83. Complaint, La Russa, at 1–7 (La Russa’s trademark infringement claim was brought under 15 U.S.C. § 1114, his false designation of origin claim and his trademark dilution claim were
half an hour of receiving the complaint. La Russa dismissed the claim after Twitter removed the case to federal court, and no payment was made by Twitter. Twitter co-founder Biz Stone blogged that La Russa’s suit “was an unnecessary waste of judicial resources bordering on frivolous.”

D. Potential Causes of Action for Username Jacking

There are various claims that a username-jacking victim can bring against a social networking site. Section 230 of the Communications Decency Act immunizes social sites from many torts committed by their third-party users, but it does not protect the sites from intellectual property claims. This Section sets out potential intellectual property claims, including cybersquatting and trademark claims. It then discusses the split of authority as to whether § 230 bars a right of publicity claim.

1. Claims Barred by § 230 of the CDA

Section 230 of the CDA states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” Thus, an interactive computer service will not be deemed a publisher or speaker of any content that third-party users post through the service. Congress defined “interactive computer service” brought under 15 U.S.C. § 1125, his cybersquatting claim was brought under the Anticybersquatting Consumer Protection Act, and his invasion of privacy claim was brought under § 3344(a) of the California Civil Code).

84. Matier & Ross, supra note 82.
89. See infra notes 110–20 and accompanying text.
90. See infra notes 121–53 and accompanying text.
91. See infra notes 173–88 and accompanying text.
92. § 230(c)(1). The Digital Millennium Copyright Act (DMCA) provides similar immunity from copyright infringement claims. See 17 U.S.C. § 512(c) (2006).
as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet." Courts have interpreted this language broadly. In the pre-Web 2.0 era, § 230 immunity was generally extended to Internet Service Providers (ISPs) and Web-hosting services. As the Web became more interactive, courts held that any site with third-party interaction was an interactive computer service. Social networking sites, which thrive on third-party interaction, fall squarely within the common law interpretation of "interactive computer service." Thus, § 230 will protect social networking sites.

Congress passed the CDA with the goal of protecting interactive computer services from liability for defamatory content created by third-party users. Congress expressly sought to promote the growth

---

94. Web 2.0 refers to the rise of Web technologies that users can interact with, like social sites. See Li & Bernoff, supra note 70, at 10–11 (citing Internet observer Tim O'Reilly).
96. See Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 671 (7th Cir. 2008) (holding Craigslist immune under § 230 for defamatory user-generated content); Fair Hous. Council of San Fernando Valley v. Roommates.com, L.L.C., 521 F.3d 1157, 1162 (9th Cir. 2008) (noting that the plaintiff did not dispute that Roommates.com, a roommate matching site on which users create profiles, was an interactive computer service); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123–24 (9th Cir. 2003) (commenting that "reviewing courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of "interactive computer service" while upholding immunity for a matchmaking Web site on which users created profiles); Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 846 (W.D. Tex. 2007) (noting that the plaintiff did not contest that MySpace was an interactive computer service provider under the CDA); DiMeo v. Max, 433 F. Supp. 2d 523, 529 (E.D. Pa. 2006) (holding that an online message board that allowed users to post anonymous comments was an interactive computer service); Parker v. Google, Inc., 422 F. Supp. 2d 492, 501 (E.D. Pa. 2006) (holding "there is no doubt" Google is an interactive computer service because "Google either archived, cached, or simply provided access to content that was created by a third party"); Faegre & Benson, L.L.P. v. Purdy, 367 F. Supp. 2d 1238, 1249 (D. Minn. 2005) (holding that a site on which users could post comments was an interactive computer service); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1119 (W.D. Wash. 2004) (noting that the plaintiff did not contest that Amazon, which houses shops run by third-party vendors, qualified as an interactive computer service); Schneider v. Amazon.com, Inc., 31 P.3d 37, 40–41 (Wash. Ct. App. 2001); Doe v. Bates, No. 505-CV-91-DJ-CMC, 2006 WL 3813758, at *2 (E.D. Tex. Dec. 27, 2006) (finding that Yahoo! was an interactive computer service); see also Ken S. Myers, Wikimmunity: Fitting the Communications Decency Act to Wikipedia, 20 Harv. J.L. & Tech. 163, 179–81 (2006) (arguing that Wikipedia is an interactive computer service).
97. Batzel v. Smith, 333 F.3d 1018, 1029 (9th Cir. 2003) (noting that Congress passed the CDA to overrule Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063-94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), which held that the owner of an online bulletin board could be liable for
of the Internet "unfettered by State or Federal regulation."98 Requiring Web sites to continually police massive volumes of potentially defamatory user-generated content would severely limit the Web's potential to continually develop for society's benefit.99 Such defamation lawsuits would prevent Web companies from innovating. Courts have since extended CDA immunity well beyond defamation to claims like fraud, negligence, intentional infliction of emotional distress, negligent misrepresentation, and invasion of privacy.100

The CDA carves out four exceptions to immunity for Web site operators.101 One exception, subsection (e)(2), states that "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property."102 Courts have used this language to hold that Web site operators do not enjoy § 230 immunity for trademark claims, which encompass cybersquatting.103 At least two courts have used

defamatory content posted by its third-party users); Zeran, 129 F.3d at 328-29, 331 (stating that Congress enacted § 230 in response to Stratton and holding that the CDA barred a claim against AOL for third-party defamatory material posted through AOL's services, particularly false notices that Mr. Zeran had Oklahoma City bombing paraphernalia for sale).

98. 47 U.S.C. § 230(b)(1)-(2) ("It is the policy of the United States—(1) to promote the continued development of the Internet and . . . (2) to preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation . . .").

99. § 230(a)(3) ("The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."); Zeran, 129 F.3d at 330 ("Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium.").


101. The four claims that do not enjoy immunity are claims that impair enforcement of (1) any federal criminal statute, (2) "any law pertaining to intellectual property," (3) "any state law that is consistent with this section," and (4) the Electronic Communications Privacy Act of 1986. 47 U.S.C. § 230(e)(1)-(4). However, § 230(e)(3) states that "[n]o liability may be imposed under any State or local law that is inconsistent with this section."

102. § 230(e)(2).

103. Universal, 478 F.3d at 422–23 (stating that plaintiff's trademark dilution claim was brought under Florida trademark law and "[c]laims based on intellectual property laws are not subject to Section 230 immunity"); Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 413
subsection (e)(2) to hold that the CDA does not bar claims under state intellectual property laws.\textsuperscript{104}

Section 230 immunity also does not apply to any Web site that participates in the creation or development of the content at issue. Participation in content development would make the site an “information content provider.”\textsuperscript{105} Section 230 defines “information content provider” as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet.”\textsuperscript{106} Courts have held that facilitating the posting of user-generated material by providing fields for users to enter content does not make a Web site an information content provider.\textsuperscript{107} Nor does deleting portions of user-generated content.\textsuperscript{108} Whether a social networking site retains § 230 immunity will depend on the role it played in creating or developing the user-generated content at issue.\textsuperscript{109}

---


\textsuperscript{105} Right of publicity grants a person the right to control the commercial value of his name. See, \textit{e.g.}, Rogers v. Grimaldi, 875 F.2d 994, 1003–04 (2d Cir. 1989).


\textsuperscript{107} \textit{Universal}, 478 F.3d at 419 (holding that Lycos did not lose § 230 immunity for facilitating third-party postings to a message board); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003) (granting § 230 immunity to a Web site on which “the selection of the content was left exclusively to the user” even though the site provided a questionnaire for the user to fill out); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1118 (W.D. Wash. 2004) (“Although Amazon may have encouraged third parties to use [its] platform and provided tools to assist them, that does not disqualify it from immunity under § 230 because the [third-party] vendor ultimately decided what information to put on its site.”); Schneider v. Amazon.com, Inc., 31 P.3d 37, 38–39, 43 (Wash. Ct. App. 2001) (finding that Amazon retained immunity despite providing fields for users to enter and post book reviews).

\textsuperscript{108} Ben Ezra, Weinstein & Co. v. AOL, Inc., 206 F.3d 980, 985–86 (10th Cir. 2000) (holding that a site’s deletion of some user-generated content to correct errors did not constitute development or creation of the information at issue); Donato v. Moldow, 865 A.2d 711, 719–20 (N.J. Super. Ct. App. Div. 2005) (upholding § 230 immunity for an online bulletin board operator that controlled the “content of the discussion” by posting messages of his own, commenting on messages posted by other users, deleting messages posted by other users, and banning users who were disruptive).

\textsuperscript{109} See infra notes 195–99 and accompanying text.
2. Cybersquatting Claims

La Russa brought a cybersquatting claim in his complaint against Twitter. La Russa claimed Twitter was in "direct violation" of the Anticybersquatting Consumer Protection Act (ACPA). The ACPA was enacted in 1999 to prevent cybersquatting, which is the "bad faith, abusive registration and use of the distinctive trademarks of others as Internet domain names, with the intent to profit from the goodwill associated with those trademarks." The Act also protects "a personal name which is protected as a mark." Congress also provided protection against the cybersquatting of non-trademarked personal names in the Intellectual Property and Communications Omnibus Reform Act of 1999, which outlawed the "act of registering someone else's name as a domain name for the purpose of demanding remuneration from the person in exchange for the domain name." The ACPA provides for the creation of a domain name dispute resolution procedure; the Uniform Domain Name Dispute Resolution Policy (UDRP), created by the Internet Corporation for Assigned Names and Numbers (ICANN), is an example of such a procedure.

J. Thomas McCarthy, author of the foremost treatise on trademark and unfair competition law, summarizes the four elements of cybersquatting liability as

1. The defendant has registered, trafficked in or used a domain name;
2. Which is identical to or confusingly similar to a mark owned by the plaintiff;
3. The defendant has done so with bad faith intent to profit from the goodwill associated with the plaintiff's mark;
4. The defendant's registration and use of the domain name is likely to cause confusion among consumers.

---


"Defendant's actions . . . including its registration and use of the domain name twitter.com/TonyLaRussa in an intentional attempt to divert the public away from Plaintiff's authorized websites to Defendant's website, constitute a bad faith intent to profit from and injure Plaintiff's mark, is intended to increase traffic to Defendant's site, or were done with knowledge that injury to Plaintiff's mark was substantially certain to occur.

111. Id. at 5; see also 15 U.S.C. § 1125(d) (2006).

112. Shields v. Zuccarini, 254 F.3d 476, 481 (3d Cir. 2001); see also Ford Motor Co. v. Catalano, 342 F.3d 543, 549 (6th Cir. 2003) ("Registering a famous trademark as a domain name and then offering it for sale to the trademark owner is exactly the wrong Congress intended to remedy when it passed the ACPA.").


114. S. J. THOMAS McCARTHY, McCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:80 (4th ed. 2010) (quoting 145 CONG. REC. S14,715 (daily ed. Nov. 17, 1999), which also notes that this section is not "intended to create a right of publicity of any kind with respect to domain names").

3. The mark was distinctive at the time of the defendant’s registration of the domain name; [and]
4. The defendant has committed the acts with a bad faith intent to profit from the plaintiff’s mark.\textsuperscript{116}

The interpretation of the first element is critical in username-jacking lawsuits. For a jacking victim to succeed in his claim, a social network username must be a “domain name.”\textsuperscript{117} Element four—bad faith intent to profit—may also raise questions in username-jacking suits.\textsuperscript{118}

The Lanham Act provides nine factors for courts to consider in assessing bad faith:

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;
(II) the extent to which the domain name consists of the legal name of the person . . .
(III) the person’s prior use . . . of the domain name in connection with the . . . offering of any goods or services;
(IV) the person’s bona fide noncommercial or fair use of the mark

(V) the person’s intent to divert consumers from the mark owner’s online location . . .
(VI) the person’s offer to transfer, sell, or otherwise assign the domain name to the mark owner . . .
(VII) the person’s provision of material and misleading false contact information when applying for the registration of the domain name . . .
(VIII) the person’s registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others . . .
(IX) the extent to which the mark incorporated in the person’s domain name registration is or is not distinctive and famous\textsuperscript{119}

Part III.B discusses how these factors apply to username-jacking suits.\textsuperscript{120}

3. Trademark Violation Claims

Trademark violation is another potential cause of action that may be brought in username-jacking suits. A jacking victim can bring a variety of trademark claims, including trademark infringement,\textsuperscript{121} di-

\textsuperscript{116} McCarthy, \textit{supra} note 114, § 25:78 (emphasis added).
\textsuperscript{117} See \textit{infra} notes 203–11 and accompanying text.
\textsuperscript{118} See \textit{supra} note 114 and accompanying text.
\textsuperscript{120} See \textit{infra} notes 212–43 and accompanying text.
\textsuperscript{121} Trademark infringement is a violation of a trademark holder’s rights in the mark. See 15 U.S.C. § 1114.
Two issues are particularly pertinent to username-jacking suits: (1) whether the social network used the mark in a manner likely to confuse consumers and (2) whether the network used the mark "in connection with the sale, offering for sale, distribution, or advertising of any goods or services." This Section also discusses the issue of contributory (secondary) liability for social networking sites in username-jacking situations.

a. Likelihood of Confusion Requirement

The core element of any trademark claim is whether the unauthorized use of the mark is likely to cause confusion or suggest false affiliation or sponsorship. Likelihood of confusion is a requisite of all trademark claims, except dilution. To determine the likelihood of confusion, some federal courts have looked to several factors including (1) the strength of the plaintiff's mark, (2) the similarity of the marks at issue, (3) whether consumers were actually confused, (4) the extent of potential confusion, (5) whether the defendant harbored bad faith, and (6) the degree to which the products compete. To determine the likelihood of confusion of a post-domain path like a username, courts will consider whether consumers were initially confused into visiting the fake page and whether the social network harbored bad faith. Courts will also consider whether the page was a parody or gripe, which would not be likely to cause confusion.

To determine the likelihood of confusion in domain name cases, some courts have applied the concept of "initial interest confusion."
Initial interest confusion is "customer confusion that creates initial interest in [a] competitor’s product; although dispelled before actual sale occurs, initial interest confusion impermissibly capitalizes on goodwill associated with [the] owner’s mark." Some courts have found initial interest confusion sufficient to spur trademark infringement even when the defendant’s site contained a disclaimer that it was not associated with the plaintiff’s trademark.

The initial interest confusion doctrine could be applied to username-jacking situations. For instance, a user could search for a celebrity on Google and initially think, based on the search result, that a jacked social media page is the celebrity’s real page. Although the user may quickly realize the page is a fake once he visits the page, he was still initially confused into clicking on the search result. A user could be lured into clicking on a search listing based on the content of that listing. The search listing contains the page’s title, for example (Sarah Palin — Facebook), the page’s URL, for example (facebook.com/sarahpalin), and a short description of the page, which is called the “search snippet.” Search engines pull the search snippet from the page’s description meta tag. A description meta tag is a piece of Web page code that can be used to provide search engines with a description of a page. For instance, the description meta tag

![Image](https://example.com/image.png)

initial interest confusion in the sense that, by . . . diver[ing] people looking for [plaintiff’s mark] to its web site, [defendant] improperly benefits from the goodwill that [plaintiff] developed in its mark.”


133. PACCAR Inc. v. TeleScan Techs., L.L.C., 319 F.3d 243, 253 (6th Cir. 2003) (“A disclaimer disavowing affiliation with the trademark owner read by a consumer after reaching the [infringing] web site comes too late. This ‘initial interest confusion’ is recognized as an infringement under the Lanham Act.”); OBH, Inc. v. Spotlight Magazine, Inc., 86 F. Supp. 2d 176, 190 (W.D.N.Y. 2000) (finding initial interest confusion despite a disclaimer because when users seek the plaintiff’s site and arrive “instead at defendants’ web site, they cannot help being confused—even if only momentarily”); N.Y. State Soc’y of Certified Pub. Accountants v. Eric Louis Assocs., Inc., 79 F. Supp. 2d 331, 342 (S.D.N.Y. 1999) (finding initial interest confusion because “[p]ersons using [the infringing domain] are expecting to arrive at the [plaintiff’s] Web site” even though defendant provided a disclaimer); Planned Parenthood Fed’n of Am., Inc. v. Bucci, No. 97 Civ. 0629 (KMW), 1997 U.S. Dist. LEXIS 3338, at *39 (S.D.N.Y. Mar. 19, 1997) (holding that defendant’s unauthorized registration of plannedparenthood.com caused “confusion among Internet users and may cause Internet users who seek plaintiff’s web site to expend time and energy accessing defendant’s web site” even though defendant provided a disclaimer).

134. See supra note 39.


136. Id. Another kind of meta tag that has been a source of litigation is the keyword meta tag, which contains keywords describing the site. See Promatek Indus., Ltd. v. Equitrac Corp., 300 F.3d 808, 813 (7th Cir. 2002) (finding that the defendant’s use of the plaintiff’s trademark in the meta tags of the defendant’s site could violate trademark law). Keyword meta tags are irrelevant to username-jacking suits because the tags are no longer used by major search engines to
of Sarah Palin's Facebook page contains the text: "Welcome to the official Facebook Page of Sarah Palin. Get exclusive content and interact with Sarah Palin right from Facebook." Google uses this exact text for the search snippet. Therefore, a Web site could use an infringing mark in a description meta tag, Google could display that mark in the page's search snippet, and this—along with the page title and URL—could initially confuse a searcher into clicking on the listing.

Other courts have rejected the initial interest confusion doctrine, holding that it is easy for a user to leave a false site to find the real site. In Lamparello v. Falwell, the United States Court of Appeals for the Fourth Circuit found that initial interest confusion was not sufficient to prove trademark infringement unless the unauthorized site sought to profit from the confusion. The defendant in Lamparello registered fallwell.com (a common misspelling of Reverend Jerry Falwell's name) to criticize Falwell's stance on homosexuality. The court held that despite the initial interest confusion the site created, the registrant was not using the confusion for financial gain—he was only parodying Falwell.

137. See Sarah Palin Facebook, supra note 38 (view page code by clicking on "view" and then "source" in the browser, then search for "description" to find the description meta tag).
138. See sources cited supra note 39.
139. See N. Am. Med. Corp. v. Axiom Worldwide, Inc., 522 F.3d 1211, 1221 n.8 (11th Cir. 2008) (finding likelihood of confusion because "[plaintiff's] trademarks appeared in the Google search result as part of the description of [defendant's] website. . . . [T]he meta tags caused the search result and thus the likelihood of confusion").
140. Hasbro, Inc. v. Clue Computing, Inc., 232 F.3d 1, 2 (1st Cir. 2000) (stating that the likelihood of initial interest confusion in this case was not "legally significant"); Strick Corp. v. Strickland, 162 F. Supp. 2d 372, 377 (E.D. Pa. 2001) ("‘Internet surfers are inured to the false starts and excursions awaiting them' and are 'unlikely to be dissuaded, or unnerved' when, after 'taking a stab at what they think is the most likely domain name for a particular web site' guess wrong and bring up another's webpage.") (quoting Chatam Int'l, Inc. v. Bodum, Inc., 157 F. Supp. 2d 549, 559 n.17 (E.D. Pa. 2001) (alteration in original)); Teletech Customer Care Mgmt., Inc. v. Tele-Tech Co., 977 F. Supp. 1407, 1414 (C.D. Cal. 1997) (finding “brief confusion” that results in merely clicking on the wrong Web site "not cognizable under the trademark laws").
142. Id. at 315.
143. Id. at 315-17.
Courts have also dealt with the likelihood of confusion of post-domain paths, which are analogous to social network usernames. A post-domain path is the text after the .com in a URL, like “Tony-LaRussa” in twitter.com/TonyLaRussa. The United States Court of Appeals for the Sixth Circuit stated in Interactive Products Corp. v. A2Z Mobile Office Solutions, Inc. that “[b]ecause post-domain paths do not typically signify source, it is unlikely that the presence of another’s trademark in a post-domain path of a URL would ever violate trademark law.” Interactive Products could pose a hurdle to a username-jacking victim’s ability to prove likelihood of confusion. But the victim could argue that social media profiles—because of the mass adoption of social networking—do actually “signify source” of a celebrity or brand. Thus, likelihood of confusion in username cases will hinge on (1) whether the court subscribes to the initial interest confusion doctrine, (2) whether the profile is a parody/gripe, and (3) whether the court follows Interactive Products’ holding that post-domain paths are not likely to cause confusion.

b. Commercial Use Requirement

In addition to the likelihood of confusion, a username-jacking victim will also have to prove that the infringing trademark was used commercially. A trademark infringement claim is not actionable unless the unauthorized use of the mark is commercial. To succeed on a trademark infringement claim, a username-jacking victim must show

---


145. Interactive Prods. Corp. v. A2Z Mobile Office Solutions, Inc., 326 F.3d 687, 692, 698 (6th Cir. 2003) (holding that there was no likelihood of confusion from defendant’s use of the trademark “laptraveller” in the post-domain path of the URL a2zsolutions.com/desks/floor/lap-traveller/dkfl-it.htm). The court was also not swayed that the URL would show up in search engine results for the keyword “laptraveler.” Id. at 698. The court concluded this based on expert testimony that “the path name does not bias a search engine.” Id. at 698 n.6. While this expert may have been correct in 2003, it is now widely agreed that keywords within a URL do influence search rankings. Barry Schwartz, Google’s Matt Cutts on Keywords in the URL, SEARCH ENGINE LAND (Mar. 18, 2009, 9:34 AM), http://searchengineland.com/googles-matt-cutts-on-keywords-in-the-url-16976 (quoting Google’s Matt Cutts as saying it makes sense for Web sites to have keywords in their URLs to positively impact their site’s search engine rankings for those keywords). See also Patmont Motor Werks, Inc. v. Gateway Marine, Inc., No. C 96-2703 TEH, 1997 U.S. Dist. LEXIS 20877, at *13 n.6 (N.D. Cal. Dec. 17, 1997) (“The Court is aware that the [trademark] ‘goped’ appears at the secondary level in the [defendant’s] website’s URL: ‘www.idiosync.com/goped.’ However . . . such use does not suggest [the trademark owner’s] sponsorship or endorsement, because the Go-Ped mark did not appear in the website’s ‘domain name.’”).

146. See infra notes 254–56 and accompanying text.

147. MCCARTHY, supra note 114, § 25:76.
that the social site used his mark “in connection with the sale, offering for sale, distribution, or advertising of any goods or services.”

The Federal Trademark Dilution Act (FTDA) explicitly states that comparative commercial advertising, news reporting, and commentary are noncommercial uses that are not actionable under the statute. Courts have also held that the use of a trademark for parody or criticism is noncommercial, even if the defendant makes money from the use.

c. Contributory (Secondary) Trademark Infringement

Username-jacking victims may also bring claims for contributory trademark infringement. For a social networking site to be contributorily liable for a third-party user’s infringement, the jacking victim must show that the site either (1) intentionally induced the user to infringe on a trademark or (2) continued to supply services to “one whom it [knew] or ha[d] reason to know [was] engaging in trademark infringement.” The social networking site must have more than “general knowledge” that its users might infringe on others’ trademarks; the site must have “contemporary knowledge” of which specific profiles are infringing.

---


149. § 1125(c)(3)(A) (identifying “parodying, criticizing, or commenting upon the famous mark” as not actionable as dilution); 141 Cong. Rec. S19,310 (daily ed. Dec. 25, 1995) (statement of Sen. Hatch) (“The [Trademark Dilution Bill] will not prohibit or threaten noncommercial expression, such as parody, satire, editorial and other forms of expression that are not a part of a commercial transaction.”).


151. Charles Atlas, Ltd. v. DC Comics, Inc., 112 F. Supp. 2d 330, 332, 338–39 (S.D.N.Y. 2000) (finding that DC Comic’s creation of a comic book story that parodied body building company Atlas’ ad was noncommercial free expression despite the fact that DC sold the comics); Mattel, Inc. v. MCA Records, Inc., 28 F. Supp. 2d 1120, 1142 (C.D. Cal. 1998) (commenting that Mattel was unlikely to succeed on a dilution claim regarding MCA’s Barbie Girl song because the song was a parody of “the ‘party-girl’ image that Barbie has acquired”).

152. Tiffany, Inc. v. eBay, Inc., 600 F.3d 93, 106 (2d Cir. 2010) (quoting Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 854 (1982)).

153. Id. at 107.
4. Right of Publicity Claims

Another potential cause of action is a right of publicity claim. This Section first describes the right of publicity. It then discusses a split of authority as to whether § 230 immunizes Web site operators from publicity claims.

a. Right of Publicity Background

Tony La Russa, who happens to hold a law degree,\textsuperscript{154} said, "There is a law against improperly using a person's name without authorization.\textsuperscript{155} That law in California, under which La Russa brought his claim, is California Civil Code § 3344(a). Section 3344(a), California's right of publicity statute, provides that "[a]ny person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent . . . shall be liable for any damages."\textsuperscript{156} To succeed on a right of publicity claim, a plaintiff must show that (1) he "owns an enforceable right in the identity," (2) the "defendant, without permission, has used some aspect of the identity or persona in such a way that plaintiff is identifiable," and (3) the "[d]efendant's use is likely to cause damage to the commercial value of that persona.\textsuperscript{157}

Right of publicity is a state right recognized by roughly half the states either in common law\textsuperscript{158} or by statute; at least fifteen states have partially or completely codified the right.\textsuperscript{159} In practice, the right applies primarily to celebrities.\textsuperscript{160} Unlike a noncelebrity, a celebrity's

\begin{footnotes}
\item[154.] Golen, \textit{supra} note 53 (quoting La Russa as saying that the public perception was that he was upset by the criticism, but that he was really only upset with the improper use of his name).
\item[155.] \textit{Id}.
\item[156.] \textit{CAL. CIVIL CODE} § 3344(a) (West 2000); La Russa framed this claim as an invasion of privacy claim, which alleges infringement of the right of publicity, but goes even further by claiming emotional and reputational damage. Complaint, La Russa v. Twitter, Inc., No. CGC-09-488101, at 6 (Cal. Super. Ct. June 5, 2009). See also 1 J. Thomas McCarthy, \textit{The Rights of Publicity and Privacy} § 3:2 (2d ed. 2009) for a discussion of the right of publicity.
\item[157.] See, e.g., McCarthy, \textit{supra} note 156, § 3:2.
\item[158.] Rogers v. Grimaldi, 875 F.2d 994, 1004 (2d Cir. 1989) ("The common law right of publicity, where it has been recognized, grants celebrities an exclusive right to control the commercial value of their names . . . .")
\item[159.] Edward H. Rabin et al., \textit{Fundamentals of Modern Property Law} 1287 (5th ed. 2006) (citing nineteen state right of publicity statutes).
\end{footnotes}
name has "associative value," which is "the perceived ability to confer value on that which might be associated with the celebrity." Courts and the Restatement of Unfair Competition view the right of publicity as a property right. In addition, courts have held that the right of publicity is an intellectual property right.

Unlike trademark infringement law, the right of publicity requires no proof of the likelihood of consumer confusion or false belief of association or sponsorship. However, the First Amendment can trump publicity rights, when, for example, the celebrity's persona is used in a parody. In terms of commercial use, the plaintiff must prove that the defendant intended to obtain a commercial advantage through use of his identity; actually obtaining a commercial advantage is irrelevant. Confusion as to whether the celebrity actually endorses the defendant's product is not required; all that a plaintiff needs to prove is that his name has impermissibly been associated with the product.

The Third Restatement of Unfair Competition states that the measure of damages for a right of publicity violation "focuses on the pecuniary loss to the plaintiff or the unjust pecuniary gain to the defendant." Courts have used this standard to award publicity plaintiffs the amount they should have been paid for the use of their persona and the amount of damage done to the persona's endorse-

---


162. See Cardtoons, L.C. v. Major League Baseball Players Ass'n, 95 F.3d 959, 968 (10th Cir. 1996) (stating that publicity rights "are a form of property protection"); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 cmt. g (1995) ("The interest in the commercial value of a person's identity is in the nature of a property right."); McCarthy, supra note 156, § 10:7 n.1 (listing cases that have held right of publicity as a property right in California, Florida, Georgia, Michigan, Minnesota, Missouri, Nevada, New Jersey, New York, Oklahoma, Pennsylvania, Tennessee, Texas, Virginia, and Wisconsin).

163. Perfect 10, Inc. v. CCBill, L.L.C., 488 F.3d 1102, 1107 (9th Cir. 2007); Acme Circus Operating Co. v. Kuperstock, 711 F.2d 1538, 1541 (11th Cir. 1983); Atl. Recording Corp. v. Project Playlist, Inc., 603 F. Supp. 2d 690, 704 (S.D.N.Y. 2009); Friendfinder Network, Inc., 540 F. Supp. 2d at 302.

164. McCarthy, supra note 156, § 3:10.

165. See, e.g., Cardtoons, 95 F.3d at 962 (holding that there is a parody exception in Oklahoma's right of publicity statute and that the defendant's "First Amendment right to free expression outweighs [the plaintiff's] proprietary right of publicity").

166. Doe v. TCI Cablevision, 110 S.W.3d 363, 370–71 (Mo. 2003) ("[T]he commercial advantage element of the right of publicity focuses on the defendant's intent or purpose to obtain a commercial benefit . . . . [I]n meeting [this] element, it is irrelevant whether defendant intended to injure the plaintiff . . . or actually succeeded in obtaining a commercial advantage . . . . ").

167. Halpern, supra note 160, at 1035 (citing Cardtoons, 95 F.3d at 967).

At least one state has barred celebrity publicity plaintiffs from recovering damages for emotional or reputational harm, while other states—particularly California—have allowed these awards. In most states, punitive damages are awarded in publicity cases only when there is "proof of defendant's knowing use of plaintiff's identity."  

b. The Right of Publicity and § 230  

Whether § 230 bars a right of publicity claim depends on one's interpretation of subsection (e)(2). Subsection 230(e)(2) states that "[n]othing in this section shall be construed to limit . . . any law pertaining to intellectual property." Federal courts are split as to whether the "any law" language in § 230 bars only federal intellectual property claims or both federal and state intellectual property claims, which would include the state law right of publicity.  

In Perfect 10 v. CCBill, the United States Court of Appeals for the Ninth Circuit recognized that subsection (e)(2) limits § 230 immunity, but noted that "the CDA does not contain an express definition of 'intellectual property.'" The court stated that federal intellectual property laws were well established, but state intellectual property laws—like publicity rights—were not uniform. These laws "bear various names, provide for varying causes of action and remedies, and have varying purposes and policy goals." Because Web site content is viewed across state lines, "permitting the reach of any particular state's definition of intellectual property to dictate the contours of § 230 immunity would be contrary to Congress's expressed goal of insulating the development of the Internet from the various state-law regimes." Thus, the Ninth Circuit held that "intellectual property" in subsection (e)(2) means "federal intellectual property." This in-

170. TCI Cablevision, 110 S.W.3d at 368 (noting that the right of publicity is not meant to protect a person's feelings).  
171. Waits v. Frito-Lay, Inc., 978 F.2d 1093, 1103 (9th Cir. 1992) (stating that California law allows celebrity right of publicity plaintiffs to recover for "humiliation, embarrassment, and mental distress" (quoting Motschenbacher v. R. J. Reynolds Tobacco Co., 498 F.2d 821, 824 & n.11 (9th Cir. 1974))).  
172. McCARTHY, supra note 156, § 11:36.  
174. Perfect 10, Inc. v. CCBill, L.L.C., 488 F.3d 1102, 1108, 1118 (9th Cir. 2007) (involving the publicity rights of perfect10.com models who had assigned those rights to Perfect 10).  
175. Id. at 1118.  
176. Id.  
177. Id.  
178. Id. at 1119.
terpretation immunizes Web site operators from state law right of publicity claims and spells doom for Ninth Circuit plaintiffs like La Russa.179 The court also held that any state law inconsistent with § 230, including right of publicity laws, cannot interfere with § 230 immunity."180

The United States District Court for the District of New Hampshire, when faced with the same issue in Doe v. Friendfinder Network., took the opposite stance. The court held that subsection (e)(2) allows federal and state intellectual property claims, thus allowing a right of publicity claim against Web site operator AdultFriendFinder.com.181 The court relied on Universal Communications Systems v. Lycos, which stated in dicta that Florida’s trademark dilution statute (a state law) was an intellectual property claim under subsection (e)(2) and thus was not barred by § 230.182

The Friendfinder court criticized the Ninth Circuit’s reading of subsection (e)(2), stating that subsection (e)(2) “does not suggest a limitation to federal intellectual property law.”183 The court cited the U.S. Supreme Court for the rule of law that “the modifier ‘any’ amounts to ‘expansive language [that] offers no indication whatever that Congress intended [a] limiting construction.’”184 Friendfinder noted that the Ninth Circuit ignored the fact that Congress mentions “federal” and “state” in other parts of § 230.185 Thus, where “Congress wished to distinguish between state and federal law in § 230, it knew how to do so.”186 The court also dismissed the Ninth Circuit’s fear that allowing state intellectual property claims to trump the CDA would “be contrary to Congress’s expressed goal of insulating the development of

179. Id.
180. Id. at 1118.
182. Id. at 298 (citing Universal Commc’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 422–23 (1st Cir. 2007)).
183. Id. at 299.
184. Id. (alteration in original) (quoting Harrison v. PPG Indus., 446 U.S. 578, 589 (1980)).
185. Id. at 300.
186. Id. (citing 47 U.S.C. § 230(e)(1) (2006) which states, “Nothing in this section shall be construed to impair the enforcement of [named federal criminal statutes] or any other Federal criminal statute” and § 230 (e)(3): “Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section”). The only other court to address this issue is the United States District Court for the Southern District of New York, which used this same reasoning in Atlantic Recording Corp. v. Project Playlist, Inc. in 2009 to determine that the plaintiffs’ New York state law claims of common law copyright infringement and unfair competition were not blocked by the CDA. 603 F. Supp. 2d 690, 703–04 (S.D.N.Y. 2009).
the Internet from the various state-law regimes.” The court stated that the Internet remains alive and well despite what it called a “general consensus” before Perfect 10 that the CDA did not offer immunity from state intellectual property claims.

Thus, while a username-jacking victim could bring defamation and intentional infliction of emotional distress claims, these claims will likely be barred by § 230. The victim can bring a cybersquatting claim, which will hinge on whether a username is a “domain name” as defined by the ACPA. Trademark violation claims will center on (1) the likelihood that consumers were confused by the fake profile and (2) whether the profile constitutes commercial use. Right of publicity claims will depend on the court’s interpretation of subsection (e)(2).

III. Analysis

Username-jacking victims will likely have difficulty seeking recovery from the social networking sites. This Part discusses why it is unlikely that a username-jacking victim could recover on any of the claims set out in Part II. The first Section claims that social networking sites should be immune from claims traditionally protected by § 230, such as defamation. The second Section argues that cybersquatting claims should not be actionable because usernames are not domain names as defined by the Anticybersquatting Consumer Protection Act (ACPA). This Part then claims that a jacking victim should recover for a trademark violation only when users actually believe the fake profile is the celebrity’s or brand’s real profile. It also contends that social networking sites will not be liable for contributory trademark infringement as long as they remove infringing usernames that they are aware of. Finally, this Part argues that celebrities should not recover for right of publicity claims because recovery is against Congress’s clear goal in passing the Communications Decency Act (the CDA)—to promote innovation on the Internet unfettered by state regulation.

187. Perfect 10, Inc. v. CCBill, L.L.C., 488 F.3d 1102, 1118 (9th Cir. 2007).
188. Friendfinder, 540 F. Supp. 2d at 301-02.
189. See infra notes 194-200 and accompanying text.
190. See infra notes 202-45 and accompanying text.
191. See infra notes 246-86 and accompanying text.
192. See infra notes 287-91 and accompanying text.
193. See infra notes 297-319 and accompanying text.
A. Section 230 Immunity as Applied to Social Networking Sites

Social networking sites qualify for § 230 immunity. These sites were built around third-party site interaction, which makes them “interactive computer services” under § 230.194 Thus, social sites will be immune from many of the torts of their third-party users, including defamation and intentional infliction of emotional distress. The only way a social networking site could lose § 230 immunity is if the site participated in jacking the username.195 When a user signs up for a social networking site, the site provides a field by which the user can choose a username.196 Providing this field will not destroy § 230 immunity. In Carafano v. Metrosplash.com, the Ninth Circuit held that even though metrosplash.com provided third parties with an online form to enter content, “the selection of the content was left exclusively to the user.”197 Deleting portions of user-generated content also will not destroy § 230 immunity.198 Because social networking sites leave username selection “exclusively to the user,” they should retain § 230 immunity.

For a social networking site to lose § 230 immunity, it would likely have to create the fake profile itself, as occurred when Yahoo! created fake dating profiles to induce users to remain members of its online dating service.199 This possibility will likely be a non-issue in most username-jacking cases. Thus, the social sites will likely retain immunity for claims that fall under § 230, like defamation, intentional infliction of emotional distress,200 and, in some jurisdictions, right of publicity.201

194. See supra note 96 and accompanying text.
195. See supra notes 105–06 and accompanying text.
196. See Twitter: Create an Account, supra note 43; Facebook: Create a Page, supra note 72.
197. See also Universal Commc’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007) (finding that Lycos retained immunity despite facilitating third-party message board postings); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1118 (W.D. Wash. 2004) (“Although Amazon may have . . . provided tools to assist [third parties], that does not disqualify it from immunity under § 230 . . . .”); Schneider v. Amazon.com, Inc., 31 P.3d 37, 42–43 (Wash. Ct. App. 2001) (finding that Amazon retained immunity despite providing fields for third parties to enter book reviews).
198. See Ben Ezra, Weinstein & Co. v. AOL, Inc., 206 F.3d 980, 985–86 (10th Cir. 2000) (holding that the site’s deletion of some user-generated content to correct errors did not constitute development or creation of the information at issue); Donato v. Moldow, 865 A.2d 711, 719–20 (N.J. Super. Ct. App. Div. 2005) (upholding § 230 immunity for an online bulletin board operator that controlled the “content of the discussion” by posting messages of his own, commenting on messages posted by other users, deleting messages posted by other users, and banning users who were disruptive).
200. See supra notes 97–100 and accompanying text.
201. See supra notes 173–88 and accompanying text.
B. Likelihood of Recovery: Cybersquatting

A username-jacking victim will also likely not succeed in a cybersquatting claim because (1) the ACPA only protects domain names, not usernames, and (2) the social networks do not act with bad faith intent to profit in username-jacking situations. The ACPA protects against cybersquatting—the bad faith registration of another's trademark as a domain name and the offering for sale of that name to the trademark owner. Usernames, which appear in the post-domain path of a URL, are not domain names under the ACPA; they are post-domain paths within the twitter.com or facebook.com domain name. Courts have stated that post-domain paths are not domain names—albeit before the ACPA’s enactment. The ACPA defines “domain name” narrowly as “any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.” This definition, according to Congress, was meant to exclude “screen names, file names, and other identifiers not assigned by a domain name registrar or registry.” Therefore, the jacking victim will have to show that the social site is a domain name registrar to prove that a social username is a domain name.

The ACPA does not define “domain name registrar.” However, ICANN defines “registrar” as “the entity with which the Respondent has registered a domain name.” Courts have confirmed this definition. ICANN maintains a list of accredited and operational regis-

---

202. To sue the social networking site, a username-jacking victim would have to prove that the social site—not the individual jacker—acted with bad faith intent to profit.


204. Bally Total Fitness Holding Corp. v. Faber, 29 F. Supp. 2d 1161, 1165 (C.D. Cal. 1998) (holding that the defendant “[d]id not use Bally in his domain name” in the URL compupix.com/ballysucks because Bally was only mentioned in the post-URL path); Patmont Motor Werks, Inc. v. Gateway Marine, Inc., No. C 96-2703 TEH, 1997 U.S. Dist. LEXIS 20877, at *13 (N.D. Cal. Dec. 17, 1997) (finding, regarding the URL www.idiosync.com/goped, that the Go-Ped trademark appeared in a post-domain path and “did not appear in the website’s ‘domain name’”).


206. 145 Cong. Rec. S14,715 (daily ed. Nov. 17, 1999) (emphasis added); see also Bally, 29 F. Supp. 2d at 1162 n.1 (stating “[d]omain names are licensed to individuals by Network Solutions, Inc.” (a registrar)).


209. Weber-Stephen Prods. Co. v. Armitage Hardware & Bldg. Supply, Inc., No. 00 C 1738, 2000 U.S. Dist. LEXIS 6335, at *4 n.1 (N.D. Ill. May 3, 2000) (“The term ‘registrar’ refers to the entity (such as Network Solutions, Inc. or America Online) through which a company or individual can register a domain name.”).
trars, which does not include any of the social networking sites.\textsuperscript{210} Thus, social networking sites are not domain name registrars who assign domain names.

Even if a social networking site was considered a domain name registrar, courts have held that registrars do not violate the ACPA because they do not "traffic in" domain names as required by § 1125(d)(1)(A)(ii).\textsuperscript{211} A registrar does not traffic in a domain name because it assigns the domain name to a third party, which then traffics in the name. Therefore, to prove that a social media username is a domain name, the jacking victim will have to make the difficult showing that (1) the social networking site was a domain name registrar that assigned the username as a domain name to a third party, and (2) the social networking site itself continued to traffic in the domain name after assigning it to the third party.

In addition to proving that a username is a domain name, the jacking victim would also have to prove that the social network acted with bad faith intent to profit from the victim's name. Cybersquatting often entails an attempt to sell a domain name to the trademark holder.\textsuperscript{212} The difference between cybersquatting and username jacking is that a user never owns a social network username, he just controls it. Thus, the user does not have the right to sell the name. The social networking site owns the username and can take it back at any time, for any reason.\textsuperscript{213} Social networking sites prohibit the selling or transferring of usernames.\textsuperscript{214} They also have trademark violation complaint processes to ensure that authorized parties control trademarked usernames.\textsuperscript{215} These safeguards make it difficult for a


\textsuperscript{211} See, e.g., Bird v. Parsons, 289 F.3d 865, 881 (6th Cir. 2002) (holding that a domain name registrar, as well as a second site that offered the domain name for auction, did not traffic in the allegedly infringing domain name and were therefore not liable under the ACPA). The ACPA states that "‘traffics in’ refers to transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration." 15 U.S.C. § 1125(d)(1)(E). Domain name registrars are also not liable for monetary relief to a trademark holder as long as they do not refuse to remove or transfer the infringing domain. § 1114(2)(D)(i)(I).

\textsuperscript{212} See, e.g., Ford Motor Co. v. Catalano, 342 F.3d 543, 549 (6th Cir. 2003).

\textsuperscript{213} See supra note 65 and accompanying text.

\textsuperscript{214} Id.

username-jacking victim to make the required showing that the social networking site acted "with bad faith intent to profit from the plaintiff's mark."  

The ACPA provides nine factors for courts to use in evaluating bad faith in cybersquatting cases. An evaluation of these factors demonstrates that a court would not likely find that a social networking site acted in bad faith in a username-jacking situation. The first factor is "the trademark or other intellectual property rights of the person, if any, in the domain name." This factor recognizes "that there may be concurring uses of the same name that are noninfringing, such as the use of the 'Delta' mark for both air travel and sink faucets." A social networking site would not be acting in bad faith if it assigned a username to a user who could be a bona fide owner of that name. The second factor—"the extent to which the domain name consists of the legal name of the person"—accounts for situations where two or more users have the same legal name. A social networking site would not be acting in bad faith if it assigned a username to someone with a legal right to that name—like the non-Senator John McCain on LinkedIn.  

The third factor—"the person's prior use ... of the domain name in connection with the ... offering of any goods or services"—is not applicable to username-jacking situations. The fourth factor is "the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name." Congress meant this fourth factor to "balance the interests of trademark owners with the interests of those who would make lawful noncommercial or fair uses of others' marks online, such as comparative advertising, comment, criticism, parody, news reporting, etc." The majority of username-jacking incidents involve criticism or parody. Courts have rejected ACPA work, to contact MySpace); Copyright Policy, Linkedin, http://www.linkedin.com/static?key=copyright_policy&trk=hb_ft_copy (last visited Jan. 25, 2011).  

217. See supra note 119 and accompanying text.  
222. See supra note 75 and accompanying text.  
226. See supra notes 44-64 and accompanying text.
claims where domain names were used for gripe and parody sites.\footnote{227} Thus, social networking sites are not acting in bad faith when they allow gripe/parody profiles.

The fifth factor takes into account the potential cybersquatter’s “intent to divert consumers from the mark owner's online location.”\footnote{228} ACPA liability has been triggered for domain names registered with intent to divert traffic from competitors, capitalize on brand name recognition, and divert traffic to a parody.\footnote{229} In *People for Ethical Treatment of Animals v. Doughney*, the United States Court of Appeals for the Fourth Circuit held that the defendant’s registration of peta.org as a parody diverted people looking for PETA’s real site because users “who mistakenly access the [parody site] may fail to continue to search for [PETA’s] own home page due to anger, frustration, or the belief that plaintiff’s home page does not exist.”\footnote{230} Fake profiles can rank highly in the search engine results.\footnote{231} But it is wrong to think, as the PETA court did, that Web searchers will just give up searching when they mistakenly access a site. Searchers will simply go back to the search results page and find the real site.\footnote{232} Therefore, fake social

\footnote{227. See Lucas Nursery & Landscaping, Inc. v. Grosse, 359 F.3d 806, 811 (6th Cir. 2004) (rejecting Lucas Nursery’s ACPA claim against the plaintiff, who registered lucasnursery.com and used it solely to gripe about Lucas); TMI, Inc. v. Maxwell, 368 F.3d 433, 438 (5th Cir. 2004) (finding no ACPA violation for registration of defendant’s trademark “TrendMaker Homes” as a domain name used to complain about the plaintiff, despite that the site also contained an area where people could recommend contractors); Mayflower Transit, L.L.C. v. Prince, 314 F. Supp. 2d 362, 369 (D.N.J. 2004) (“Defendant’s ‘cyber-griping’ is a far cry from the ‘squatting’ activity made illegal by the ACPA.”).}


\footnote{229. Coca-Cola Co. v. Purdy, 382 F.3d 774, 784 (8th Cir. 2004) (finding ACPA liability when defendant registered domain names including drinkcoke.org and mymcdonalds.com with intent to capitalize on the famous marks to divert users to anti-abortion content); PETA v. Doughney, 263 F.3d 359, 365 (4th Cir. 2001); Advanced Magazine Publishers, Inc. v. Vogue Int'l, 123 F. Supp. 2d 790, 800 (D.N.J. 2000) (inferring intent to divert based on plaintiff's statement that his registration of vogue-international.com made people think it was “an off-shoot of Vogue magazine”); Morrison & Foerster, L.L.P. v. Wick, 94 F. Supp. 2d 1125, 1133 (D. Colo. 2000) (finding ACPA liability for registering plaintiff's law firm's domain name with the intent to divert people looking for lawyers to the site to distribute his message criticizing lawyers); DaVinci Tech. Corp. v. Rubino, No. Civ. 05-1561, 2005 WL 1249462, at *8 (D.N.J. May 25, 2005) (finding intent to divert customers from plaintiff's site to infringing domain registered by defendant); Mattel, Inc. v. Internet Dimensions Inc., No. 99 Civ. 10066(HB), 2000 U.S. Dist. LEXIS 9747, at *15 (S.D.N.Y. July 13, 2000) (“The diversion of internet users to a site presenting pornographic images [barbiesplaypen.com], if viewed by a consumer hoping to view information about one of Mattel's products, may well tarnish the image of Mattel's BARBIE products in the minds of those consumers.”).}

\footnote{230. PETA, 263 F.3d at 365.}

\footnote{231. For instance, Stephen Colbert's fake Twitter profile ranks number five for a “Stephen Colbert” Google search. See *supra* note 41 and accompanying text.}

\footnote{232. In the Colbert example, Colbert's native site, www.colbertnation.com, ranks number one for a “Stephen Colbert” Google search.}
profiles are not likely to divert traffic from the celebrity's or brand owner's native site. As stated in *Chatam International v. Bodum*, "Internet surfers are inured to the false starts and excursions awaiting them."233 They are “unlikely to be dissuaded[ ] or unnerved” when they mistakenly pull up the wrong Web page.234

The sixth factor— "the person’s offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain”235—falls in favor of the social networking site because the networks expressly ban the selling of usernames.236 An individual user could sell a username without the knowledge of the social networking site,237 but the site would not be responsible because it would not be involved.

The seventh factor is “the person’s provision of material and misleading false contact information when applying for the registration of the domain name . . . or the person’s prior conduct indicating a pattern of such conduct.”238 This factor does not apply to social networking sites because the sites do not “apply [ ] for the registration”239 of usernames. They merely assign usernames upon user request.240 This statutory language adds to the overwhelming amount of evidence that usernames are not domain names under the ACPA.

The eighth factor is “the person’s registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others.”241 “This factor recognizes the increasingly common cybersquatting practice known as ‘warehousing,’ in which a cybersquatter registers multiple domain names.”242 Twitter guards against username “warehousing” by monitoring “the number of accounts created” by a single user.243 Twitter also removes accounts that are inactive for more than six months to prevent users from registering a name just to hold onto it until someone offers to

---

www.google.com (last visited Jan. 25, 2011) (search for “Stephen Colbert”). Searchers can easily go back and find Colbert’s real site if they happen to land on his fake Twitter page.
234. Id.
236. See supra note 65.
237. A user could provide his log-in information to a buyer to give the buyer control over a profile.
239. Id.
240. See supra note 42 and accompanying text.
policies like these suggest that a social networking site is not likely acting in bad faith regarding this factor.

The ninth factor—"the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous"—will take into account the brand’s or celebrity’s fame and is not particularly relevant to most jacking situations. Most jacked usernames will be at least famous enough for someone to want to jack them. All these factors indicate that a court will probably find that most social networking sites are not acting with bad faith intent to profit from the jacking of brand or celebrity usernames. This result—along with the fact that usernames are not likely domain names under the ACPA—shows that a jacking victim probably will not recover against a social networking site for cybersquatting.

C. Likelihood of Recovery: Trademark Violations

Another potential cause of action is a trademark violation. In these cases, a plaintiff must show (1) likelihood of confusion and (2) commercial use. This Section sets out and analyzes the factors that should be considered in determining likelihood of confusion and commercial use in username-jacking cases. It also evaluates whether a social networking site could be liable for contributory infringement.

1. Likelihood of Confusion Requirement

In any username-jacking situation, whether the jacked profile confused users will be the central point of analysis. In analyzing the likelihood of confusion, jacked username situations fall into three categories: (1) instances in which the profile is obviously fake and a reasonable person could not be confused, as in fake Tony La Russa on Twitter, (2) instances in which a reasonable person could think the profile is real and actually be confused, as in fake Governor Palin on Facebook, and (3) instances in which the user comes across a fake profile through a search engine, clicks because he is initially confused, and then quickly realizes the profile is a fake. Likelihood of confusion should only be found in the second category, where there could be actual confusion.

244. Id.
246. See supra notes 61–62 and accompanying text.
247. See supra notes 56–60 and accompanying text.
248. See supra notes 132–43 and accompanying text.
a. Determining the Likelihood of Confusion

Whether likelihood of confusion exists depends on the content of the individual page. This must be analyzed on a case-by-case basis. For instance, a username-jacking victim should not recover when there is no confusion, as in gripe and parody cases. McCarthy states that gripe sites are a "vehicle for the exercise of free speech protected by the First Amendment, which can trump trademark law."\textsuperscript{249} The parody or gripe must be clear to a reasonable person. Clarity can be achieved by labeling the profile. For example, La Russa's fake profile says, "Parodies are fun for everyone."\textsuperscript{250} Clarity can also be achieved through the profile's name or URL, such as twitter.com/ThriftyCarsucks or twitter.com/McdonaldsSucks. Clarity can also be achieved by the profile's content, based on the principle from Lamparello that no user would ever believe Reverend Falwell, the plaintiff, would sponsor a site criticizing himself.\textsuperscript{251} The number of fans or followers a profile has should also be considered in deciding if users were actually confused, but it should not be outcome determinative. For instance, it is plausible to argue that because the fake Governor Palin had 600 Facebook friends, users were confused. But, the obviously fake Gary Busey Twitter page has 58,000 followers not because users are confused, but because they find fake Gary Busey amusing.\textsuperscript{252} Messages between the fans and the fake profile creator should also be considered. The fact that fake Governor Palin's friends sent her earnest messages could indicate confusion.\textsuperscript{253} Thus, courts should look to the content of the jacked profile to determine the likelihood of confusion.

If a third party squats on a username without creating any content on the profile, users are not likely to be confused. A blank profile does not give the user sufficient evidence to make a decision as to whether the profile is real. Because the likelihood of confusion should be based on the profile's content, confusion cannot be gauged unless the profile has content.

A username-jacking victim should recover when there is actual confusion—despite the Interactive Products line of cases. These cases hold that it is unlikely that an infringing trademark in a URL's post-

\begin{itemize}
\item \textsuperscript{249} McCarthy, supra note 114, § 25:76.
\item \textsuperscript{250} Complaint, La Russa v. Twitter, Inc., No. CGC-09-488101, at Exhibit A (Cal. Super. Ct. June 5, 2009).
\item \textsuperscript{251} Lamparello v. Falwell, 420 F.3d 309, 315 (4th Cir. 2005).
\item \textsuperscript{252} See Not Gary Busey (GaryJBusey) on Twitter, http://twitter.com/GaryJBusey (last visited Jan. 25, 2011). The page is obviously a parody because it is named “Not Gary Busey.”
\item \textsuperscript{253} Rosman, supra note 2.
\end{itemize}
domain path could cause confusion,\textsuperscript{254} and they rest on the assertion that "post-domain paths do not typically signify source" of a trademark.\textsuperscript{255} It is easy to see that a user would not confuse the URL a2zsolutions.com/desks/floor/laptraveler/dkfl-it.htm as the "laptraveler" trademark's actual source.\textsuperscript{256} The a2zsolutions.com/desks/floor/laptraveler/dkfl-it.htm URL clearly indicates that a2zsolutions—not laptraveler—controls the domain. But due to the massive celebrity and brand adoption of social networking, a user could reasonably think that a URL like twitter.com/TonyLaRussa is controlled by La Russa; the URL signifies the source of La Russa. Consumers expect brands and celebrities to be present on the social networks and thus can be actually confused by a post-domain path (username).\textsuperscript{257}

Social networks realize that profiles which intend to confuse or mislead could give rise to liability. Twitter's impersonation policy, for example, ensures that users know that a permissible parody must be clear: "Accounts with the clear intent to confuse or mislead may be permanently suspended."\textsuperscript{258} However, some profiles apparently intended to mislead remain active.\textsuperscript{259} Such profiles are likely to confuse users and should provide a basis for liability for a trademark violation.

b. Initial Interest Confusion

Initial interest confusion should have no bearing in username-jacking situations, despite the fact that some courts have found trademark infringement when users were initially confused into visiting an infringing Web page.\textsuperscript{260} Initial interest confusion is "the confusion that creates initial interest in [a] competitor's product; although dispelled

\textsuperscript{254} See supra note 145 and accompanying text.
\textsuperscript{255} Interactive Prods. Corp. v. A2Z Mobile Office Solutions, Inc., 326 F.3d 687, 692, 698 (6th Cir. 2003).
\textsuperscript{256} Id. at n.7.
\textsuperscript{257} See supra notes 32–34 and accompanying text.
\textsuperscript{259} For example, live fake profile twitter.com/StephenColbert does not indicate that it is a parody and even attempts to mislead users into thinking it is the real Colbert profile. STEPHEN COLBERT ON TWITTER, supra note 41 (containing the tweet directed at Colbert's real profile, "Which is the real me? (I think it's me)"); see also STEPHEN T. COLBERT ON TWITTER, http://twitter.com/stephencolbert_ (last visited Jan. 25, 2011) (containing the bio "That's right, I'm the REAL Stephen Colbert" even though the profile is fake); STEPHEN COLBERT ON TWITTER, http://twitter.com/stephencolbert (last visited Jan. 25, 2011) (giving no indication that the profile is fake and spamming 96,000 followers with links to deals for products ranging from eyewear to car insurance).
before actual sale occurs, initial interest confusion impermissibly capitalizes on goodwill associated with [the] owner’s mark.” The “competitor’s product” in a username-jacking case is the fake profile; it is competing on the search results page with the brand or celebrity’s native site or real social profile. Courts are split as to whether initial interest confusion spurs trademark infringement in domain name cases. The doctrine is “sporadically applied.” Initial interest on the Web is quickly dispelled by clicking the “back” button. Such confusion is too fleeting to have any bearing and should not be legally significant in username cases. Thus, a username-jacking victim should not recover when users are initially confused.

The initial interest confusion doctrine should have no place in domain name trademark suits. The court in Planned Parenthood Federation of America v. Bucci found initial interest confusion from the defendant’s unauthorized registration of plannedparenthood.com because “Internet users who seek [the] plaintiff’s Web site [may] expend time and energy accessing defendant’s Web site.” This holding is faulty because the mere seconds it takes a user to enter “plannedparenthood.com” into a browser is not sufficient “time and energy” to be legally cognizable. Planned Parenthood and other domain name initial interest confusion cases should not be followed in username cases. For instance, suppose a celebrity’s Facebook profile has been jacked. A searcher goes to Google, searches for that celebrity, and is given search results containing the celebrity’s native site and the celebrity’s fake Facebook profile. The Facebook result may spark the searcher’s interest because it is titled “[Celebrity’s Name] — Facebook,” has description text from the page’s meta description which includes the celebrity’s name, and displays the URL “facebook.com/[celebrity’s name].” The searcher clicks on the listing and quickly realizes the profile is a parody, goes back to the search results, and clicks on the native site result. This user hardly expends any time and energy. Even if it takes the user a few minutes to realize the profile is fake, the time and energy spent by the user is still minimal. If the user is looking for the celebrity’s real Facebook page and comes across a fake page—either by searching on Facebook, directly navigating to what they think could be the celebrity’s Facebook URL,

262. See supra notes 133–43 and accompanying text.
263. Lamparello v. Falwell, 420 F.3d 309, 315 (4th Cir. 2005).
264. See supra note 140 and accompanying text.
or using a search engine—the user can also quickly go back and find the real profile.\textsuperscript{266}

Lamparello noted that courts have only applied the initial interest confusion doctrine when the defendant attempts to use the plaintiff’s mark for financial gain.\textsuperscript{267} It will be difficult to show that a social networking site attempted to use a trademark holder’s mark for financial gain. This is because the social site would not be trying to sell the username to the trademark holder. The site is not likely competing with the trademark holder to sell similar goods or services. The site will remove an infringing profile in good faith upon request.\textsuperscript{268} And if the profile is a gripe or parody, it is noncommercial and the social site is not liable, even if the site is running advertising on the profile.\textsuperscript{269}

Thus, initial interest confusion should not be used to determine the likelihood of confusion in username cases. The likelihood of confusion should be based solely on the content of the profile, taking into account all indicators of parody or gripe. If a page clearly intends to confuse, likelihood of confusion could be found. The social networking site could then be liable for a trademark violation.

2. Commercial Use Requirement

In addition to proving the likelihood of confusion, a username-jacking victim will also have to prove commercial use to recover for a trademark violation. Similar to likelihood of confusion, a finding of commercial use will depend on the content of the jacked profile. If the profile is not a parody or gripe page, the jacking victim will probably be able to prove commercial use by showing that the social networking site contained a commercial aspect, such as advertising.

\textsuperscript{266} This is assuming the brand or celebrity has a real profile. If they do not, the fake profile cannot compete with a nonexistent profile.

\textsuperscript{267} Lamparello, 420 F.3d at 317 (citing PACCAR Inc. v. TeleScan Techs., L.L.C., 319 F.3d 243, 253 (6th Cir. 2003) (finding initial interest confusion where defendant attempted to use the strength of the “Peterbilt” and “Kenworth” marks to drive business to his truck locator service)); Promatek Indus., Ltd. v. Equitrac Corp., 300 F.3d 808, 812–13 (7th Cir. 2002) (finding possible initial interest confusion where the plaintiff and defendant were competitors and the defendant used the plaintiff’s mark in its meta tags to attempt to drive business away from the plaintiff); Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036, 1056 (9th Cir. 1999) (finding initial interest confusion where plaintiff and defendant were competitors).

\textsuperscript{268} See supra note 215 and accompanying text.

Facebook, MySpace, and LinkedIn contain advertising on profile pages and are therefore commercial.270 Twitter began running advertising in April 2010 on internal search results pages;271 but, as of August 2010, it is not running ads on profile pages. Twitter does have licensing deals in place with Google and Microsoft’s Bing that allow the engines to feed tweets into their search results pages.272 Reports say that the Bing deal involved a several million dollar payment to Twitter, as well as ad revenue sharing.273 Thus, a Twitterjacking victim could argue that Twitter sold fake tweets under his name to Google and Bing. Additionally, as more celebrities and brands—real or fake—open Twitter profiles, more consumers use Twitter to see what these celebrities and brands are saying, thereby increasing Twitter’s commercial value.274 In this way, a Twitter profile page may have a commercial aspect sufficient to spur a trademark violation.

If the profile is a parody, gripe page, or contains political speech, the use will likely be deemed noncommercial.275 There is a line of domain name parody and gripe cases finding commercial use that should not be followed in username situations. For instance, the PETA court held that the defendant’s registration of peta.org constituted commercial use because the site linked to more than thirty commercial operations that sold goods and services, and the defendant told PETA to “make him an offer” for the domain name.276 Commercial use was found even though the site was a clear parody on PETA: “People Eating Tasty Animals.”277 PETA is an outlier and is distin-

274. See generally Jessica E. Vascellaro & Michael Corkery, Twitter’s Value Is Set at $1 Billion, WSJ.COM (Sept. 28, 2009), http://online.wsj.com/article/SB125382643140938735.html.
275. See supra notes 149–51 and accompanying text.
277. Id. at 366, 362.
guishable from username-jacking cases because the PETA defendant offered to sell the domain name to PETA.\textsuperscript{278} A social networking site would not likely offer to sell a jacked username to a trademark holder. Thus, even though parody or gripe social media pages have a commercial aspect, these pages should be deemed noncommercial because the social site is not attempting to sell the username.

\textit{Planned Parenthood}\textsuperscript{279} and \textit{Jews for Jesus v. Brodsky}\textsuperscript{280} are other gripe/parody cases where the court found commercial use. These cases should not be followed in username-jacking situations. The \textit{Planned Parenthood} court stated that the defendant's use of plannedparenthood.com was commercial because the defendant's actions were "designed to, and do, harm [the] plaintiff commercially."\textsuperscript{281} The U.S. District Court for the District of New Jersey came to a similar holding in \textit{Jews for Jesus}.\textsuperscript{282} Commercial use constituting infringement was found in both \textit{Planned Parenthood} and \textit{Jews for Jesus} merely because the defendants registered domain names intended to intercept the plaintiffs' audiences.\textsuperscript{283} Despite these holdings, the registration of a domain name should not alone constitute commercial use. Other courts have been critical of the \textit{Planned Parenthood} and \textit{Jews for Jesus} cases. The \textit{Ford Motor Co. v. 2600 Enterprises} court stated that if the "'commercial use' requirement is to have any meaning, it cannot be interpreted so broadly as to include any use that might disparage or otherwise commercially harm the mark owner."\textsuperscript{284} The \textit{Ford} court also declared that "the 'in connection with goods or services' requirement is not satisfied simply because a prospective user of the Internet may face some difficulty in finding the home page

\begin{itemize}
\item \textsuperscript{278} Id. at 368.
\item \textsuperscript{281} Planned Parenthood, 1997 U.S. Dist. LEXIS 3338 (KMW), at *5-7 (finding defendant's use competitive because "defendant's appropriation not only provides Internet users with competing and directly opposing information, but also prevents those users from reaching plaintiff and its services and message. In that way, defendant's use is classically competitive.").
\item \textsuperscript{282} See Jews for Jesus, 993 F. Supp. at 308 ("The conduct of the Defendant also constitutes a commercial use of the Mark . . . because [the use] is designed to harm the Plaintiff Organization commercially by disparaging it and preventing [it] from exploiting the Mark . . . "); \textit{but see} Ford Motor Co. v. 2600 Enters., 177 F. Supp. 2d 661, 664 (E.D. Mich. 2001) (rejecting Ford's claim that defendant's registration of fuckgeneralmotors.com constituted dilution-related commercial use in the sense that it disparaged and prevented Ford from fully exploiting its mark).
\item \textsuperscript{283} Jews for Jesus, 993 F. Supp. at 308 (finding infringement because defendant religious activist created "a bogus 'Jews for Jesus' site intended to intercept, through the use of deceit and trickery, the audience sought by the Plaintiff"); \textit{Planned Parenthood}, 1997 U.S. Dist. LEXIS 3338, at *9 (finding infringement because defendant religious activist intended to intercept Planned Parenthood's audience and expose them to a right to life message).
\item \textsuperscript{284} Ford Motor Co., 177 F. Supp. 2d at 665.
\end{itemize}
he is seeking."\textsuperscript{285} McCarthy states that "neither merely reserving a domain name nor use of a domain name solely to indicate a site on the Internet, in and of itself, constitutes 'goods or services' in the Lanham Act sense. Rather, one must consider the content of the site identified by the domain name."\textsuperscript{286}

Courts evaluating username jacking should take a stance similar to that of the \textit{Ford} court and McCarthy and look to the content of the profile in question. If the page is a parody or gripe—or if there is no content at all because the third party is merely squatting on the name—there should be no commercial use. If the profile’s content suggests the intent to confuse consumers—and thus possibly compete with the celebrity’s or brand’s native site or real social media profile—a court should find commercial use.

3. \textit{Contributory Trademark Infringement}

In addition to suing for direct infringement, username-jacking victims may also sue for contributory trademark infringement. A jacking victim will not likely be able to prove contributory infringement unless the social networking site fails to remove an infringing profile upon receiving notice that the profile is infringing.

As long as the social networking sites remove profiles that they know are infringing, they will not be contributorily liable for their users' infringements. \textit{Tiffany v. eBay} held that for a service provider to be contributorily liable, it must have more than "general knowledge" that its service can be used for infringement.\textsuperscript{287} The \textit{Tiffany} court found eBay not contributorily liable for third-party users selling counterfeit Tiffany goods because eBay removed the listings in question when it discovered they were counterfeit.\textsuperscript{288} eBay gained knowledge of the counterfeit listings through its own monitoring practices, buyer complaints, and complaints from Tiffany.\textsuperscript{289} Thus—as long as eBay removed the counterfeit listings upon gaining specific knowledge that they were counterfeit—it was not contributorily liable for having general knowledge that its site could be used to sell counterfeit goods.\textsuperscript{290} Social networking sites have general knowledge that users

\begin{itemize}
\item \textsuperscript{285} \textit{Id.} See also Strick Corp. v. Strickland, 162 F. Supp. 2d 372, 379 (E.D. Pa. 2001) ("Any inconvenience to an Internet user searching for plaintiff's web site is trivial. Searches for plaintiff's web page on popular internet search engines, including google.com... list Plaintiff's web site as their first or second 'hits.'").
\item \textsuperscript{286} \textit{McCarthy, supra} note 114, \S 25:76.
\item \textsuperscript{287} \textit{Tiffany, Inc. v. eBay, Inc.}, 600 F.3d 93, 107 (2d Cir. 2010).
\item \textsuperscript{288} \textit{Id.} at 109.
\item \textsuperscript{289} \textit{Id.}
\item \textsuperscript{290} \textit{Id.} at 107.
\end{itemize}
can jack others' usernames. But, per Tiffany, they can only be contributorily liable if they do not remove infringing usernames that they have specific knowledge of. As long as a social networking site does not intentionally shield itself from learning about infringing usernames and removes infringing usernames that it is aware of, it will not be contributorily liable.

Thus, for a jacking plaintiff to recover for a trademark violation, the content of the jacked profile must be (1) commercial and (2) likely to confuse users into thinking the profile is real. Because the social networking sites strictly prohibit the creation of profiles that intend to confuse users, there will not likely be many cases that satisfy these requirements. Contributory infringement is also unlikely, assuming the sites remove infringing usernames upon gaining knowledge of the infringement.

D. Likelihood of Recovery: Right of Publicity

Username-jacking victims should also have difficulty recovering for right of publicity violations. The state right of publicity protects a person’s interest in profiting from the use of his persona. This Section analyzes whether § 230 of the CDA immunizes Web site operators from right of publicity claims, in light of the federal court split on the issue. It then examines additional challenges that jacking victims will likely face in publicity actions.

1. Federal Court Split: Which Rule Is More Consistent with the Policy of § 230?

Courts are split on whether § 230 bars state right of publicity claims. The United States Court of Appeals for the Ninth Circuit held in Perfect 10 that § 230 immunizes Web site operators from right of publicity claims. The United States District Court for the District of New Hampshire took the opposite stance in Friendfinder. Friendfinder held that the word “any” in (e)(2)— “[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property”—meant that § 230 did not immunize Web site operators from any intellectual property claims—federal or state. But (e)(3) states

291. Id. at 109.
292. See supra notes 155–56 and accompanying text.
293. See infra notes 297–318 and accompanying text.
294. See infra notes 318–35 and accompanying text.
295. Perfect 10, Inc. v. CCBill, L.L.C., 488 F.3d 1102, 1118–19 (9th Cir. 2007).
that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." Right of publicity laws are state laws that are "inconsistent" with § 230. Thus, social networking sites should be immune from right of publicity claims.

To allow a right of publicity claim against a social site would undermine § 230's express purpose—to promote unfettered growth and innovation on the Internet. When passing § 230, Congress could not have imagined the benefits to society derived from the mass adoption of social networking. Nevertheless, Congress paved the way for these benefits by granting broad immunity to Web site operators. Social networking sites are a direct result of Congress's goal of advancing innovation on the Internet. These sites could not have evolved without Congress's broad protection. The value of a celebrity's persona deserves protection. But it does not deserve protection to the degree that social networking sites are sued into extinction because they cannot continually police their mass volume of third-party content.

*Friendfinder* stated that the Internet evolved despite a "general consensus" before *Perfect 10* that § 230 did not immunize Web site operators from state intellectual property claims, such as the right of publicity. But *Friendfinder* did not offer much support for this

---

300. See supra notes 98–99 and accompanying text.
301. See supra notes 32–34 and accompanying text. Social networking sites connect people who want to be connected, allowing for the sharing of user product reviews. See Li & Bernoff, supra note 70, at 234–35. Social networking sites amplify consumer opinions, allowing people to help one another discover new products. William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. Ill. L. Rev. 1105, 1112–13 (noting that "[m]arkets function better when individual consumer purchasing decisions rely on improved information, as they do in an environment saturated with accessible and relevant peer opinions").
302. 47 U.S.C. § 230(a)(1)–(5) lays out the five reasons for granting this immunity:
   The Congress finds the following:
   (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.
   (2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.
   (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
   (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of governmental regulation.
   (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.
303. See *Friendfinder*, 540 F. Supp. 2d at 301–02.
“general consensus.” The court cited only two cases to support its contention, neither of which involved the right of publicity: (1) Universal, which stated in dicta that Florida’s trademark dilution statute was a state intellectual property claim not barred by § 230, but then decided the dilution claim was more like a defamation claim, and (2) Gucci America, Inc. v. Hall & Associates, a trademark case which stated that subsection (e)(2) applied to both federal and state intellectual property claims. Gucci dealt with Lanham Act claims as well as New York common law trademark infringement and unfair competition claims. The state trademark laws involved in Gucci were similar to federal trademark laws; allowing liability under these laws is less likely to be inconsistent with the purpose of § 230. Right of publicity laws, on the other hand, do not have a federal counterpart; they should be analyzed separately from state trademark laws to determine if they are inconsistent with § 230. The question of whether § 230 bars a right of publicity claim was not even answered until Perfect 10. Thus, it was impossible for a “general consensus” to have emerged.

The Friendfinder decision threatens to open the floodgates of litigation in username-jacking situations. A right of publicity claim requires no showing of the likelihood of consumer confusion. A celebrity would only have to show that the social networking site used, without permission, some aspect of his identity likely to hurt his persona’s commercial value. This includes showing that the network used the persona for a commercial purpose. To show commercial purpose, the celebrity could point to advertisements running on the profile page or distribution deals. Courts have held that if the use of a celebrity persona is deemed to be largely for commercial purposes, the right of publicity outweighs the First Amendment right to

304. Id. at 298, 302 (citing Universal Commc’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 422–23 (1st Cir. 2007)).
305. Id. at 302 (citing Gucci Am., Inc. v. Hall & Assoc., 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001)).
307. Id.
308. See Perfect 10, Inc. v. CCBill, L.L.C., 488 F.3d 1102 (9th Cir. 2007).
309. See supra note 164 and accompanying text.
310. See supra notes 157–67 and accompanying text. This could even extend to situations in which the third party does not jack the celebrity’s username. For instance, the third party could be using a photo or other aspect of the celebrity’s personality. See, e.g., Henley v. Dillard Dep’t Stores, 46 F. Supp. 2d 587, 591–95 (N.D. Tex. 1999) (finding that plaintiff [Eagles’ singer Don Henley] was sufficiently identified by an advertisement that said “This is Don’s henley”); Hirsch v. S.C. Johnson & Son, Inc., 280 N.W.2d 129, 137 (Wis. 1979) (finding that plaintiff was identified by a nickname).
312. See supra notes 270–74 and accompanying text.
free expression through gripe or parody. For instance, the court in White v. Samsung Electronics America allowed Vanna White’s right of publicity claim against Samsung when the company used a parody robot version of White in a television advertisement. The court rejected Samsung’s First Amendment parody argument by stating that the First Amendment does not bar all right of publicity actions against forms of expressive activity. In commercial advertising, the First Amendment will not bar a publicity claim, even if the use is a parody. This could make it too easy for username-jacking victims to recover in situations where the profile is a clear parody or gripe. Courts evaluating username jacking should consider other factors—like whether users were actually confused by the profile—before victims are allowed to recover.

Perfect 10 held that subsection (e)(2) immunized interactive computer services from state intellectual property laws. The court stated that any other reading of subsection (e)(2) would be contrary to Congress’s expressed goals in enacting the CDA. Right of publicity laws—whether by state common law or statute—are inconsistent with the CDA. Even though Friendfinder’s reading of subsection (e)(2) is plausible, username-jacking courts should embrace Perfect 10 and Congress’s policy “to promote the continued development of the Internet.”

2. Additional Challenges for Jacking Victims

Even if a court takes the Friendfinder view and allows state right of publicity claims, a username-jacking victim could still have difficulty recovering. The jacking victim must prove that the social networking site’s use of his persona was “likely to cause damage to the commercial value of that persona.” This should be determined based on the content of the profile. For instance, if the profile is a clear parody, no reasonable user will believe that the celebrity authorized the profile. Thus, damage to the persona’s commercial value is unlikely.

315. Id. at 1401 n.3.
316. Id.
317. Perfect 10, Inc. v. CCBill, L.L.C., 488 F.3d 1102, 1118 (9th Cir. 2007).
318. Id.
320. See McCarthy, supra note 156, § 3:2.
321. See Roberta Rosenthal Kwall, A Perspective on Human Dignity, the First Amendment, and the Right of Publicity, 50 B.C. L. Rev. 1345, 1368–69 (2009) (“[I]t is precisely because the
This is consistent with the United States Court of Appeals for the Tenth Circuit's decision in *Cardtoons v. Major League Baseball Players Ass'n*. The court held that Oklahoma's right of publicity statute contained a First Amendment parody exception. Right of publicity could outweigh free expression in instances where the use of the persona is deemed primarily commercial. But, even though social media profiles contain advertising, they do not use the celebrity personas in the ads, as in the Vanna White case. Thus, social media profiles are generally not primarily commercial, and parody/gripe profiles will be protected by the First Amendment.

Additionally, some scholars have advocated that right of publicity actions used to protect a persona's commercial value should be treated differently than publicity actions used to protect a person's sense of dignity. This has implications for § 230 immunity. For instance, La Russa alleged emotional and reputational damage as part of his right of publicity claim. Perhaps a publicity claim alleging harm to a celebrity's personal dignity is less like an intellectual property claim and more like a defamation claim, which is routinely barred by § 230. The clear policy of § 230 is to disallow causes of actions based on hurt feelings. It is thus consistent with § 230 to bar a right of publicity claim that is based on emotional distress or reputational damage. This, however, can affect monetary damages. Without damages for emotional distress, embarrassment, or bruised reputation, a username-jacking victim would only be able to recover damages for specific commercial loss.

Specific commercial loss could be small in username-jacking cases. Damages for publicity violations focus on actual damage to the celebrity and profit (revenue minus expenses) to the infringer from the unauthorized use. Revenue to the social network from a jacked profile is likely very low. For instance, Twitter had little to no revenue

---

323. *See supra* notes 313–16 and accompanying text.
325. Complaint, La Russa v. Twitter, Inc., No. CGC-09-488101, at 6 (Cal. Super. Ct. June 5, 2009) ("Plaintiff has suffered emotional distress, damage to his reputation and general damages in the sum to be shown according to proof.").
326. *See supra* notes 97–100 and accompanying text.
327. *See, e.g.,* CAL. CIV. CODE § 3344(a) (West 2000) ("In establishing such profits, the injured party or parties are required to present proof only of the gross revenue attributable to such use, and the person who violated this section is required to prove his or her deductible expenses.").
until April 2010, when it rolled out its first revenue model. Facebook’s 2009 revenues are estimated to be $700 million from a base of approximately 36 billion visits. Thus, Facebook makes about 1.94 cents per visit. Even if each of fake Governor Palin’s 600 friends visited the fake page every day for the two months it was jacked, Facebook would only make about $700 from the page. Thus, even a successful publicity plaintiff may receive an award not worth the cost of the lawsuit.

Additionally, punitive damages are available in publicity cases only when the infringer knowingly used the persona. It will be difficult for a jacking victim to prove that the social networking site knowingly used his persona, because the site did not actually use the persona at all—a third party did. The lack of punitive damages—in addition to small profits to the social network and no damages for dignity harm—make it difficult for publicity plaintiffs in jacking suits to recover a worthwhile amount of money. Statutory damages are low—for instance, $750 in California. The court will award the celebrity an injunction, but the results of an injunction could have been achieved simply by asking the social networking site to remove the jacked profile.

Username-jacking plaintiffs should have difficulty recovering from the social sites. Section § 230 will block defamation claims. The ACPA likely does not protect username squatting. The large majority of cases will lack the requisite likelihood of confusion to succeed in a trademark violation claim. Finally, courts should embrace Congress’s policy to promote Internet growth unfettered by state regulations like

328. Stone, supra note 271.
331. This number was derived from the $700 million in revenue divided by the thirty-six billion visits and assumes that each visit was equally valuable.
332. The number of visits was derived from the 600 users multiplied by the 60 days the profile was live to get 36,000 visits. That number was then multiplied by the 1.94 cents that Facebook receives in revenue for each visit. Facebook would be allowed to subtract its expenses for maintaining the page, which are likely low, from the revenue number. See, e.g., CAL. CIV. CODE § 3344(a).
333. MCCARTHY, supra note 156, § 11:36.
334. CAL. CIV. CODE § 3344(a).
335. See supra notes 66–69 and accompanying text.
right of publicity laws. Even in jurisdictions that may allow a publicity action, the legal costs may not be worth the potential damage awards.

IV. IMPACT

The large majority of username-jacking situations should be resolved without the involvement of the courts. This Part articulates what username-jacking victims and social networking sites can do to avoid unnecessary litigation. It also outlines what social networks are doing to prevent username jacking.

Celebrity and brand owners should first make it a priority to claim their social media usernames before someone else does. It is their responsibility to manage their online identities. With the massive growth of social networking, they cannot ignore their social network identities. If their names are jacked, they should simply contact the social networking site to recover their names. A lawsuit or a dispute resolution process along the lines of the UDRP is not necessary. All that is necessary is a conversation between the jacking victim and the social site. This Comment has shown that the majority of username-jacking victims should not succeed in lawsuits against social sites. Moreover, the few jacking victims that should succeed should be awarded an injunction, which amounts to the recovery of the profile. Monetary awards are not worth the lawsuit's cost. Thus, a jacking victim can accomplish the same result—an injunction—by talking to the social site instead of suing it.

Social sites do enough to prevent username jacking. Any further precautions would impair their ability to quickly grow for the benefit of the Internet and society in general. Pre-jacking precautions are difficult for social networking sites to implement because, in order to grow their user bases, the sites must make it easy for users to sign up. It is also impossible and burdensome to users for the social sites to verify every user before allowing them to claim a username. Because of the latitude that the social sites must give users in signing up and choosing usernames, there will always be some risk of username jacking despite policies that forbid users from claiming usernames that they do not have rights to. The sites therefore take precautions to

337. See infra notes 341–45 and accompanying text.
338. The UDRP governs domain name disputes and provides that the dispute “must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name.” Uniform Domain Name Dispute Resolution Policy, supra note 115.
339. See supra notes 324–35 and accompanying text.
340. See Facebook Statement of Rights and Responsibilities, supra note 65; Twitter Support, supra note 65.
protect tradmarked names once they have been jacked. For instance, Facebook requires that a user be an official representative of the brand or celebrity to create a page for that brand or celebrity. If a user violates this rule, Facebook removes the user and the unauthorized page. Twitter also bans users who do not comply with trademark and parody guidelines. Twitter also uses “verified accounts,” which indicate that Twitter has “been in contact with the person or entity the account is representing and verified that it is approved.” The account then receives a “verified account” badge that informs consumers that the brand or celebrity is really who they say they are. Thus, social sites are working to prevent username jacking.

But social sites cannot catch every jacking attempt. Sometimes the sites will not know that a profile has been jacked until the jacking victim makes the site aware. The social sites need to actively avoid litigation by being responsive to jacking victims. For instance, La Russa sued Twitter after trying to reach them for a week to get his fake profile removed. Twitter deleted the profile after receiving the complaint and La Russa quickly dropped the suit. La Russa’s suit was either a scare tactic to recover his profile or the only mechanism he felt he had left to achieve what he wanted. Conversely, Facebook “worked quickly to resolve the situation and was very responsive” when Sarah Palin’s attorney asked them to remove Palin’s fake profile. MySpace was quick to return candidate Barack Obama’s profile at the request of his campaign. Lawsuits were avoided in both of these instances. A lawsuit likely could have been avoided in La Russa’s situation had Twitter been more responsive.

La Russa could have used Twitter’s trademark violation complaint process in lieu of suing. But celebrities and brand owners cannot be expected to comply with a username recovery process when they do not know how long it will take, especially when their name is being defamed in the meantime. Twitter does not need to have a twenty-

341. Facebook: Create a Page, supra note 72.
342. Facebook Statement of Rights and Responsibilities, supra note 65.
343. The Twitter Rules, supra note 65.
344. Twitter Verified Account, supra note 41.
345. Id.
346. Matier & Ross, supra note 82.
347. Id.
348. Natural gas distributor Oneok may have also used its suit against Twitter as a scare tactic. Oneok dropped the suit one day after filing when Twitter returned Oneok’s handle. Oneok Drops Trademark Lawsuit, supra note 86.
349. Rosman, supra note 2 (quoting Sarah Palin’s attorney).
350. Rosmarin, supra note 44.
351. Trademark Policy, Twitter Support, supra note 215.
four hour jacking hotline; it simply needed to return La Russa's phone calls. Thus, celebrities, brands, and social networking sites can all better communicate to prevent this unnecessary litigation.

V. Conclusion

The majority of username-jacking victims will probably not succeed in court against the social networking sites on causes of action such as defamation, intentional infliction of emotional distress, cybersquatting, trademark infringement, and right of publicity violations. Cybersquatting laws should not apply to usernames because the ACPA covers domain names, not sub-domains like Facebook vanity URLs and Twitter handles. Celebrities should not recover on right of publicity claims under § 230 because Congress passed the CDA in large part to promote the unfettered growth of the Internet. Allowing username-jacking publicity claims would impede the growth of social networking, which has benefited society. The social networking sites should also be free from contributory liability as long as they remove infringing profiles upon gaining knowledge of the profiles. Jacking victims should not recover for trademark violations when the profile is clearly a gripe or parody, as this would violate First Amendment freedom of expression. Thus, jacking victims should only recover for trademark violations when the jacked profile is likely to confuse users into thinking that the profile is really controlled by the celebrity or brand, and the social networking site does not remove the profile upon gaining notice of its existence.

However, jacking victims can achieve the same remedy—an injunction preventing the use of the username—by working with the social sites to reclaim jacked usernames instead of suing the sites. Social networking sites have sufficient username dispute resolution processes in place, and it is a waste of judicial resources for celebrities and brands to sue for username jacking. On the other hand, social sites need to help avoid litigation by being responsive to brands and celebrities whose profiles have been jacked.

Dan Malachowski*

---

* J.D. Candidate 2012, DePaul University College of Law; Bachelor of Science 2003, Boston College. Thank you to Aaron White for valuable feedback and direction, the DePaul Law Review Volumes 59 and 60 for editorial help, and my wife Madeline for support through this entire process.