Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 23 *Volume XXIII*
Number 3 *Volume XXIII Book 3*

Article 5

2013

Access Denied: How Social Media Accounts Fall Outside the Scope of Intellectual Property Law and into the Realm of the Computer Fraud and Abuse Act

Tiffany Miao
Fordham University School of Law, tmiao@law.fordham.edu

Access Denied: How Social Media Accounts Fall Outside the Scope of Intellectual Property Law and into the Realm of the Computer Fraud and Abuse Act

Cover Page Footnote

Managing Editor, Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIII; J.D. Candidate, Fordham University School of Law, May 2013; B.S., Business Administration, University of California Berkeley, 2006. Endless thanks to Ryan Fox for his patient support and invaluable insight, and Meredith Hatic and the IPLJ staff for their helpful contributions. I would also like to thank Professor Ron Lazebnik for his input and guidance. Lastly, a special thanks to my friends for bearing with me while I "noted" and my family for never asking me, "What is a Note?"

Access Denied: How Social Media Accounts Fall Outside the Scope of Intellectual Property Law and into the Realm of the Computer Fraud and Abuse Act

Tiffany A. Miao∗

∗ Managing Editor, Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIII; J.D. Candidate, Fordham University School of Law, May 2013; B.S., Business Administration, University of California Berkeley, 2006. Endless thanks to Ryan Fox for his patient support and invaluable insight, and Meredith Hatic and the IPLJ staff for their helpful contributions. I would also like to thank Professor Ron Lazebnik for his input and guidance. Lastly, a special thanks to my friends for bearing with me while I "noted" and my family for never asking me, "What is a Note?"

INTRODUCTION

Friendship is priceless, but a Facebook friend—probably $2.50. In November 2011, the cellphone blog and review company PhoneDog filed a lawsuit claiming each follower to a Twitter

account is worth $2.50.[1] With 17,000 Twitter followers at $2.50 each, a lot of money was at stake. In fact, PhoneDog claimed a total of $340,000 in damages: $42,500 for each of the eight months after its former employee, Noah Kravitz, changed the Twitter account from "@PhoneDog_Noah" to "@noahkravitz."[2] Although social media began as a predominately interpersonal method of connecting with friends and family, it has now immersed itself in the business world.

As consumers become inextricably tied to their social networks, businesses too are now compelled to establish their presence on social media.[3] For example, many company websites now include a Facebook, Twitter, or LinkedIn plugin.[4] Moreover, companies have hired employees for the sole purpose of managing and updating their social media accounts ("SMAs").[5] In fact, the use of SMAs span across industries. For example, the National Basketball Association ("NBA") created the Twitter account "@NBA_Labor" to communicate directly with fans and the media about the 2011 season lockout, seeking to also clarify any rumors or misinformation that might have been floating around.[6] Even utility companies have established SMAs to engage stakeholders in a discussion about clean energy and to spread the word about smart grids.[7] Consequently, this unprecedented realm of interaction has left businesses, individuals, and the legal community struggling to determine the acceptable boundaries within social media. This challenge stems from the desire to protect legitimate business interests and employees' rights and mobility with the innovative and progressive potential provided through social networks.

---

1 PhoneDog v. Kravtiz, No. C 11 03474 MEJ, 2011 WL 5415612, at *4 (N.D. Cal. Nov. 8, 2011).

2 *Id*.

3 *See* Carolyn Elefant, *The "Power" of Social Media: Legal Issues & Best Practices for Utilities Engaging in Social Media*, 32 ENERGY L. J. 1, 4 (2011).

4 *See* Leyl Master Black, *How To: Use Facebook Plugins on Your Website*, MASHABLE.COM (Mar. 22, 2011), *available at* http://mashable.com/2011/03/22/facebook-social-plugins-2.

5 *See* cases cited *infra* Part I.B.

6 Mike Saechang, *Twitter's Impact on the NBA Lockout*, EDELMAN DIGITAL (Dec. 20, 2011), *available at* http://www.edelmandigital.com/2011/12/20/twitter-nba-lockout.

7 *See* Elefant, *supra* note 3, at 6–7.

Given the benefits and competitive necessity, for at least some businesses, to use social media, explicit ownership of an SMA allows a business to control how and what it communicates to its customers and to the public. This scope of ownership can be determined based upon control over the three key assets of an SMA: access information, posted content, and subscriber lists. Access information—the login and password—is a crucial element of ownership, without which a business loses its ability to communicate to its consumers and public.[8] Another valuable asset is the content posted. SMA posts provide a platform for virtually instantaneous information exchange between consumers and the business, where consumers can respond to new products or features and businesses can implement targeted marketing.[9] The third asset is the subscribers. Subscribers to an SMA are the motivation behind creating an SMA, and arguably these subscribers represent monetary value to the company.[10] Consequently, the key for employers in protecting their business's SMA is being able to claim ownership over all three assets—the password, content, and subscriber list.

This Note will argue that intellectual property law provides an inappropriate legal framework for employers in claiming ownership rights over their SMAs, because each of the relevant intellectual property regimes fails to address all three assets of an SMA. Part I of this Note provides a brief description of social media including the current litigation over SMAs, and lays out the relevant legal frameworks—Trademark, Copyright, Trade Secrets, and the Computer Fraud and Abuse Act ("CFAA"). Part II examines how the three intellectual property regimes apply to SMAs and reveals how they fail to provide adequate ownership

---

[8] In many of the current cases involving SMAs, the litigation stemmed from one party changing the access information to prevent the other party from accessing the account. *See, e.g.*, *PhoneDog*, 2011 WL 5415612 at *1 (describing how the suit ensued after the former employee changed the Twitter handle and password).

[9] *See* Bart Perkins, *Is Social Connectivity Friend or Foe to Corporations?*, COMPUTERWORLD (Jan. 6, 2012), *available at* http://www.computerworld.com/s/article/9223200/Bart_Perkins_Is_social_connectivity_friend_or_foe_to_corporations_.

[10] *See* John Biggs, *A Dispute Over Who Owns a Twitter Account Goes to Court*, N.Y. TIMES, Dec. 25, 2011, at B1, *available at* http://www.nytimes.com/2011/12/26/technology/lawsuit-may-determine-who-owns-a-twitter-account.html.

protection over the main assets of an SMA. In Part III, this Note proposes the CFAA as a more effective framework for asserting account ownership.

I. BACKGROUND: SOCIAL MEDIA AND INTELLECTUAL PROPERTY LAWS

A. The Development of Social Media

"Social media" is a term used to describe web-based technologies that provide a platform for interactive information exchange, user-created content, and visible social connections.[11] These websites typically allow users to create their own public profiles and connect with other users based on shared interests such as music, movies, other activities, and even mutual friends.[12] Typically, through public profiles, users are able to provide basic personal information, upload photos, and post commentary. Once users are connected, each may view and browse other users' profiles. The most recognized and used social media websites include Facebook.com, Twitter.com, and Linkedin.com.[13]

What began as personal social media—one person establishing connections with friends, family members, and acquaintances[14]—has now evolved into a multi-million dollar industry.[15] The first social media websites were developed with a focus on the individual user and forming personal connections with friends or new acquaintances.[16] This new motivation marked a shift from already-existing Interest-based platforms—namely discussion boards—toward a platform more along the lines of personal networks, with the individual user at the center.[17] Due to the

---

[11] *See generally* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMMC'N 210 (2007), *available at* http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/pdf.

[12] *See id.* at 212–13.

[13] *See* Sorav Jain, *40 Most Popular Social Networking Sites of the World*, SOCIALMEDIA TODAY (Oct. 6, 2012), http://socialmediatoday.com/node/195917.

[14] *See* Boyd & Ellison, *supra* note 11, at 214–15.

[15] *See e.g.*, John Letzing, *LinkedIn Sets Tone for Social Networks*, WALL ST. J., Feb. 10, 2012, at B7.

[16] *See* Boyd & Ellison, *supra* note 11, at 214–15.

[17] *See id.* at 219.

popularity and growth of social media websites, account holders have expanded from individuals to businesses, and uses have expanded from simply staying connected with friends to furthering corporate initiatives.[18] Given the growing connectedness between individuals via social media, companies are now beginning to contemplate social media's potentially high-impact role for their business and in their business.[19]

B. Recent Litigation

In the past few years, the increasing role of social media in the corporate world has created a niche of lawsuits between employers and employees. Looking at the background of just a few of these cases helps to introduce the difficulty in using—or misusing—intellectual property claims to assert ownership rights over an SMA. Along with *PhoneDog*, two other noteworthy cases that demonstrate this challenge include *Ardis Health, LLC v. Nankivell* and *Eagle v. Morgan*.

In *PhoneDog*, the company hired Kravitz as a product reviewer and video blogger. PhoneDog gave Kravtiz permission to access and use the Twitter account "@PhoneDog_Noah," in conjunction with promoting the company's services.[20] After over four years with PhoneDog, Kravitz resigned, and when the company asked him to hand over the account, Kravitz instead changed the Twitter handle to "@noahkravitz."[21] In response, PhoneDog sued Kravtiz, alleging, among other claims, misappropriation of its trade

---

[18] For example, Twitter has an entire website dedicated to professional Twitter accounts. According to the website, a business' Twitter account allows the company to quickly share information, gather market intelligence and insights, and build relationships with people who care about company. *See Twitter 101*, TWITTER, https://business.twitter.com/twitter-101 (last visited Mar. 27, 2013). Similarly, Facebook also has an entire website designated for businesses, providing an in depth guide for creating a company Facebook page, promoting the page, and expanding the page. *See Facebook for Business*, FACEBOOk, https://www.facebook.com/business/build (last visited Mar. 27, 2013).

[19] *See* Perkins, *supra* note 9.

[20] PhoneDog v. Kravtiz, No. C 11 03474 MEJ, 2011 WL 5415612, at *4 (N.D. Cal. Nov. 8, 2011).

[21] *Id.*

secrets—specifically its account password and Twitter followers.[22] The district court declined to dismiss PhoneDog's claim for misappropriation of trade secrets, suggesting that Twitter followers and a Twitter password may in fact be trade secrets.[23] In the end, the parties settled,[24] leaving open the issues of whether a password and followers are trade secrets, and more broadly, what legal framework should be applied in determining the ownership rights to an SMA.

Eagle v. Morgan is an example of an employer-employee dispute over a LinkedIn account that incorporates CFAA and Lanham Act claims.[25] In 1987 Linda Eagle co-founded Edcomm, a banking education company.[26] During her later years of employment with Edcomm,[27] Eagle created and used the LinkedIn account to develop and maintain an extensive network of professional contacts for the business.[28] In 2011, after her termination, Eagle attempted to access the account; however, the company had already changed the account name, photograph, and password.[29] Immediately, Eagle filed suit, pro se, against her employers. In October 2012, just over a year later, the district court granted the defendants' motion for summary judgment for both Eagle's CFAA and Lanham Act claims.[30] In doing so, the

---

22 *See id.* at *1 (listing all of PhoneDog's claims, which include "(1) misappropriation of trade secrets; (2) intentional interference with prospective economic advantage; (3) negligent interference with prospective economic advantage; and (4) conversion").

23 *See id.* at *10 (dismissing PhoneDog's intentional and negligent interference with prospective economic advantage claims).

24 *See* Stipulation for Dismissal After Settlement, PhoneDog v. Kravtiz, No. 3:11-cv-03474-MEJ, 2013 WL 207773 (N.D. Cal. Jan. 7, 2013).

25 Eagle v. Morgan, No. 11-4303, 2012 WL 4739436, at *2 (E.D. Pa. Oct. 4, 2012). In addition to the federal claims, the plaintiff also asserted state law claims including: (1) unauthorized use of name in violation of 42 PA. CON. STAT. § 8316 (2003); (2) invasion of privacy by misappropriation of identity; (3) misappropriation of publicity; (4) identity theft; (5) conversion; (6) tortious interference with contract; (7) civil conspiracy; and (8) civil aiding and abetting. *See id.*

26 *See id*. at *1.

27 In 2010, Edcomm was bought out by SISCOM, which employed the individual defendants to this suit. *See id.* at *1.

28 *Id*. at *1.

29 *Id*. at *2.

30 *Id*. at *9. The district court did, however, deny the defendants' motion for summary judgment for Eagle's state law claims. The parties went to trial on October 16, 2012. *See id.* On March 12, 2013, the district court issued its decision, finding the results of the

court stated Eagle failed to present "legally cognizable loss or damages" to sustain her CFAA claim[31] and also failed to provide sufficient evidence of a lack of confusion to corroborate her Lanham Act claim.[32]

In contrast to the first two cases, *Ardis Health LLC v. Nankivell* is an example of what can be considered a more straightforward SMA dispute—the former employee never changed the account information, never attempted to use the SMAs after termination, and the employer had a written agreement in place.[33] Ashleigh Nankivell was hired as a Video and Social Media producer by two herbal and beauty product companies owned by the same founder, Jordan Finger. Her responsibilities included maintaining the usernames, passwords, and login information to the company's SMAs and other third party server accounts.[34] After Nankivell was terminated, she refused to return the account's access information, and the employer sued on the basis of a work-for-hire agreement "within the meaning of the Copyright Act of 1976."[35] In its motion for a preliminary injunction to return the access information, the district court stated that employers "own[ed] the rights to the Access Information,"[36] and would suffer irreparable harm as a result of Nankivell's refusal to return the access information.[37]

The above cases demonstrate the difficulty in fitting social media accounts into existing intellectual property regimes—with courts entertaining the possibility that an SMA may fall within trade secrets law,[38] may be protected by trademark law,[39] or may

case "a somewhat mixed bag for both sides." *See* Eagle v. Morgan, No. 11-4303, slip op. at *17 (E.D. Pa. Mar. 12, 2013). Despite the wins and losses on the claims for both parties, the court ultimately ruled that Eagle failed to provide sufficient evidence in support of compensatory and punitive damages. *See id.*

31 *Id.* at *3.

32 *Id.* at *8.

33 Ardis Health, LLC v. Nankivell, No. 11 Civ. 5013(NRB), 2011 WL 4965172, at *1 (S.D.N.Y. Oct 19, 2011).

34 *Id.* at *2.

35 *See id.* at *1.

36 *Id.* at *3.

37 *Id.*

38 *See, e.g.*, PhoneDog v. Kravtiz, No. C 11 03474 MEJ, 2011 WL5415612 (N.D. Cal. Nov. 8, 2011) (finding an employer sufficiently alleged a misappropriation of trade

simply fall outside intellectual property law altogether.[40] Thus far in the development of appropriate legal regimes to tackle social media issues broadly, it is clear that, as far as ownership rights are concerned, courts have struggled to fit SMAs into existing intellectual property regimes.

Moreover, these cases reiterate the specific assets of value associated with an SMA. For example, in *PhoneDog*, the employer primarily valued the followers ("subscribers"), whereas in *Eagle*, the employee was suing over the interactive platform of her LinkedIn account, and in *Ardis Health*, the employers specifically sought the username and password ("access information"). Despite the varying focuses of the cases, in at least at one point in litigation, the parties demonstrated an interest in all three assets of an SMA: (1) the subscribers; (2) the interactive platform/content; and (3) the access information. As such, and given the variety of social media networks (i.e., Facebook and Twitter accounts), this Note will focus the analysis of ownership rights over social media accounts based on a "generic SMA" embodying these three main assets.

C. Relevant Intellectual Property Regimes

Intellectual property law is commonly viewed as a means of protection for owners of creative works—securing for the owner the returns on their creative labor. For many, the security of this protection is what is believed to incentivize individuals and businesses to create. For copyright and patent law, this right stems from Article I, Section 8 of the United States Constitution, which

secrets claim over a Twitter account); Christou v. Beatport, LLC, 849 F. Supp. 2d 1055, 1074–77 (D. Colo. 2012) (finding an employer sufficiently alleged a misappropriation of trade secrets claim over a MySpace account).

[39] *See, e.g.*, Maremont v. Susan Fredman Design Grp., Ltd., No. 10-C7811, 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011) (denying a summary judgment motion against an employee's Lanham Act claim over the use of a Twitter and Facebook account); *cf.* Eagle v. Morgan, No. 11-4303, 2012 WL 4739436 (E.D. Pa. Oct. 4, 2012) (granting a motion to dismiss an employee's Lanham Act claim for failing to provide sufficient evidence of a likelihood of confusion over a LinkedIn account).

[40] *See, e.g.*, Ardis Health, 2011 WL 4965172. And arguably all the cases mentioned in this section, given their lack of a concrete decision, contribute to this conclusion. *See* sources cited *supra* notes 38–39.

serves "[t]o promote the Progress of Science and useful Arts, [secures] for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[41] Trademark law, through the Lanham Act, offers protection against unfair competition[42] and "secur[es] to a mark's owner the goodwill of his business."[43] Although not a federal intellectual property regime, trade secrets law, most recognized as an adopted form of the Uniform Trade Secrets Act,[44] protects the owner of a secret, or at least not generally known discovery or work, from unlawful disclosure or use.[45] With this broad backdrop of intellectual property law—which serves to incentivize creativity by protecting the exclusive ownership rights to a work—this section will provide a basic background of the intellectual property regimes relevant to SMAs, beginning with trademark law, followed by copyright law, and ending with trade secrets law.

1. Trademark Law

The statutory definition of a trademark includes "any word, name, symbol, or device, or any combination thereof . . . to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown."[46] Trademark infringement claims are generally brought under Lanham Act § 43(a), which governs false designations of origin, false descriptions, and dilution. A claim under section 43(a) requires the plaintiff to satisfy two elements: (1) that the mark is protectable and (2) that there is a likelihood of consumer confusion.[47] For the purposes of this Note, it will be assumed that the employer holds a protectable trademark insomuch as it satisfies

41 U.S. CONST. art I, § 8, cl. 8.

42 Trademark Act of 1946 (Lanham Act), ch. 540, 50 Stat. 427 (codified as amended in scattered sections of 15 U.S.C.).

43 *See* Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 763 (1992).

44 UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005).

45 *See* Kewanee Oil Co., v. Bicron Corp, 416 U.S. 470, 475 (1974).

46 15 U.S.C. § 1127 (2006).

47 *See* Nasdaq Stock Mkt., Inc. v. Archipelago Holdings, LLC, 336 F. Supp. 2d 294, 304 (S.D.N.Y. 2004).

the first element of section 43(a).[48] Therefore, as demonstrated in *Eagle v. Morgan*, the relevant issue is whether the continued use of a social media account by a former employee leads to a likelihood of consumer confusion.[49]

A likelihood of consumer confusion is "[t]he core element of trademark infringement."[50] Consumer confusion exists so long as the public "belie[ves] that the mark's owner sponsored or otherwise approved the use of the trademark."[51] The analysis involves a multi-factor balancing test, with different courts applying their own version of the test.[52] Factors that are usually considered include: (1) the strength of the mark; (2) similarity between the marks; (3) similarity between the products or services offered; (4) actual confusion; (5) the defendant's intent; (6) consumer care and sophistication; (7) likelihood of expanding products or services offered; and (8) marketing channels used.[53] Despite the difference in factors considered, the circuit courts all view the analysis as a fact-specific inquiry where no one factor

---

[48] To delve into whether a business's trademark is protectable would digress from the purpose of this Note. For example, PhoneDog is a registered trademark with the PTO. *See* PHONEDOG, Registration No. 3,828,071.

[49] *See* Eagle v. Morgan, No. 11-4303, 2012 WL 4739436 (E.D. Pa. Oct. 4, 2012). Although the court found the employee failed to prove her Lanham act claim, the facts of that case differ slightly than this scenario because Eagle did not continue to use the LinkedIn account after her termination. *Id.* at *1.

[50] Brookfield Commc'n, Inc. v. West Coast Entm't Corp., 174 F.3d 1036, 1053 (9th Cir. 1999) (quoting Official Airline Guides, Inc. v. Goss, 6 F.3d 1385, 1391 (9th cir. 1993)).

[51] Star Indus. v. Bacardi & Co., 412 F.3d 373, 384 (2d Cir. 2005) (quoting Dallas Cowboys Cheerleaders, Inc. v. Pussycat Cinema, Ltd., 604 F.2d 200, 204–05 (2d Cir. 1979).

[52] *See* 4 MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 23:19 (4th ed. 2013).

[53] *See e.g.*, Interactive Prods. Corp. v. a2z Mobile Office Solutions, Inc., 326 F.3d 687 (6th Cir. 2003); AMF Inc. v. Sleekcraft Boats, 599 F.2d 341 (9th Cir. 1979). Some circuits apply slightly different factors. For example, the Second Circuit "*Polaroid*" test does not include "marketing channels used" as a separate factor, but rather incorporates the use of marking channels under its "proximity" factor; and instead, includes a separate factor of "quality of defendant's products or services." *See* Polaroid Corp. v. Polarad Elecs. Corp., 287 F.2d 492 (2d Cir. 1961) *cert denied*, 368 U.S. 820 (1961); *see also* 4 MCCARTHY, *supra* note 52, § 23:19.

necessarily weighs more than another,[54] and where the burden of proving a likelihood of confusion belongs to the plaintiff.[55]

There is a spectrum of scenarios to which the continued use of an SMA may lead to consumer confusion. At one end, the former employee retains the account and does not change the name or any other aspect of the account. At the opposite end of the spectrum, the former employee has changed the name so that it no longer includes the protected mark. In the grey area between these poles exist situations when the former employee changes the name of the account but the new name may be reminiscent of the original name. Regardless of where the facts fall on this spectrum, a court would still apply a likelihood of confusion analysis.

2. Copyright Law

The Copyright Act protects "original works of authorship,"[56] where "originality requires independent creation plus a modicum of creativity."[57] In order for a social media account to receive protection under the Copyright Act, the "work" must be original—"[t]he sine qua non of copyright is originality"[58]—and the work must be "fixed in any tangible medium of expression."[59] Three possible ways to view the "work" of an SMA include: (1) the work in terms of each individual post, (2) the SMA as a compilation, or (3) the SMA as a work-for-hire. The following section will briefly explain only the first requirement—originality—as it is the more controversial issue, and the issue of fixation will not be addressed since it is unlikely to be disputed.[60]

---

54 *Star Indus.*, 412 F.3d at 384 ("Our analysis is not mechanical, but rather, focuses on the ultimate question of whether, looking at the products in their totality, consumers are likely to be confused."); *Brookfield*, 174 F.3d at 1054 ("[T]he relative importance of each individual factor will be case-specific.").

55 *See* KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc., 543 U.S. 111, 17–18 (2004).

56 17 U.S.C. § 102(a) (2006).

57 Feist Publ'ns, Inc., v. Rural Tel. Servs. Co., 499 U.S. 340, 346 (1991).

58 *Id.* at 345.

59 17 U.S.C. § 102(a).

60 Fixation requires a work to be "fixed in a tangible medium of expression when its embodiment in a copy . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." 17 U.S.C. § 101 (2006). Generally, courts apply the fixation requirement broadly. *See*

a) Originality

As stated above, "[t]he sine qua non of copyright is originality," and the "work must be original to the author."[61] For a work to be considered original, it must be independently created by the author and, most significantly, "posse[ss] at least some minimal degree of creativity."[62] Originality does not require novelty; in fact, "the requisite level of creativity is extremely low."[63] The range of works found to be original span from an opening sentence of a poem[64] to sculptures[65] to computer programs.[66] One fundamental aspect of copyright law is that "no one may claim originality as to facts."[67] A key factor in determining whether an SMA's individual posts or the whole compilation of posts are protected by copyright is if either possesses the requisite originality.

b) Work-Made-For-Hire

The Copyright Act states that ownership of the copyright "vests initially in the author or authors of the work."[68] An exception exists for "works made for hire," where "the employer or other person for whom the work is prepared is considered the author."[69] Under the Copyright Act, there are two mutually

Williams Elecs, Inc. v. Artic Int'l, Inc., 685 F.2d 870, 877 (3d Cir. 1982) ("By its broad language, Congress opted for an expansive interpretation of the term[] 'fixation'. . . ."). An SMA, similar to video games and computer programs which have been established as "fixed," is most likely also sufficiently permanent or stable to permit it to be perceived, particularly where the SMA is stored in the social media platform's server and posts remain on account pages of the owners and subscribers. *See Williams Elec.*, 685 F.2d at 874–75; Stern Elec., Inc. v. Kaufman, 669 F.2d 852, 855 (2d Cir. 1982) (both finding storage in memory devices satisfies the fixation requirement).

61 *Feist*, 499 U.S. at 345.

62 *Id.*

63 *Id.*

64 *See* Stern v. Does, No. CV 09—01986 DMG (PLAx), 2011 WL 997230, (C.D. Cal. Feb. 10, 2011), *aff'd* No. 11-55436, 2013 WL 1137390 (9th Cir. Mar. 20, 2013).

65 *See* Cmty. for Creative Non-Violence v. Reid (*CCNV*), 490 U.S. 730, 731 (1989).

66 *See* Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240 (3d Cir. 1983), *cert. denied*, 464 U.S. 1033 (1984).

67 *Feist*, 499 U.S. at 437 (quoting 1 NIMMER & D. NIMMER, Copyright §§ 2.01[A], [B] (1990)).

68 17 U.S.C. § 201(a) (2006).

69 17 U.S.C. § 201(b).

exclusive ways in which a work may be considered a work-made-for-hire: (1) as a work "prepared by an employee within the scope of his or her employment,"[70] or (2) as a "specially ordered or commissioned" work, as specified in a written instrument, by an independent contractor.[71] The Act enumerates the nine categories of "specially ordered or commissioned" works that qualify as works-made-for-hire:

> (1) As a contribution to a collective work,
> (2) As a part of a motion picture or other audiovisual work,
> (3) As an translation,
> (4) As a supplementary work (a work prepared for publication as a secondary adjunct to a work by another author for the purpose of introducing, concluding, illustrating, explaining, revising, commenting upon, or assisting in the use of the other work),
> (5) As a compilation,
> (6) As an instructional text,
> (7) As a test,
> (8) As answer material for a test, or
> (9) As an atlas.[72]

Given the two prongs of the work-made-for-hire provision, the threshold issue is whether the individual hired to manage the SMA qualifies as an employee or rather as an independent contractor.[73] With an employee, the ownership of the copyright would belong to the company. With an independent contractor, the ownership of the copyright would belong to the hired party if it does not fall within one of the nine categories of "specially ordered or commissioned" works. The statute does not provide a definition of employee; however, the Supreme Court has held that "the term 'employee' should be understood in light of the general common law of agency."[74] To determine whether a hired party is an

---

70 17 U.S.C. § 101(1) (2006).
71 *See* 17 U.S.C. § 101(2); *see also CCNV*, 490 U.S. 730, 731 (1989).
72 *See* 17 U.S.C. § 101(2).
73 *See CCNV*, 490 U.S. at 751.
74 *Id*. at 741.

employee as opposed to an independent contractor, courts look to various factors to determine how much control the hiring party possesses and the "means by which the product is accomplished."[75]

The work-made-for-hire analysis presents another possible framework for determining ownership rights to an SMA.[76] When a business hires an individual to create or manage the SMA, the hired party is generally responsible for posts, often in connection with a company's marketing objectives,[77] maintaining any usernames and passwords,[78] and, in some situations, a hired party is also given a company laptop or computer to work from.[79] As exemplified by *PhoneDog*, the relationship between the company and hired party is not always clearly defined in a written agreement.[80] And, even when there is an agreement in place, ownership of any account may still be disputed.[81] Regardless, the analysis turns on whether the hired party is an employee or independent contractor.

3. Trade Secrets Law

Trade secrets law is a common law intellectual property regime. The Uniform Law Commission published the Uniform Trade Secrets Act ("UTSA") with the intention of unifying this body of law amongst the states. So far, forty-six states have adopted the UTSA. For the purposes of this Note, the discussion

---

[75] *Id.* at 751. A court will also consider (1) the skill required; (2) the source of the instrumentalities and tools; (3) the location of the work; (4) the duration of the relationship between the parties; (5) whether the hiring party has the right to assign additional projects to the hired party; (6) the extent of the hired party's discretion over when and how long to work; (7) the method of payment; (8) the hired party's role in hiring and paying assistants; (9) whether the work is part of the regular business of the hiring party; (10) whether the hiring party is in business; (11) the provision of employees benefits; (12) and the tax treatment of the hired party. None of these factors are dispositive. *Id.* at 751–52.

[76] *See id*. at 750 (stating Congress' goal behind the work-made-for-hire provision was to "ensur[e] predictability through advance planning").

[77] *See, e.g.*, Ardis Health, LLC v. Nankivell, No. 11 Civ. 5013(NRB), 2011 WL 4965172, at *1 (S.D.N.Y. Oct 19, 2011).

[78] *See, e.g.*, *id*.

[79] *See, e.g.*, *id.*

[80] *See, e.g.*, PhoneDog v. Kravitz, No. C 11 03474 MEJ, 2011 WL5415612 (N.D. Cal. Nov. 8, 2011).

[81] *See, e.g.*, *Ardis Health*, 2011 WL 4965172.

will refer to the language in the UTSA rather than any state-specific version of the act. The key elements of a trade secret can be broke down as:

> (1) "information, including a formula, pattern, compilation, program device, method, technique or process, that:
> (2) derives independent economic value, actual or potential,
> (3) from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> (4) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[82]

Classic examples of trade secrets include formulas (i.e., Coca-Cola's beverage formula),[83] customer lists,[84] sales or marketing information and other forms of confidential information.[85] The trade secret holder is protected "against the disclosure or unauthorized use of the trade secret."[86] As a corollary, the trade secret is not protected from "discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering."[87] The value of trade secret protection is the preservation of the discovery and its commercial advantages exclusively to the benefit of the inventor, while sanctioning "the competitor who by unfair means, or as the beneficiary of a broke

---

82 UNIFORM TRADE SECRETS ACT § 1(4) (1985).

83 *See* William Lee Adams, *Is This the Real Thing? Coca-Cola's Secret Formula 'Discovered,'* TIME (Feb. 15, 2011), http://newsfeed.time.com/2011/02/15/is-this-the-real-thing-coca-colas-secret-formula-discovered.

84 *See, e.g.*, Suzanne Kapner, *BofA Sues Ex-Employees Over 'Trade Secrets,'* FT.COM (Dec. 9, 2010, 9:40 PM), http://www.ft.com/intl/cms/s/0/626b961c-03d6-11e0-8c3f-00144feabdc0.html#axzz2OTyRiDUZ.

85 *See, e.g.*, Azam Ahmed, *Ex-Citadel Employee Charged with Stealing Trade Secrets*, N.Y. TIMES (Oct. 13, 2011, 5:03 PM), http://dealbook.nytimes.com/2011/10/13/ex-citadel-employee-charged-with-stealing-trade-secrets.

86 Kewanee Oil Co., v. Bicron Corp., 416 U.S. 470, 475–76 (1974).

87 *Id.* at 477.

faith, obtains the desired knowledge without himself paying the price in labor, money, or machines expended by the discover."[88]

As evidenced in *PhoneDog*, a business may allege trade secret claims for the misappropriation of the access information and subscribers of its social media account. The threshold issue is the existence of a trade secret—whether or not the access information or the subscriber list constitute trade secrets.

4. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") is the primary piece of legislation concerning computer fraud violations. The CFAA was enacted in 1986, when Congress sought to address rising concerns of computer-related crimes.[89] More specifically, Congress created the statute in response to the threat of "hackers" gaining access to highly private information belonging to the government and financial institutions.[90] According to the legislative history, Congress viewed the statute as "doing for computers what trespass and burglary laws did for real property."[91] Although the CFAA began as a criminal statute, Congress included in its 1994 amendments a private civil cause of action, codified at 18 U.S.C. § 1030(g).[92] Over the years, Congress has recognized the evolution of computers and computer use and amended the statute accordingly.[93] Not only did Congress expand the statute to include the private right of action, it also broadened the scope of targeted computers from "federal interest computers" to all "protected computers,"[94] and removed the requirement that

---

88 *Id*. at 482 (quoting A. O. Smith Corp. v. Petroleum Iron Works Co., 73 F.2d 531, 539 (6th Cir. 1934).

89 *See* Shawn E. Tuma, *"What Does CFAA Mean And Why Should I Care?"—A Primer On The Computer Fraud And Abuse Act For Civil Litigators*, 63 S.C. L. REV. 141, 155–56 (2011).

90 Matthew Kapitanyan, *Beyond Wargames: How the Computer Fraud and Abuse Act Should be Interpreted in the Employment Context*, 7 I/S: J. L. & POL'Y FOR INFO. SOC'Y 405, 410 (2012).

91 *Id.*

92 *See* Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, J. Marshall Rev. Intell. Prop. L. 155, 160 (2008).

93 Kapitanyan, *supra* note 90, at 415.

94 *Id.*

information under section 1030(g), subsection (a)(2)(C) involve interstate or foreign communication.[95]

While the majority of CFAA claims remain directed at "classic hacking activities,"[96] there has been a steep increase in civil claims. "Employers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."[97] As such, section 1030(g) civil claims present a ripe framework for determining SMA ownership.

A civil action may be asserted under section 1030(g) so long as it involves any of the seven violations under section 1030(a) and at least one of the five elements under section 1030(c)(4)(A)(i) ("the Cause subsection").[98] The most common element claimed under the Cause subsection is subsection (c)(4)(A)(i)(I) ("the $5,000 loss element"), which requires that one or more persons suffered at least $5,000 in losses during any one-year period.[99] The subsections that speak to the issue of an employer-employee dispute over SMA ownership consist of section 1030(a)(2)(C)[100] ("the Intentional Access subsection") and section 1030(a)(4) ("the Intent to Defraud subsection").[101]

To better understand the applicability of the CFAA to SMAs, this section will outline the pertinent elements facing a CFAA claim over an SMA: (1) the definition of a "computer," (2) the scope of "authorization," and (3) "loss."

---

95 This clause was omitted in September 2008 under the Identity Theft Enforcement and Restitution Act. *See* Pub. L. 110-326, § 203, 112 Stat. 3560, 3561 (2008).

96 P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504, 510 (3d Cir. 2005).

97 *Id.* (quoting Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003)).

98 18 U.S.C. § 1030(g) (2006).

99 18 U.S.C. § 1030(c)(4)(A)(i)(I) ("loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value"); *See* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 435 (2009).

100 18 U.S.C. § 1030(a)(2)(C).

101 18 U.S.C. § 1030(a)(4).

a) Definition of a "Computer"

The CFAA defines a "computer" as

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;[102]

and the relevant definition of a "protected computer" as

> a computer which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[103]

Courts have found that a cell phone,[104] game console,[105] and website[106] all qualify as a "computer" under the CFAA. In fact, some commentators have stated that effectively any computer connected to the Internet is a "computer" under the CFAA.[107]

In an SMA ownership dispute between an employer and employee, there are two possible "computers" at issue: the first being the social media website and the second being the actual SMA. As mentioned, courts recognize websites as "computers" under the CFAA, due to the fact that in order for a website to access the Internet, it must access its host server.[108] Applying this

---

[102] 18 U.S.C. § 1030(e)(1).

[103] 18 U.S.C. § 1030(e)(2)(B).

[104] *See* United States v. Kramer, 631 F.3d 900, 904 (8th Cir. 2011).

[105] *See* Sony Computer Entm't Am. LLC v. Hotz, No. CV 110167, 2011 WL 347137, at *1 (N.D. Cal. Jan. 27, 2011).

[106] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001); United States v. Drew, 259 F.R.D. 449, 456–57 (C.D. Cal. 2009).

[107] Brenton, *supra* note 99, at 433; Tuma, *supra* note 89, at 168–71; Liccardi, *supra* note 92, at 60.

[108] *Drew*, 259 F.R.D. at 456–57 (reasoning that for a website to access the Internet, it must access a server hosting the website).

reasoning to an individual SMA suggests that it is also a "computer." The entirety of an SMA, including the content posted, login information, messages, and photos, is also stored within servers.[109] And, given the social media website's and an SMA's connection to the Internet, it would follow that each would also be a "protected computer" under the CFAA. Lastly, and perhaps more important to CFAA protection, any individual harmed by the unlawful access of a protected computer has standing to sue—not limited the owner of the computer.[110]

b) Scope of "Authorization"

A major issue in both (a)(2)(C) and (a)(4) claims is the phrase "without authorization, or exceeds authorized access."[111] The scope of the phrase is probably the most litigated issue in CFAA cases.[112] Despite the fact that the statute explicitly defines "exceeds authorized access,"[113] the courts are split as to how and when access becomes unauthorized in an employment context.[114]

The Seventh Circuit, in *International Airports Centers, LLC v. Citrin*, established an agency-based view of the statute, where an employee breaches her duty of loyalty to the employer when she accesses the employer's computer and uses the information obtained in a manner adverse to the employer's economic interest.[115] In breaching her duty of loyalty, she terminates her agency relationship with the employer such that she no longer has

---

109 *See* Steven J. Vaughan-Nichols, *How Social Networking Works*, ITWORLD (Jan. 7, 2010, 12:54 PM), http://www.itworld.com/software/91803/how-social-networking-works.

110 See Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir. 2004) (reversing the district courts reading of an "ownership or control requirement into the Act," on grounds that the language of the Act clearly permits a civil remedy to "[*a*]*ny* person").

111 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4).

112 *See* Tuma, *supra* note 89, at 171.

113 18 U.S.C § 1030(e)(6). "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.*

114 *Compare* United States v. Nosal (*Nosal II*), 676 F.3d 854 (9th Cir. 2012) (en banc), *with* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

115 *Citrin*, 440 F.3d at 420.

the authorization that might otherwise have existed.[116] Thus, under the *Citrin* standard, an employee is "unauthorized" when she never had authorization to begin with, as well as when she accesses the computer in a way that contradicts the employer's interest.[117]

However, the Ninth Circuit has declined to read an agency-based theory into the scope of authorization.[118] Instead, it has embarked on a more literal application. Beginning with *LVRC Holdings LLC v. Brekka*, the Ninth Circuit narrowly construed "authorization," such that when an employee is given permission to access the employer's computer, *any* subsequent permitted use of the computer is considered "authorized," regardless of its wrongfulness.[119] More recently, the Ninth Circuit upheld the *Brekka* application of "without authorization," but toyed with the scope of "exceeds authorized access."[120] After hearing the case en banc, the court similarly adhered to a more technical understanding of "authorization," holding that an employee only "exceeds authorized access" when she is given permission to access certain information on a computer but then accesses information beyond that which she is permitted to access, and not when she misuses the information.[121]

The premise of this circuit split appears to be based on a fine line between "improper access of computer information" versus "misuse or misappropriation."[122] Essentially, under an agency-based theory, an employee is unauthorized to access a protected computer when she does so in violation of the employer's interest. Under the Ninth Circuit's more narrow interpretation, an employee is unauthorized when she never had permission to access the

---

116 *Id*. at 420–21.

117 *See id.* at 420 (deciding agency law defined "authorization"); *see also* RESTATEMENT (SECOND) OF AGENCY § 112 (1958) ("[T]he authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.").

118 United States v. Nosal, 642 F.3d 781, 786 (9th Cir. 2011), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012).

119 LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (clarifying that "without authorization" means "without any permission at all").

120 *See Nosal II*, 676 F.3d 854.

121 *See id.* at 857.

122 *See id.* at 863.

computer to begin with or when she is authorized to access the computer but accesses information that she was not permitted to access, regardless of how she subsequently uses the information.

c) Definition of "Loss"

The CFAA defines "loss" as

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of the interruption of service.[123]

This definition of "loss" can be described as two types of losses: response costs and interruption of service damages.[124] Reasonable response costs may include expenses towards discovering the identity of the offender, assessing the damage to a hacked system, and upgrading security.[125] Interruption of service damages may include loss of revenue, but only if the loss results directly from the unauthorized access itself.[126] On the other hand, claims for "lost business opportunities, damaged reputation, loss of assets, and other missed revenue," usually do not constitute "loss."[127] Given the narrow scope of eligible "losses,"[128] this element may pose the greatest challenge for companies claiming ownership of an SMA under the CFAA.

---

123 18 U.S.C. § 1030(e)(11) (2006).

124 "[T]he term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11); s*ee also* Tuma, *supra* note 89, at 185.

125 *See* AtPac, Inc. v. Aptitude Solutions, Inc., 730 F. Supp. 2d 1174, 1184 (E.D. Cal. 2010); *see also* Tuma, *supra* note 89, at 187.

126 *See AtPac*, 730 F.Supp.2d at 1184–85.

127 Eagle v. Morgan, No. 11-4303, 2012 WL 4739436, at *7 (E.D. Pa. Oct. 4, 2012).

128 *See AtPac*, 730 F.Supp.2d at 1185.

II. INTELLECTUAL PROPERTY LAWS FAIL TO ESTABLISH OWNERSHIP RIGHTS TO SOCIAL MEDIA ACCOUNTS

The rise in litigation over the ownership of SMAs presents new challenges to the scope and relevance of intellectual property laws, namely Trademark, Copyright, and Trade Secrets. An analysis of how the three intellectual property regimes would apply to the issue of ownership further highlights the challenges and limitations of intellectual property as the governing body of law over SMAs. This section will first highlight the practical inadequacies of using Trademark, Copyright, and Trade Secrets to determine ownership rights to an SMA. Then, this section will discuss the theoretical underpinnings of why SMAs are unsuitable for intellectual property protection.

A. Intellectual Property Laws as Applied to Social Media Accounts: Failure to Protect Key Assets

The key assets of an SMA consist of the access information, the subscribers, and the content.[129] Ownership of an SMA allows one to, exclusively, reap the benefits that flow from these assets. This section will go through the relevant application of each intellectual property regime to this issue of SMA ownership—revealing how intellectual property laws only provide partial ownership rights.

1. Trademark

The value of a trademark stems from the association between the mark and the product or service, "to secure to the owner of the mark the goodwill of his business and to protect the ability of consumers to distinguish among competing producers."[130] Many businesses incorporate their protected marks in an SMA's account name, functioning as a way to notify subscribers that that particular SMA is associated with that particular business. When individuals that are hired to manage these SMAs on behalf of the company leave the company and continue to operate the SMAs, there are two possible scenarios for a trademark claim: (1) the former

---

129 *See supra* Part I.B.

130 Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 774 (1992).

employee keeps the same account name, or (2) the former employee changes the account name.[131] In both instances, whether or not there is a trademark infringement would depend on the likelihood of confusion.[132]

a) Likelihood of Confusion

The main factors at issue would most likely be the similarity between the two names and the similarity between the services offered. With regard to the similarity between the names, courts "analyze the mark[s'] overall impression on a consumer, considering the context in which the marks are displayed and the totality of the factors that could cause confusion."[133] As such, if the former employee changes the name so that the SMA no longer incorporates the company's mark, or only retains a portion of the company's mark, then it would be more difficult for the company to establish sufficient similarity between the two names.[134]

With regard to the similarity of the services, courts look to "the nature of the services and the structure of the relevant market and include[] consideration of the 'class of consumers to whom the goods are sold.'"[135] If the employee was hired specifically to promote the company's products or services, and after the name change continues to post content referencing the company's products or services, then this factor would likely weigh in favor of finding a likelihood of confusion. This would be further substantiated by the high probability that the audience—the

131 *See supra* Part I.B.

132 *See id.*

133 *New York City Triathlon, LLC v. NYC Triathlon Club, Inc.*, 704 F. Supp. 2d 305, 316–17 (S.D.N.Y. 2010).

134 For example, if an SMA name was originally "PhoneDog_Noah" and changed to "PhoneReviewer_Noah," it would be more difficult for the company to demonstrate a likelihood of confusion based on similarity of marks. *See Everest Capital Ltd. v. Everest Funds Mgmt, LLC*, 393 F.3d 755, 761 (8th Cir. 2005) (finding that the use of a dominant word that is part of the protected product name insufficiently similar). Not to mention, PhoneDog did not even assert a Lanham Act claim for Kravtiz' use of the account. *See* PhoneDog v. Kravtiz, No. C 11 03474 MEJ, 2011 WL5415612 (N.D. Cal. Nov. 8, 2011). Conversely, *Eagle v. Morgan* serves as an example of when a plaintiff attempted to assert a Lanham Act claim after the account name was changed, and the court ruled otherwise. *See* Eagle v. Morgan, No. 11-4303, 2012 WL 4739436 (E.D. Pa. Oct. 4, 2012).

135 *New York City Triathlon*, 704 F. Supp. 2d at 317.

subscribers—would be predominantly the same as before the change.[136] Additionally, if the name change is slight, the similar use could suggest the former employee's intention to benefit from the protected mark's good will.[137] Nonetheless, although the subscribers may be effectively the same, a court may find that this particular class of consumers, the social media subscribers, are arguably savvy enough to know that the name change signifies the termination of a relationship between the poster and the company, or at least savvy enough to question if there still exists an association between the two.[138] Whether and how the former employee changes the account name and subsequently uses the account greatly affects the availability of trademark protection.

b) Limitations

The strength of a trademark claim depends on the likelihood of confusion as to the association between the SMA and its owner, primarily through the name of the account. This, however, fails to fully address the issue of who owns the SMA, because the focus of the analysis is not on whom the account belongs to, but rather turns on who has the ability to change the name of the account—regardless of whether or not that access is proper.[139] Moreover, trademark law does not directly address any of the main assets of an SMA. There is no infringement claim available over the ownership of the content posted, the subscribers, nor the access information. Instead, trademark law only governs the ownership rights to use the mark, not the account. If anything, ownership of a mark might undermine ownership of an SMA, at least where the employee completely changes the name and use of an SMA. Given that the key requirement is a protectable mark, the protection afforded by trademark law goes to the owner of that

136 *Id.* (finding a likelihood of confusion where both parties marketed to and serviced the same individuals and organizations).

137 *See* Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 778 n.4 (1992).

138 *See* Yellobrix, Inc. v. Yellobrick Solutions, Inc., 181 F. Supp. 2d 575, 581n.3 (E.D. N.C. 2011) (weighing the sophistication of technologically-savvy consumers towards finding an unlikelihood of confusion).

139 *See, e.g.*, *Eagle*, 2012 WL 4739436, at *2 (denying a Lanham Act claim where the defendant knew the plaintiff's password to her LinkedIn account and changed the accounts name and photo).

mark,[140] and where trademark law fails is in trying to translate that ownership right to that over an entire SMA.

2. Copyright

The Copyright Act protects "original works of authorship,"[141] vesting in the owner of the work six exclusive rights, including the right to reproduce the work, prepare derivative works, and display the work publically.[142] The Act also lists what categories of works are eligible for copyright protection.[143] In terms of SMAs, copyright law may apply to each of the individual posts[144] and to the SMA as a compilation.[145] If either the posts or compilation are copyrightable, then ownership may be established under the work-made-for-hire provision.[146]

a) Individual Posts

The content of each individual post may warrant copyright protection. Individual posts, however, vary in length, subject-matter, and style, creating a unique challenge to its copyright analysis.[147] In terms of length, most posts via an SMA are relatively short and may be limited to a specific number of characters,[148] or inherently limited by the very purpose of the

---

[140] *See* Nasdaq Stock Mkt, Inc. v. Archipelago Holdings, LLC, 336 F. Supp. 2d 294, 304 (S.D.N.Y. 2004).

[141] 17 U.S.C. § 102(a) (2006).

[142] 17 U.S.C. § 106 (2006).

[143] 17 U.S.C. § 102(1)–(8).

[144] Individual posts may qualify as literary works. The Copyright Act defines literary works as

> works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, pamphlets, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied.

17 U.S.C. § 101 (2006).

[145] *See* 17 U.S.C. § 103 (2006).

[146] *See* 17 U.S.C. § 101 (2006).

[147] *See generally, e.g.*, Adam S. Nelson, *Tweet Me Fairly: Finding Attribution Rights Through Fair Use in the Twittersphere*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 697, 728 (2012) ("Without empirical evidence, there is no way to estimate what percentage of tweets might be protectable.").

[148] For example, Twitter limits each tweet to 140 characters.

post—to convey an instant, temporary message. Similarly, the actual content of the post may range from anecdotal, such as a particular experience at a certain venue, to informative, such as notification of a promotional deal. Courts generally adhere to the idea that there is a reciprocal relationship between creativity and independent effort, where the "smaller the effort the greater must be the degree of creativity."[149] This is not to say that short sentences or simple phrases cannot be copyrighted. "[T]he copyrightability of a very short textual work—be it word, phrase, sentence or stanza—depends on the presence of creativity."[150]

The purpose of the post helps elucidate its creativity, or lack thereof. A concrete tenet of copyright is that where the "expression of [the] idea is indistinguishable from the idea itself, it is not entitled to copyright protection.[151] A post that aligns with a "form[] of expression dictated solely at functional considerations," will most likely be found to "display[] no creativity whatsoever."[152] In the case of the SMAs at issue, this poses the main challenge. If the individual post merely notifies the subscribers of promotional deals, the argument for originality is undermined by the post's primary purpose—a business function. However, if the posts are more substantive or anecdotal, like an in-depth product review, they would more likely warrant copyright protection. Although most SMA posts for business purposes may generally lack sufficient creativity, the ultimate determination still depends on the specific facts of each case.

b) As a Compilation

Given the legal and practical limitations to the copyright protection of individual posts, businesses may consider protecting their entire social media account as a compilation.[153] The

[149] Stern v. Does, No. CV 09—01986 DMG (PLAx), 2011 WL 997230, (C.D. Cal. Feb. 10, 2011) (citing Universal Athletic Sales Co. v. Salkeld, 511. F.2d 904, 908 (3d Cir. 1975)).

[150] *Id.* at *6.

[151] Feist Publ'ns, Inc., v. Rural Tel. Servs. Co., 499 U.S. 340, 347 (1991) ("This is because facts do not owe their origin to an act of authorship.").

[152] *Stern*, 2011 WL 997230 at *6 (finding a twenty-three word listserv post asking if anyone had a bad experience with the defendant's services, lacked sufficient originality).

[153] 17 U.S.C. § 103 (2006).

Copyright Act defines a compilation as a "work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."[154] Compilations may consist of material that is not within the subject matter of copyright, i.e. individual posts that serve a functional purpose.[155] Even so, compilations must satisfy the statutory requirement of originality.[156] The key to copyright protection for a compilation work is the selection, coordination, or arrangement of the preexisting material.[157]

Compilations are considered original when an author independently chooses the selection and arrangement of the material in a manner that reflects some creativity.[158] Copyright protection for the compilation as a whole, however, does not bleed into the individual elements that are compiled.[159] In the case of social media accounts, the ability to select and arrange the elements of the page is not within the owner's control—that control is exercised by the social media website.[160] The location of where the posts are displayed for an account, where the name of the account is displayed, and where the subscriber may connect with the account, is the same for each social media account for that particular platform.[161] Although copyright protection may be available to compilations that consist of material like that of the posts on an SMA,[162] the very fact that the arrangement of how the information is communicated to the subscribers is within the control of the social media platform undermines finding copyright

---

154 *See* 17 U.S.C. § 101 (2006).

155 *See supra* Part II.A.2.a.

156 *See* 17 U.S.C. § 103 (2006).

157 *See* 17 U.S.C. § 103.

158 *See Feist*, 499 U.S. at 345.

159 *See id.*

160 *See, e.g.*, Somini Sengupta, *Facebook Shows Off New Home Page Design, Including Bigger Pictures*, N.Y. TIMES, Mar. 8, 2013, at B4, *available at* http://www.nytimes.com/2013/03/08/technology/facebook-shows-off-redesign.html?pagewanted=all&_r=0 (describing how the company redesigned the user page to display larger photos and links).

161 *See, e.g.*, *id.*

162 *See supra* Part II.A.2.a.

protection of each individual social media account as a compilation work.

c) Work-Made-For-Hire

Assuming an SMA is copyrightable, as either individual posts or a compilation, the issue then becomes ownership of the copyrighted SMA. In weighing the factors delineated in *Community for Creative Non-Violence v. Reid*,[163] certain aspects of the employment relationship will weigh towards finding the hired party an employee rather than an independent contractor, and vice versa. Facts that would support an employer-employee relationship, where the company possesses the "right to control the manner and means by which the product is accomplished,"[164] may include the company supplying the tools,[165] (i.e., the username and password, and in some instances a computer or cell phone); the company hiring the individual with long-term intentions rather than for temporary work;[166] the hired party's compensation is not dependent on the completion of a specific job;[167] and if the hired party only manages the SMA of one company at a time.[168] However, facts that sound in independent discretion might favor finding the hired party as an independent contractor.[169] For example, if the hired party is given the access information or a company laptop to work from and is capable of posting from any location, such mobility and discretion might undermine an

163 490 U.S. 730, 731 (1989).

164 *Id*. at 751.

165 *See id.* at 751–52 (stating that the fact the hired party "supplied his own tools," favored finding him an independent contractor).

166 *See, e.g.*, *id.* at 752–53 (listing a hired party "retained for less than two months, a relatively short period of time" as a factor towards finding an independent contractor relationship).

167 *See, e.g.*, Holt v. Winpisinger, 811 F.2d 1532, 1540 (D.C. Cir. 1987) (stating that compensation based on completion of a specific job is typically found in an independent contractor relationship).

168 *See, e.g.*, Dumas v. Gommerman, 865 F.2d 1093, 1105 (9th Cir. 1989) (listing working for multiple businesses as an indication of an independent contractor relationship).

169 *See CCNV*, 490 U.S. at 751–52 (laying out factors that suggest an independent contractor relationship).

employment relationship.[170] Furthermore, the lack of daily supervision and control over the details of the work (i.e., the content or frequency of the posts) would also suggest the hired party is an independent contractor and not an employee.[171]

Although certain aspects of the job—access, flexibility, and deference to manage an SMA—typically align with characteristics of an independent contractor, these elements may carry less weight in this context because companies hire such social media managers with the very intention that the manager runs the account.[172] Also, these aspects are not without boundaries. The hired party cannot simply post anything she wants; rather, the job usually requires the manager to use the SMA to improve brand awareness or boost web traffic on behalf of the company.[173] In balancing these factors, it would seem that an SMA is the work product of an employee—the kind of work "motivated by a desire to further [the company's] corporate goals."[174] Ownership rights, then, would belong to the employer. On the other hand, finding the hired party as an independent contractor limits the company's ability to assert ownership rights; the only way for the company to claim ownership of the SMA would be if it fits within one of the nine categories of "specially or commissioned" works and if there is a written agreement signed by both parties explicitly indicating that the work is a work-made-for-hire as understood under the

---

170 *But see* Avtec Sys., Inc. v. Peiffer, 21 F.3d 568, 571–72 (4th Cir. 1994) (finding that "courts have tended no to grant employees authorship rights solely on the basis that the work was done at home on off-hours").

171 *See, e.g.*, *CCNV*, 490 U.S. at 752 (listing the impossibility for daily supervision because the artist worked in his own studio and freedom to decide when and how long to work as reasons for finding an independent contractor relationship).

172 Not to mention, the Supreme Court's rejection of applying the actual control (how closely the hiring party monitors the production process) and right to control (the hiring party's ability to control the product) test in determining whether or not a hired party is an employee. *See id.* at 750.

173 *See, e.g.*, PhoneDog v. Kravtiz, No. C 1103474 MEJ, 2011 WL 5415612, at *1 (N.D. Cal. Nov. 8, 2011) (describing the hired party's duties, which include promoting the company's services); *see also* LAWRENCE RAGAN COMM'N, INC. & NASDAQ OMX, STRUCTURING A SOCIAL MEDIA TEAM 13 (2012), *available at* http://web.ragan.com/raganforms/Structuring_A_Social_Media_Team.pdf (last visited Apr. 8, 2013).

174 *See Avtec Sys*., 21 F.3d at 572 (citing RESTATEMENT (SECOND) OF AGENCY § 236, cmt. b (1958)).

Copyright Act.[175] Nevertheless, ownership rights to an SMA, under the work-made-for-hire provision, ultimately depend on the existence of a valid copyright.[176]

d) Limitations

With regard to the three main assets of an SMA, copyright law actually speaks directly to one—the content. If individual posts are deemed copyrightable, then this framework is one step closer to establishing ownership rights to the SMA. However, as the analysis above demonstrates, the copyrightability of individual posts is questionable.[177] Even assuming the individual posts are copyrightable, this does not clarify ownership rights to the remaining assets of an SMA—the access information and subscribers.[178] If the posts are found to be copyrightable and the owner is the employee, the ownership dispute over the actual account would still remain. Although the work-made-for-hire provision appears as an efficient solution—speaking directly to ownership—the ownership rights afford are limited to all "the rights comprised in the copyright."[179] Taking the previous scenario, the employer may then own the copyrights to the posts, but still the issue of who owns the access information and subscribers remains unresolved. As such, to the extent individual posts are copyrightable, copyright law can only provide partial and limited ownership of an SMA.

3. Trade Secrets

The essence of a trade secret is "the secrecy of [the] information" that gives the owner a competitive advantage over its

---

175 *See* 17 U.S.C. § 101(2) (2006).

176 *See supra* Part II.A.2.a–b.

177 *See supra* Part II.A.2.a.

178 Finding originality in the access information and subscribers would far more challenging than in the individual posts. Arguably, access information serve a functional purpose—to log-in to the account, and subscriber lists are merely names—facts. *See* Feist Publ'ns, Inc., v. Rural Tel. Servs. Co., 499 U.S. 340, 347 (1991); Stern v. Does, No. CV 09—01986 DMG (PLAx), 2011 WL 997230, at *6 (C.D. Cal. Feb. 10, 2011), *aff'd* No. 11-55436, 2013 WL 1137390 (9th Cir. Mar. 20, 2013).

179 *See* 17 U.S.C. § 201(b) (2006).

competitors.[180] Trade secret disputes are common in the employer-employee context, which supports its popular use in recent SMA litigation.[181] Additionally, the scope of what may constitute a trade secret can be applied broadly—any "information . . . that derives independent economic value . . . from . . . not being generally known."[182] SMAs, as an emerging business tool, present an interesting challenge to the traditional understanding of trade secrets law, namely whether access information and subscribers may be trade secrets.

a) Access Information

The question of whether access information, the username and password, may be considered trade secrets has been addressed in a few jurisdictions. For example, in Virginia, courts have found that access-passwords, those "whose only value is to access other potentially valuable information," are not trade secrets.[183] Similarly, in applying Pennsylvania law, the court in *Eagle v. Morgan* determined that an employer identification number/password did not possess any economic value, and thus, could not be a trade secret.[184] In California, the courts have not dismissed the possibility that access information may constitute trade secrets,[185] but they have yet to rule on the actual merits of the issue.[186]

---

[180] Sys. Dev. Services, Inc. v. Haarmann, 389 Ill.App.3d 561, 572 (Ill 2009) (quoting Pope v. Alberto Culver Co., 296 Ill.App.3d 512 (1998)).

[181] *See supra* Part I.B.

[182] *See* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005).

[183] *See* Tryco., Inc. v. U.S. Med. Source, LLC, No. CL-2009-8914, 2010 WL 7373703, at *4 (Va. Cir. Ct. Aug. 3, 2010); *see also* State Analysis, Inc. v. Am. Fin. Serv. Ass'n, 621 F. Supp. 2d 309, 321 (E.D. Va. 2009) (finding a password that merely provides access not a trade secret).

[184] Eagle v. Morgan, Civil Action No. 11-4303, 2011 WL 6739448, at *11 (E.D. Pa. Dec. 22, 2011).

[185] *See, e.g.*, Therapeutic Research Faculty v. NBTY, Inc., 488 F.Supp.2d 991, 999 (E.D. Cal. 2007); TMX Funding, Inc., v. Impero Tech., Inc., No. C 10-00202 JF (PVT), 2010 WL 2509979, at *4 (N.D. Cal. June 17, 2010); PhoneDog v. Kravtiz, No. C1103474 MEJ, 2011 WL5415612, at *7 (N.D. Cal. Nov. 8, 2011).

[186] In all three cases, *Therapeutic Research*, *TMX Funding*, and *PhoneDog*, the California courts only denied motions to dismiss, and so far, only the parties in *PhoneDog* reached a settlement. *See Therapeutic Research*, 488 F.Supp.2d at 999; *TMX Funding*, 2010 WL 2509979, at *4; *PhoneDog*, 2011 WL5415612, at *7; Stipulation for

In those jurisdictions that have yet to address this question, whether or not access information constitutes trade secrets will be a highly fact-specific inquiry. Looking to the elements of a trade secret, arguments can be made for and against each. As the Virginia and Pennsylvania courts point out, one challenge with access information is satisfying the "independent economic value" requirement of a trade secret. Arguably, the access information possess some economic value—they are the key to accessing the coveted information or discovery—but it is far more difficult to argue they possess any *independent* economic value.[187] The argument being the username and password combination is merely a barrier and does not itself give rise to a substantial business advantage.[188] With regard to the actual secrecy of the access information, facts that support finding a trade secret would be if the employer identified the information as confidential and only the account manager knew the password.[189] However, if the employee created the password, and the employer never knew the password, then these facts could go against finding a trade secret—suggesting the employer failed to maintain its secrecy.[190] Lastly, as one court suggested,[191] the username/password combination may fail to even satisfy the first requirement of a trade secret, because it is not actual information.[192]

Dismissal After Settlement, PhoneDog v. Kravtiz, No. 3:11-cv-03474-MEJ, 2013 WL 207773 (N.D. Cal. Jan. 7, 2013).

187 *See State Analysis*, 621 F. Supp. 2d at 321.

188 *See id.* at 321; *see also* Sasqua Group, Inc. v. Courtney, No. CV 10-528 (ADS) (AKT), 2010 WL 3613855, at *19 (E.D.N.Y. Aug. 2, 2010).

189 *But see* Agency Solutions.com, LLC v. TriZetto Grp., 819 F. Supp. 2d 1001, 1015 (E.D. Cal. 2011) (stating that labeling information "Confidential" cannot enlarge the scope of a trade secret).

190 *See Sasqua Group*, 2010 WL 3613855, at *17 (considering whether trade secret protection should be afforded when the plaintiff did not acquire the information itself).

191 *See* MicroStrategy, Inc. v. Bus. Objects, S.A., 331 F. Supp. 2d 309, 429 n.4 (E.D. Va. 2004) (doubting whether or not a CD Key constitutes a trade secret where is it just a series of random numbers and not information).

192 *See Agency Solutions.com*, 819 F. Supp. 2d at 1016–17 (E.D. Cal. 2011) (finding a trade secret tends to be an idea that "communicate[s] (disclose[s]) the idea or fact to another," and where the information only identifies functionality, it is not a trade secret) (quoting Silvaco Data Sys. v. Intel Corp., 184 Cal.App.4th 210, 220–21 (Cal. Ct. App. 2010)).

b) Subscriber Lists

The trade secrets claim most related to the subscribers of a social media account is one regarding customer lists.[193] Customer lists have long been recognized as information that qualifies for trade secret protection.[194] The proprietary information in customer lists may vary, but most claims tend to include proprietary information such as the names of customers, customer preferences, and pricing strategies.[195] Additionally, customer lists are usually stored in a computer database or filing system.[196] Although customer lists tend to be recognized trade secrets, it is another question whether a subscriber list to an SMA is sufficiently comparable.

The first issue is whether a subscriber list constitutes "information." Information in a customer list satisfies the first requirement of a trade secret where it consists of information including customer preferences, special pricing, or any other personal notes.[197] However, if the list merely contains public information, it will not fall within trade secret protection.[198] A subscriber list generally just lists the names or even just usernames of it subscribers,[199] is most likely public information, and if anything, the information about each subscriber is not specifically tailored to the benefit of the business.[200] A list of names or basic information, even if public, may be protectable, but only if there is

---

193 Customer lists may also be referred to as client lists.

194 *See* Kewanee Oil Co., v. Bicron Corp, 416 U.S. 470, 483 (1974) (noting how protecting customer lists as trade secrets "encourages businesses to initiate new and individualized plans of operation, and constructive competition results").

195 *See, e.g.*, Sasqua Group, Inc. v. Courtney, 2010 WL 3613855 (E.D. N.Y. Aug. 2, 2010) (referring to other cases involving customer lists such as North Atlantic, Webcraft Technologies, 674 F. Supp. 1039 (S.D.N.Y. 1987)).

196 *See* cited cases *supra* Part I.C.3.

197 *See, e.g.*, Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc., 86 F.Supp.2d 1102, 1106 (D. Kan. 2000).

198 *See, e.g.*, *Fireworks*, 86 F. Supp. 2d at 1106; *see also* UNIFORM TRADE SECRETS ACT § 1(4) (1985).

199 *See, e.g.*, *FAQs About Following*, TWITTER HELP CENTER, http://support.twitter.com/articles/14019-faqs-about-following (last visited Mar. 25, 3013).

200 *See, e.g.*, *id.* (explaining how followers to a Twitter account see the account holder's tweets).

some extra degree of work involved in putting the names on a list.[201] In the case of SMAs, however, it is not the account holder that puts the names on the subscriber list, it is the subscribers themselves that elect to be on the list.[202] These factors suggest that the type of information actually involved, such as usernames, falls outside of that which is protected by trade secrets law.

Moreover, a subscriber list must not be "readily ascertainable" by others who would gain a competitive advantage by disclosing or using the information.[203] The first part of this element strikes at a pivotal factor with an SMA—its visibility. Subscribers to an SMA are generally visible to the public.[204] In fact, a company's subscriber list is intended to be publicly visible, because it allows its current and potential subscribers to see who else is subscribed, whether it be a friend, a celebrity, or a trusted voice in the industry, adding to brand reputation or credibility. Not only does a subscriber list's visibility contribute to its ascertainability, but also the ability to create or duplicate the list.[205] (For example, a

---

[201] *See Fireworks*, 86 F. Supp. 2d at 1106 (finding a customer list a trade secret where the company compiled its list over many years and thousands of hours); N. Atl. Instruments, Inc. v. Haber, 188 F.3d 38, 45 (2d Cir. 1999) (finding a client list a protectable trade secret where the list "took great time and effort to compile, including 'development of a specialized knowledge of the customer's operations and needs'") (quoting Webcraft Techs., Inc. v. McCaw, 674 F. Supp. 1039, 1044 (S.D.N.Y. 1987)).

[202] *See, e.g.*, *FAQs About Following*, TWITTER HELP CENTER, http://support.twitter.com/articles/14019-faqs-about-following (last visited Mar. 25, 3013) (explaining how followers choose which Twitter accounts to follow); *see also* Amanda Ashworth, *Twitter Tips for Proper Use by Brands*, SOCIALMEDIA TODAY (Jan. 21, 2013), http://socialmediatoday.com/recsocially/1173366/brands-simply-aren-t-using-twitter-or-aren-t-using-it-properly (explaining how brands see Twitter as a one-way channel, using it as they would traditional mediums like TV or print).

[203] *See* UNIFORM TRADE SECRETS ACT § 1(4) (1985).

[204] Anyone with an SMA on the same platform can view the subscriber list to that account by clicking on a "followers" (for Twitter) or "friends" (for Facebook) tab. *See, e.g.*, *Timeline*, FACEBOOK HELP CENTER, https://www.facebook.com/help/115450405225661 (stating that the default setting allows "everyone [to] see who your friends are").

[205] *See, e.g.*, Sasqua Group, Inc. v. Courtney, No. CV 10-528 (ADS)(AKT), 2010 WL 3613855, at *22 (E.D.N.Y. Aug. 2, 2010) (denying trade secret protection to a client list based on the "exponential proliferation of information made available through full-blown use of the Internet and the powerful tools it provides to access such information . . . a very different story").

competitor could, after viewing the subscribers to a company's SMA, contact each of those subscribers.)

The second half of the "readily ascertainable" factor considers the competitive advantage conferred to a trade secret holder from the secrecy of the information—the independent economic value of a trade secret.[206] Evidence of independent economic value varies based on the facts of each case. If the company can show that the subscriber list is the but-for cause of its success or can provide similar evidence that the subscriber list gives the company a competitive advantage over its competitors, this factor would weigh in favor of finding the list a valid trade secret.[207] The economic advantage provided must also be a result of the list's confidentiality.[208] The subscribers to an SMA undoubtedly possess some economic value,[209] i.e. developing brand awareness, but whether or not the secrecy of the list actually confers a competitive advantage worthy of trade secret protection is questionable.[210]

c) Limitations

Trade secrets law protects confidential business information with two policy goals in mind: (1) promoting standards of commercial ethics, and (2) encouraging invention.[211] The idea, of course, is that there are certain discoveries that are not protectable or not best protected under patent law.[212] Whether an owner of an

---

206 *See* UNIFORM TRADE SECRETS ACT § 1 (4) (1985).

207 *See Sasqua Group*, 2010 WL 3613855, at *19 (citing Dorazio v. Capitol Specialty Plastics, Inc., 2002 WL 31750215, at *4 (E.D.Pa. Dec. 9, 2002)); *see also* Fireworks Spectacular, Inc. v. Premier Pyrotechnics, 86 F. Supp. 2d 1102, 1006 (D. Kans. Feb. 23, 2000) (pointing to the defendant's admission that without the list he would have lost money support for finding a trade secret).

208 *See Fireworks*, 86 F. Supp. 2d at 1006.

209 *See* Amanda Ashworth, *Twitter Tips for Proper Use by Brands*, SOCIALMEDIA TODAY (Jan. 21, 2013), http://socialmediatoday.com/recsocially/1173366/brands-simply-aren-t-using-twitter-or-aren-t-using-it-properly.

210 "The information at issue must be substantially secret to impart economic value to both its owner and its competitors because of its relative secrecy." *See* Sys. Dev. Servs., Inc. v. Haarmann, 389 Ill.App.3d 561, 572 (Ill. App. 5th 2009) (quoting Pope v. Alberto Culver Co., 296 Ill.App.3d 512 (Ill. App. 1st 1998)).

211 *See* Kewanee Oil v. Bicron Corp., 416 U.S. 470, 481 (1974).

212 *See id*. at 483.

SMA can claim that account as a trade secret, however, is doubtful. The key to an eligible trade secret is not just that it is secret, but that its secrecy is a source of competitive advantage. As discussed above, the owner of an SMA faces substantial challenges in proving the access information and subscriber lists are trade secrets.[213] In addition to those obstacles, trade secrets law fails to address a key component of an SMA—the posted content. This makes sense, as posted content clearly cannot be a secret. As with copyright law, the ability for trade secrets law to establish ownership rights over the entire SMA is also limited.

B. Social Media Accounts Are Not Intellectual Property

Applying traditional intellectual property laws to SMA ownership disputes between employers and employees reveals the challenge in aligning social media accounts with traditional examples of intellectual property. Despite efforts by recent litigants to squeeze SMAs into recognized intellectual property regimes,[214] the actual application of these laws to the SMA as a whole, comprised of its three main assets, reveals the various shortfalls of this approach.[215] The incongruence between SMAs and intellectual property does not exist simply because no intellectual property regime can protect all three assets of an SMA. If anything, the difficulty in applying these laws to SMAs corroborates the more theoretical reasons why SMAs fall outside intellectual property.

A prominent view of intellectual property law is that it functions as an incentive-based legal framework, where granting exclusive rights over one's creative works rewards the owner for her creativity.[216] Not only does intellectual property law aim to provide an incentive to innovate, it also functions to promote the distribution of the creative works.[217] In doing so, as the Supreme Court stated in *Kewanee Oil Co. v. Bicron Corp.*, "the productive

---

213 *See supra* Part IIA.3.a–b.

214 *See supra* Part I.B.

215 *See supra* Part I.A.

216 Elizabeth L. Rosenblatt, *A Theory of IP's Negative Space*, 34 COLUM. J.L. & ARTS 317, 318 (2011).

217 *Id.* at 318 n.3.

effort thereby fostered will have a positive effect on society through the introduction of new products and processes of manufacture into the economy."[218] The Internet itself has spurred a new wave of innovation,[219] and considering social media's current pervasive dominance on the Internet, the use of SMAs commercially has undoubtedly contributed to the developments in new business methods and interactive technologies.[220] Based on such motivations, it is not surprising that litigants instinctively turn to intellectual property laws when disputing ownership of an SMA.[221] However, just because an issue involves the Internet, technology, or computers, does not mean it automatically becomes an intellectual property issue, and nor should it.[222] Importantly, not relying on intellectual property laws does not necessarily jeopardize the value or commercial growth of social media.[223]

If the go-to legal frameworks have been intellectual property, and as suggested, improperly so, this leaves open what legal framework should be used to determine the ownership of an SMA. The following section presents the Computer Fraud and Abuse Act as convincing solution.

III. THE CFAA AS THE APPROPRIATE FRAMEWORK FOR ESTABLISHING OWNERSHIP OF SOCIAL MEDIA ACCOUNTS

The Computer Fraud and Abuse Act, commonly referred to as the classic anti-hacking statute,[224] and more recently used to combat alleged employee misconduct,[225] offers a compelling framework for determining ownership of an SMA. The first, clear

---

[218] 416 U.S. 470, 480 (1974). The Court did not direct its statement at intellectual property law as a whole, but rather in an analysis of patent law and trade secrets law.

[219] *See* Michael L. Rustad & Diane D'Angelo, *The Path of Internet Law: An Annotated Guide to Legal Landmarks*, 2011 DUKE L. & TECH. REV. 12, *30 (2011).

[220] *See* Elefant, *supra* note 3, at 5–6.

[221] *See* Rustad & D'Angelo, *supra* note 219, at *30–84 (describing in detail how the Internet has affect intellectual property law).

[222] *See* Rosenblatt, *supra* note 216, at 321–22.

[223] *See generally id.* (describing how industries have thrived creatively and economically absent robust intellectual property law protection).

[224] *See* Tuma, *supra* note 89, at 155–56.

[225] *See* P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504, 510 (3d Cir. 2005).

distinction between the CFAA and intellectual property law is its focus on the unauthorized access of a computer—and not the substance of the information obtained.[226] Second, as the legislative history has indicated,[227] the type of violation envisioned under the CFAA is one that clearly identifies the property owner and the intruder.[228] This section first describes the practical application of potential CFAA claims in the employer-employee SMA dispute. Then, this section hones in on the key to this ownership dispute—authorization, and why the CFAA best addresses this issue.

A. Potential Claims: The Intentional Access Subsection and The Intent to Defraud Subsection

A company could assert a claim under the Intentional Access or the Intent to Defraud subsection when a former employee accesses an SMA account and changes the access information and account name. The elements of a civil claim under The Intentional Access subsection, § 1030(a)(2)(C), are as follows:

> (1) intentional access of a computer,
> (2) without authorization or exceeding authorized access,
> (3) thereby obtaining information
> (4) from any protected computer (if the conduct involved interstate or foreign communication), and
> (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.[229]

The elements of a civil claim under the Intent to Defraud subsection, § 1030 (a)(4), are as follows:

> (1) access of a protected computer,
> (2) without authorization or exceeding authorized access,
> (3) knowingly and with intent to defraud, thereby

---

[226] *See, e.g.*, Brenton, *supra* note 99, at 441 (identifying how the CFAA can "protect information that trade secret law would hold unprotectable").

[227] *See* Kapitanyan, *supra* note 90, at 410.

[228] *See* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 Cal. L. Rev. 439, 475–77 (2003) (describing how the CFAA exemplifies the concept of property owner and trespasser).

[229] *See* LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1131 (9th Cir. 2009).

> (4) furthering the intended fraud and obtained anything of value, causing
> (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.[230]

Since the major elemental difference between the two claims is that of fraud, this Note will approach the claims together, beginning with an analysis of whether or not the former employee's actions were "without authorization" or "exceeded[ed] authorized access." Then, this section will proceed to analyze the Intent element under the Intentional Access subsection, the Fraud element under the Intent to Defraud subsection, and ending with the $5,000 loss requirement.

1. Scope of Authorization

The nuanced differences between the *Citrin* standard and the *Brekka-Nosal* standard bear significant implications for determining ownership of an SMA in the context of an employer-employee dispute. A "without authorization" argument most likely would only work in a *Citrin* jurisdiction, on the grounds that the employee was no longer employed by the company when she logged back in the SMA and changed the access information, undermining her duty of loyalty to the company.[231] In comparison, a *Brekka-Nosal* jurisdiction would find it difficult to rule that the employee was "without authorization," where she was given permission to access the SMA in the beginning.[232] Given that the *Citrin* standard is an agency-based theory, it is not surprising that a CFAA claim would favor a finding that the SMA belonged to the company.

Moreover, if the employee was given permission to log into the account, and after her employment ended, decided to access the account, the question of whether or not the employee "exceeded authorization," would produce different results under *Citrin* and *Brekka-Nosal*. Under *Citrin*, the employee would be found to have

---

230 *See Brekka*, 581 F.3d at 1131.

231 Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21.

232 *See Brekka*, 581 F.3d at 1133 (clarifying that "without authorization" means "without any permission at all"); *Nosal II*, 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (explaining that "without authorization" applies to "*outside*" hackers).

unlawfully accessed the account, because the employee "resolved to act contrary to [the company's] interest."[233]

On the other hand, the *Brekka-Nosal* standard would apply a narrower interpretation of authorization. After *Nosal II*, it is not entirely clear if an employee, by merely changing the access information, would be considered to have "exceeded authorization" when the employee was permitted to access the social media website to begin with. *Nosal II* states that one "exceeds authorized access" when an employee is authorized to access only certain information but then accesses unauthorized information; the issue of how the information is used is irrelevant.[234] It appears, then, that the question is, does changing the password constitute a "use" violation or "access to unauthorized information"?[235] Given the examples that the Ninth Circuit provides,[236] it would appear the changing a password would be considered the latter, as an "unauthorized procurement or alternation of information."[237] Although this interpretation of the *Nosal II* favors company ownership, this standard of applying "exceeds authorization" is less certain than under the *Citrin* standard.

2. Intent

The Intentional Access subsection essentially requires an employee to intentionally access a computer, without authorization or exceeding authorized access, and obtain information from a protected computer.[238] Whether an employee intentionally accesses a computer requires the employee's conduct to "evince a clear intent to enter, without proper authorization, computer files

---

233 *See Brekka*, 581 F.3d 2233–34 (describing the *Citrin* holding).

234 *See Nosal II*, 676 F.3d at 863.

235 *See id.* at 858.

236 *See id.* at 860 (providing examples of potential liability to include "call[ing] family members from their work phones," or "visiting www.daillysoduku.com from their work computers").

237 *See id.* at 863 (quoting Shamrock Foods Co., Gast, 535 F. Supp. 2d 969, 965 (D. Ariz. 2008)).

238 *See* 18 U.S.C. § 1030(a)(2)(C) (2006).

or data belonging to another."[239] Furthermore, the section "doesn't not require proof of intent to defraud nor proof that the defendant knew the value of the information obtained."[240] A court may also look to the defendant's "conscious objective,"[241] but ultimately, the only proof necessary is "that the defendant intentionally accessed information from a protected computer."[242] In the context of SMAs, it is difficult to imagine how one may inadvertently access an account.[243] The *Nosal II* court also highlighted the relationship between intent and authorization, suggesting that where one is found to be "without or [to] exceed authorization," it is likely that one intended such access.[244] As such, the act of entering in the access information may in and of itself corroborate intent.[245]

3. Fraud

Although the statute uses the term "fraud," the CFAA does not require proof of common law fraud.[246] Rather, the element of fraud under the Intent to Defraud subsection calls for a wrongdoing of more than unauthorized access, "a showing of some taking, or use, of information."[247] For an employer to prevail on an Intent to Defraud claim, it would have to prove that the defendant, through unauthorized access to a protected computer, obtained something of value with the intent to defraud.[248] If it is assumed that the

---

[239] United States v. Drew, 259 F.R.D. 449, 459 (C.D. Cal. 2009) (citing S. REP. No. 99-432, at 5–6 (1986)).

[240] U.S. v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007).

[241] *See Drew*, 259 F.R.D. at 459.

[242] *Willis*, 476 F.3d at 1125.

[243] Perhaps, one may inadvertently access another's SMA if the SMA is set to automatically login.

[244] In explaining why "exceed authorization" cannot extend to merely prohibited "use," the court reasoned that if it did, then "subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent," would lead to "millions of unsuspecting individuals . . . find[ing] that they are engaging in criminal conduct." *See Nosal II*, 676 F.3d at 860.

[245] *See Willis*, 476 F.3d at 1125 n.1 ("[T]he Senate emphasized that 'intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe'") (quoting S. REP. No. 99-432 (1986)).

[246] Tuma, *supra* note 89, at 163.

[247] P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504, 509 (3d Cir. 2005).

[248] Kapitanyan, *supra* note 90, at 416.

employee was without authorization or exceeded his authorized access when she logged into the social media website, simply logging in would not give rise to a section 1030(a)(4) violation.[249] However, if the employee logged in and used the account to promote her own business or that of a competitor, such conduct may constitute the "use and abuse of proprietary information," and there would be a stronger argument for finding an intent to defraud.[250] Similarly, it is possible that logging in and changing the password to an SMA demonstrates an intent to defraud.

4. $5,000 Loss

In most civil cases involving a former employee, the company must prove that one or more persons sustained a loss of $5,000 over a one-year period as a result of an investigation, prosecution, or related course of conduct involving a CFAA violation.[251] The damages typically alleged in cases involving an SMA include costs associated with replacing advertising[252] and the value of the subscribers[253]—costs that are unlikely to be considered a "loss" under the CFAA, as they tend to fall in the category of lost business opportunities or missed revenue.[254] However, this does not mean that there are not "losses" associated with investigating or assessing or repairing a company's SMA. Examples of such pleadable "losses" may include employee time or third party expenses the company incurs when reaching out to the social media website in an attempt to recover the account, or expenses

[249] *See, e.g.*, Multiven, Inc. v. Cisco Sys., 725 F.Sup.2d 887, 893–94 (N.D. Cal. July 20, 2010) (describing how the defendant demonstrated an intent to defraud where he requested the login information, logged in multiple times, and retrieved information).

[250] See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001).

[251] 18 U.S.C. § 1030(5)(B)(i); Tuma, *supra* note 89, at 183.

[252] Eagle v. Morgan, No. 11-4303, 2012 WL 4739436, at *9 (E.D. Pa. Oct. 4, 2012).

[253] First Amended Complaint for Damages and Injunctive Relief; misappropriation of Trade Secrets; Intentional Interference with Prosepctive Economic Advantage; Negligent Interference with Prospective Economic Advantage; and Conversion, at para. 19, PhoneDog v. Kravtiz, No. 3:11-cv-03474-MEJ, 2011 WL 6955632 (Nov. 29, 2011).

[254] *See Eagle*, 2011 WL6739448, at *7.

associated with determining the value of the account to the business.[255]

B. The Key Issue: Authorization

The force behind the Computer Fraud and Abuse Act as a criminal statute is unauthorized access to a protected computer, and the provision that allows for a private right of action for the same unauthorized access presents a unique opportunity to address the emerging issue of ownership rights in social media.[256] With its focus on authorization, the CFAA arguably provides an advantageous framework for determining ownership over an SMA, because it recognizes and sufficiently protects the SMA as property[257] and eliminates the need to expand, carve-out, or twist intellectual property laws.

As with the relevant intellectual property regimes, the test as to whether the CFAA can establish ownership of an SMA is if the law adequately addresses each of the three main assets. Access information in the form of a username or password is pivotal in determining authorization. For example, under a *Citrin* standard, simply logging in the SMA to use the SMA in a manner contrary to the company's interest can be seen as unauthorized—tipping the ownership balance in favor of the employer.[258] Even under a *Brekka-Nosal* standard, logging in and changing the access information may amount to "exceed[ing] authorization," which may weigh in favor of the employer or the employee, depending on which party is trying to establish ownership.[259] With regard to subscribers and posted content, both represent the "information" at the other end of the access. The CFAA better protects both of these assets, because unlike the intellectual property regimes—i.e.

---

[255] *See, e.g.*, *EF Cultural Travel*, 274 F.3d at 584–85, Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir. 2004); *see also*, Tuma, *supra* note 89, at 186–87.

[256] *See* Brenton, *supra* note 99, at 429–30.

[257] *See* Hunter, *supra* note 228, at 475–83 (describing how the "action becomes a trespass against a form of quasi land that exists online").

[258] *See also* Brenton, *supra* note 99, at 460.

[259] For example, in *Eagle v. Morgan*, the company logged into the disputed LinkedIn account after the employee was terminated, prompting the employee to file a CFAA claim. *See Eagle*, 2012 WL 4739436, at *2.

copyright over posted content, and the subscriber list as a trade secret—the CFAA does not require that each represent proprietary information.[260] The posted content does not have to be "original" and the subscriber list does not have to be "secret" to be covered under the CFAA. At the end, embedded in the CFAA's authorization element is an inherent determination of ownership.

Lastly, the nature of the development of the CFAA also supports its applicability to social media governance. Since its inception, the CFAA has been amended multiple times, fulfilling Congress' intent to "keep pace with technological development."[261] Additionally, the baseline of the statute views computer networks and the Internet as "a place . . . just like the public roads that lead to private properties on which the defendant trespasses,"[262] and doing so provides a more comprehensive legal framework for assessing the world of social media, particularly when compared to intellectual property laws. Moreover, the social media industry, in its increasing ubiquity and robustness, is arguably an industry that will continue to develop and grow, as it has, without the need for intellectual property protection.

CONCLUSION

The increasing litigation over the ownership of SMAs presents new challenges to the scope and relevance of intellectual property laws, namely Trademark, Copyright, and Trade Secrets. The discussion of how the three intellectual property regimes apply to the issue of ownership further highlights the challenges and limitations of intellectual property as the governing body of law over social media. In comparison, the CFAA protects the SMA for what it is, and does so without forcing answers to equivocal questions such as whether the subscribers belong to the company or whether the posted content is sufficiently creative. Rather, the

---

[260] *See* Brenton, *supra* note 99, at 450 (explaining how accessing a list of director names, saved on a password-protected server, may give rise to a CFAA violation but not amount to misappropriation of a trade secret, because of the list's public character).

[261] *See* Kapitanyan, *supra* note 90, at 415–16 (citing S. REP. No. 104-357, at *5 (1986)).

[262] *See* Hunter, *supra* note 228, at 477.

CFAA correctly captures the role of SMAs as another tool for business, not an independent innovation by a company.