Developments in Social Media: First Amendment, Privacy, and Misappropriation

*By Brandon J. Huffman**

I. Introduction

During the past year, courts have continued catching up with a changing social media landscape, and decisions involving free speech, privacy, and misappropriation are becoming more common. The U.S. Supreme Court decided *Elonis v. United States*,[1] which many wrongly predicted would be an extremely important decision on First Amendment rights concerning threats made on Facebook. In *Garcia v. Google, Inc.*,[2] the U.S. Court of Appeals for the Ninth Circuit, sitting en banc, reversed a panel's confounding interpretation of copyright law, remedying the potential First Amendment issues created by the panel's earlier opinion. Facebook, Zynga, Snapchat, and LinkedIn each contended with privacy lawsuits, while the National Labor Relations Board provided additional guidance to employers regarding social media.[3] A Florida court concluded that there is no ownership interest in Facebook "likes."[4]

II. First Amendment

A. *Elonis v. United States*

The U.S. Supreme Court disappointed many First Amendment scholars in its most recent term by failing to address the free speech arguments raised in *Elonis v. United States*.

Section 875(c) of Title 18 of the U.S. Code criminalizes "any communication containing any threat . . . to injure the person of another" transmitted in interstate commerce.[5] After his wife left him, Anthony Elonis took to Facebook, where he made a series of posts including original rap lyrics that contained violent imagery regarding his wife, co-workers, a kindergarten class, and law

* Brandon J. Huffman is an attorney with Hutchison, PLLC in Raleigh, North Carolina, where he counsels clients on interactive media, the Internet, intellectual property, and corporate transactions.

1. 135 S. Ct. 2001 (2015).
2. 786 F.3d 733 (9th Cir. 2015) (en banc).
3. *See infra* Parts II.E, III.
4. Mattocks v. Black Entm't Television LLC, 43 F. Supp. 3d 1311 (S.D. Fla. 2014).
5. 18 U.S.C. § 875(c) (2012).

enforcement.[6] He was later charged with five, and convicted of four, counts of violating section 875(c).[7]

The district court instructed the jury that a statement is a "true threat," and therefore not protected by the First Amendment, when it is intentionally made in circumstances in which "a reasonable person would foresee that the statement would be interpreted" as an expression of intent to harm an individual.[8] The government's closing argument emphasized that, under those instructions, the speaker's intent was irrelevant.[9] Elonis challenged the jury instructions, arguing that the jury should have been required to find that he *subjectively* intended his posts to be threats.[10] The U.S. Court of Appeals for the Third Circuit disagreed and affirmed the conviction based on the objective standard.[11]

The Supreme Court's analysis began by explaining that, although the statute does not specify the requisite mental state for a conviction under section 875(c), the omission does not mean there is no mental state requirement, invoking the "general rule" that some sort of guilty mind is "a necessary element in the indictment and proof of every crime."[12] Rejecting the positions advocated by both the defendant and the government, the Court held that the "mental state requirement . . . is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat."[13] The Court, however, declined to address whether a mental state of recklessness would also suffice.[14]

The Court explained that the lower court decisions, and Elonis's conviction, were premised on how his posts would be understood by a reasonable person—equivalent to a negligence standard in tort law.[15] Because a negligence standard is inconsistent with the criminal law, and does not apply the level of intent required by the statute, the Court reversed the conviction and remanded the case.[16] Because the Court was able to dispose of the case through its statutory, mental-state analysis, it expressly declined to consider any First Amendment issues.[17]

This outcome fails to provide any new guidance on how the First Amendment bears upon the "true threats" doctrine,[18] but does portend that future convictions under section 875(c), albeit on a standard more stringent than what the government sought, are likely to come.

6. *Elonis*, 135 S. Ct. at 2005–07.
7. *Id.* at 2007.
8. *Id.* (quoting the jury instruction).
9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.* at 2009 (quoting United States v. Balint, 258 U.S. 250, 251 (1922)).
13. *Id.* at 2012.
14. *Id.*
15. *Id.* at 2011.
16. *Id.* at 2012–13.
17. *Id.* at 2012.
18. *See* Watts v. United States, 394 U.S. 705, 708 (1969) (per curiam) (distinguishing political hyperbole from a true threat).

B. *Garcia v. Google, Inc.*

In one of the most-anticipated decisions of the year, the Ninth Circuit, sitting en banc, reversed the panel decision in *Garcia v. Google, Inc*.[19] Plaintiff Garcia, an actress, appeared in a film, titled *Innocence of Muslims*, that she was told would be "an action-adventure thriller set in ancient Arabia," but that was, in fact, a virulently "anti-Islamic polemic."[20] Shortly after a video trailer for the film was posted to YouTube in June 2012, "an Egyptian cleric issued a fatwa against anyone associated with *Innocence of Muslims*, calling upon the 'Muslim Youth in America[ ] and Europe' to 'kill the director, the producer[,] and the actors and everyone who helped and promoted this film,'" and Garcia received multiple death threats.[21] Garcia asserted that she held a copyright interest in her five-second performance, and submitted to Google a series of takedown notices under the Digital Millennium Copyright Act.[22] When Google refused to remove the video from YouTube, Garcia brought a lawsuit against Google for copyright infringement.[23] The district court denied Garcia a preliminary injunction, but a divided panel of the Ninth Circuit reversed, requiring Google to take down the video within twenty-four hours.[24]

After a rehearing en banc, the Ninth Circuit determined, as the Copyright Office had in the interim, that Garcia's performance was not a copyrightable work.[25] The en banc court invoked circuit precedent evaluating copyright claims by persons who made some contribution to a motion picture, particularly *Aalmuhammed v. Lee*,[26] and observed: "Garcia's theory of copyright law would result in the legal morass we warned against in *Aalmuhammed*—splintering a movie into many different 'works,' even in the absence of an independent fixation. Simply put, as Google claimed, it 'make[s] Swiss cheese of copyrights.'"[27]

The en banc court also addressed the First Amendment implications of the case, writing:

> The takedown order . . . gave short shrift to the First Amendment values at stake. The mandatory injunction censored and suppressed a politically significant film—based upon a dubious and unprecedented theory of copyright. In so doing, the panel deprived the public of the ability to view firsthand, and judge for themselves, a film at the center of an international uproar.

19. 786 F.3d 733 (9th Cir. 2015) (en banc).
20. *Id.* at 737.
21. *Id.* at 738 (alterations by the court).
22. *Id.*; *see* 17 U.S.C. § 512(c) (2012). Google, Inc. owns YouTube LLC. *Garcia*, 786 F.3d at 737.
23. *Garcia*, 786 F.3d at 738.
24. *Id.* at 738–39. The panel decision is Garcia v. Google, Inc., 743 F.3d 1258 (9th Cir.), *amended & superseded by* 766 F.3d 929 (9th Cir. 2014), *rev'd en banc*, 786 F.3d 733 (9th Cir. 2015).
25. *Garcia*, 786 F.3d at 740–41.
26. 202 F.3d 1227 (9th Cir. 2000).
27. *Garcia*, 786 F.3d at 742 (alteration by court).

> Although the intersection between copyright and the First Amendment is much-debated, the Supreme Court teaches that copyright is not "categorically immune from challenges under the First Amendment."[28]

The en banc court accordingly dissolved the panel's injunction.[29]

C. Other Circuit Court Decisions

Like the Supreme Court in *Elonis*, the U.S. Court of Appeals for the Fifth Circuit also tangled with threats posted to the Internet, though in the context of a challenge to a high school student's suspension, rather than a criminal prosecution. In *Bell v. Itawamba County School Board*, a public high school student was suspended after posting an original rap video to Facebook and YouTube that criticized, "with vulgar and violent lyrics," two male coaches at his school for harassing female students.[30] The student sued, alleging violation of his First Amendment free speech rights.[31] The district court granted summary judgment for the school board, holding that, under the test the Supreme Court established in *Tinker v. Des Moines Independent Community School District*,[32] the song's lyrics had caused disruption and therefore the First Amendment did not prevent the school from disciplining the student.[33] A panel of the Fifth Circuit reversed.[34]

The appellate court, assuming but not deciding that the *Tinker* test applied to off-campus activity, held that the evidence did not support a finding that the song "either substantially disrupted the school's work or discipline or that the school officials reasonably could have forecasted such a disruption."[35] The court also rejected the school board's argument that the video constituted a "true threat" outside the scope of the First Amendment.[36] Among other factors, the court noted that the song "was broadcast publicly over the Internet and not conveyed privately or directly to the coaches. Courts have recognized that statements communicated directly to the target are much more likely to constitute true threats than those, as here, communicated as part of a public protest."[37]

In February 2015, the Fifth Circuit granted rehearing en banc,[38] and on August 20, 2015, issued an opinion concluding that the *Tinker* test does, in fact apply to off-campus speech, that the recording was made with the intention that it would reach the school community, and that "regardless of whether Bell's statements in the rap recording qualify as "true threats" . . . they constitute threats, harassment, and intimidation as a layperson would understand the

28. *Id.* at 747 (footnote omitted) (quoting Eldred v. Ashcroft, 537 U.S. 186, 221 (2003)).
29. *Id.*
30. 774 F.3d 280, 282 (5th Cir. 2014), *reh'g en banc granted*, 782 F.3d 712 (5th Cir. 2015).
31. *Id.*
32. 393 U.S. 503 (1969).
33. *Bell*, 774 F.3d at 290.
34. *Id.* at 291. Bell's mother was also a plaintiff in the trial court, but the Fifth Circuit affirmed the district court's grant of summary judgment to the school board on her claims. *See id.* at 289 & n.33.
35. *Id.* at 304.
36. *Id.*
37. *Id.* at 302.
38. Bell v. Itawamba Cty. Sch. Bd., 782 F.3d 712 (5th Cir. 2015).

terms."[39] Thus, the en banc court reversed the panel decision and affirmed the trial court's order.[40] In so doing, it concluded that the rap was in violation of the school's disciplinary policy, and that, based in part on the logic of *Elonis*, the court need not reach the question of whether it constituted a "true threat."[41]

In *Graziosi v. City of Greenville,* the Fifth Circuit considered an appeal from summary judgment for the defendants in a wrongful termination case.[42] The plaintiff, a police officer, was terminated following several posts to Facebook on both her personal page and the mayor's public page critical of the department and her superior officer.[43] The appellate court determined, contrary to the district court, that the plaintiff made the statements as a private citizen outside the scope of her employment.[44] However, the appellate court held that plaintiff's postings did not address a matter of public concern.[45] As part of its analysis, the court noted that the "form" of plaintiff's speech, namely "a public post on the mayor's Facebook page," weighs in favor of a finding that she spoke on a matter of public concern.[46] Nevertheless, consideration of the "content" and "context" of the speech led the court to conclude that, on balance, it did not address a matter of public concern and that plaintiff therefore was not entitled to First Amendment protection.[47] With respect to content, the court reasoned that the plaintiff's primary motivation was her personal dissatisfaction with the department, not corruption or other matters important to the public.[48] As for context, the timing of the posts likewise supported the conclusion that the matter was a private one.[49] Finally, the court explained that, even if the plaintiff had been speaking on a matter of public concern, she failed to persuade that those interests outweighed the department's substantial interest in maintaining discipline and order within the department.[50] Thus, the Fifth Circuit affirmed the district court decision.[51]

39. Bell v. Itawamba Cty. Sch. Bd., No. 12-60264 (5th Cir. Aug. 20, 2015) (en banc).
40. *Id.*
41. *Id.*
42. 775 F.3d 731, 733 (5th Cir. 2015).
43. *Id.* at 733–34.
44. *Id.* at 737.
45. *Id.* at 737–38.
46. *Id.* at 739.
47. *Id.* at 739–40.
48. *Id.* at 739.
49. *Id.*
50. *Id.* at 740–41. In performing this balancing analysis, the court relied on the premise that, "[b]ecause 'police departments function as paramilitary organizations charged with maintaining public safety and order, they are given *more* latitude in their decisions regarding discipline and personnel regulations than an ordinary government employer.'" *Id.* at 740 (quoting Nixon v. City of Houston, 511 F.3d 494, 498 (5th Cir. 2007)). It is unclear whether the court would have applied the same standard to a plaintiff who was not a police officer, but, because the court also found that the speech was not protected, the point is moot in this case.
51. *Id.* at 741.

D. Cyberbullying

The past year also saw the rise of regulation promulgated in response to increased media coverage of cyberbullying over the past several years. There have also been challenges to such regulation.

For example, in *Beverly v. Watson*, two professors at Chicago State University filed suit against the university, challenging the school's computer usage and cyberbullying policies on First Amendment free speech grounds.[52] The plaintiffs were regular contributors to a blog that was critical of the university's administration, and defendants sent them a cease-and-desist letter demanding that they discontinue the blog.[53] In response to the university's motion to dismiss for lack of standing, the trial court held that plaintiffs had sufficiently alleged that the letter conveyed a threat to take action against them under the challenged policies, thereby meeting the "actual or imminent injury requirement" for standing.[54]

In another case, the New York Court of Appeals reversed the conviction of a sixteen-year-old high school student under a county cyberbullying law.[55] The student created a Facebook page on which he "anonymously posted photographs of high-school classmates and other adolescents, with detailed descriptions of their alleged sexual practices and predilections, sexual partners and other types of personal information," together with vulgar captions.[56] The court found that cyberbullying is not categorically immune from government regulation, but determined that it had to consider whether the law was unconstitutionally overbroad or vague.[57] The county admitted that the statute was overbroad, but contended that the severability clause in the law should save it from invalidation by the court.[58] The court expounded at length about the problem bullying presents, as well as the state's efforts to combat it, and lauded the county for its efforts.[59] In the end, however, the court determined that it could not, without exceeding the scope of its judicial role, "rewrite" the law in a way that would cure its First Amendment infirmities.[60] Accordingly, the court reversed the conviction.[61]

E. Workplace Use of Social Media

The National Labor Relations Board (NLRB or Board) continued its ongoing efforts to promulgate helpful guidelines for employers' handling of employee social media usage.

52. No. 14 C 4970, 2015 WL 170409, at *1 (N.D. Ill. Jan. 13, 2015).
53. *Id.* at *1, *3.
54. *See id.* at *4.
55. People v. Marquan M., 19 N.E.3d 480, 488 (N.Y. 2014).
56. *Id.* at 484.
57. *Id.* at 485.
58. *Id.* at 486–87.
59. *Id.* at 488.
60. *Id.* at 487–88.
61. *Id.* at 488.

In *Three D, LLC*,[62] a former employee of a sports bar and restaurant complained in disparaging terms on her Facebook page about the company's handling of her state income tax. One current employee "liked" her post, and another added a comment expressing agreement with the post.[63] Within two days, both of those employees were fired.[64] Having found that the fired employees were engaged in concerted activity that was protected under the National Labor Relations Act (NLRA or Act), the Board addressed the restaurant's position that the employees had lost the Act's protection by expressing support for the disparaging posting.[65] The Board wrote that the analytical framework set forth in *Atlantic Steel Co.*,[66] which was formulated in the context of verbal outbursts in a face-to-face workplace setting, is "not well suited" to address issues involving employees' off-duty, offsite use of social media.[67] The Board instead analyzed the employees' conduct under its "precedent relating to disloyal or defamatory statements."[68] Finding that, in context, the posting was not so disloyal as to warrant withdrawal of the Act's protection (and that the posting was not defamatory), the Board concluded that the activity was protected by the Act, and held that the company's discharge of the employees violated their protected rights.[69]

In *Weigand v. NLRB*, the U.S. Court of Appeals for the D.C. Circuit upheld an NLRB decision that a union was not responsible for threatening remarks posted by union members on a Facebook page that the union maintained for its members.[70] The Acting General Counsel

> advanced a theory that the Union had a "duty to disavow" any statements posted on the Facebook page that were "unlawful threats." In support of this theory, the Acting General Counsel relied on case law that holds a labor organization responsible for its members' picket-line misconduct when it does not correct or disavow the misconduct.[71]

The Board, however, found that the Facebook page had little in common with a picket line:

> A picket line proclaims to the public, in a highly visible way, that the striking union has a dispute with the employer, and thus seeks to enlist the public in its effort to place economic pressure on the employer. . . . In contrast, Respondent's Face-

62. 361 N.L.R.B. No. 31, 2014 WL 4182705 (Aug. 22, 2014).
63. *See id.* at *2.
64. *Id.* at *3.
65. *Id.* at *3–4.
66. Atl. Steel Co., 245 N.L.R.B. 814 (1979). Under the *Atlantic Steel* framework, the Board determines whether an employee's verbal outburst causes him to lose the protection of the NLRA by balancing four factors: "(1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee's outburst; and (4) whether the outburst was, in any way, provoked by the employer's unfair labor practices." *Three D*, 2014 WL 4182705, at *4.
67. *Three D*, 2014 WL 4182705, at *4.
68. *Id.* at *5.
69. *Id.* at *7.
70. 783 F.3d 889 (D.C. Cir. 2015).
71. *Id.* at 893 (citations omitted).

> book page does not serve to communicate a message to the public. To the contrary, it is private. Moreover, it does not draw any line in the sand or on the sidewalk.
>
> Unlike a website in cyberspace, an actual picket line confronts employees reporting for work with a stark and unavoidable choice: To cross or not to cross. Should someone acting as a union's agent make a threat while on the picket line, the coercive effect is immediate and unattenuated because it falls on the ears of an employee who, at that very moment, must make a decision concerning the exercise of his Section 7 rights.
>
> Considering the marked differences, the Respondent's Facebook page certainly does not amount to an extension of Respondent's picket line . . . .[72]

The court emphasized that it was expressing no opinion on whether the same outcome would follow if the persons posting on Facebook were agents of the union, or if the postings were on an open Internet website, rather than on a forum that was accessible only by members of the union.[73]

III. Privacy

A. Facebook

In *Campbell v. Facebook Inc.*, Facebook users brought an action seeking to represent a nationwide class and alleging that Facebook violated the Wiretap Act,[74] California's Invasion of Privacy Act (CIPA), and California's Unfair Competition Law by scanning private direct messages sent between users on the site, identifying any links to web pages in the messages, and then using that information to increment a "like" counter on the corresponding web page and to deliver targeted advertising.[75] Facebook moved to dismiss for failure to state a claim.[76]

On the Wiretap Act claim, Facebook argued that it had not engaged in any "interception" of the messages.[77] Applying a decision of the Ninth Circuit that held that an "interception" occurs when the contents are "captured or *redirected* in any way,"[78] the district court held that Facebook's use of a "web crawler" to scan the URLs in the messages could constitute "redirection."[79] Facebook also

72. *Id.* at 893–94 (quoting the ALJ's opinion, which, on those points, was adopted by the Board).
73. *Id.* at 897.
74. Congress enacted the Wiretap Act in 1968. *See* Wiretapping and Electronic Surveillance Act, Pub. L. No. 90-351, §§ 801–803, 82 Stat. 197, 211–25 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (2012)). Congress repeatedly has amended the act, including in 1986. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 101–111, 100 Stat. 1848, 1848–59 (1986) (amending the Wiretap Act and other sections of the U.S.C.).
75. Campbell v. Facebook Inc., No. C 13-5996 PJH, 2014 WL 7336475, at *1 (N.D. Cal. Dec. 23, 2014).
76. *Id.*
77. *Id.* at *3.
78. *Id.* (quoting Noel v. Hall, 568 F.3d 743, 749 (9th Cir. 2009)); *see* 18 U.S.C. § 2511(1)(a) (2012) (providing remedies against one who "intentionally intercepts . . . any . . . electronic communication").
79. *Campbell*, 2014 WL 7336475, at *3.

argued that there was no "interception" because it accessed the messages while in "storage," not during "transmission," but the court held that that determination too had to await development of the factual record.[80]

The court also found that the issue of whether Facebook's conduct fell into the "ordinary course of business" exception of the Wiretap Act could not be resolved on a motion to dismiss.[81] Discussing at length the broader and narrower interpretations of the scope of this exception, the court ultimately concluded that "Facebook has not offered a sufficient explanation of how the challenged practice falls within the ordinary course of its business."[82] The court also rejected Facebook's argument "that any activity that generates revenue for a company should be considered within the 'ordinary course of its business.'"[83]

Finally, the court rejected Facebook's argument that its users had consented to the scanning of their private messages when they agreed to Facebook's website terms of service (TOS).[84] Facebook pointed to language in the TOS that Facebook "may use the information [it] receive[s] about you . . . for . . . data analysis,"[85] but the court held "this disclosure is not specific enough to establish that users expressly consented to the scanning of the content of their messages—which are described as 'private messages'—for alleged use in targeted advertising."[86]

Plaintiffs also alleged two violations of CIPA.[87] The first claim, under a provision analogous to the Wiretap Act, withstood the motion to dismiss for the same reasons that the federal claim survived.[88] However, the court granted Facebook's motion to dismiss the second claim, predicated on a provision of CIPA that makes it unlawful to intercept a "confidential communication."[89] Relying on California precedent, the court held that "Internet-based communications," including chats, e-mail, and the "private messages" involved in the case, were not "confidential" under CIPA, because such communications can easily be shared by the recipients.[90]

The court also dismissed plaintiffs' Unfair Competition Law claim, on the ground that they could not satisfy the statute's "injury in fact" requirement because they "ha[d] not alleged that they . . . lost any money or property as a result of Facebook's conduct."[91]

In another case involving the Facebook ecosystem, *In re Zynga Privacy Litigation*,[92] users of the social network and gaming apps developed by Zynga brought

80. *Id.*
81. *Id.* at *4–8; *see* 18 U.S.C. § 2510(5) (2012) (defining "electronic, mechanical, or other device" as any device that can be used for interception, but excluding those devices "being used by a provider of wire or electronic communication service in the ordinary course of its business").
82. *Campbell*, 2014 WL 7336475, at *6.
83. *Id.* at *7 (quoting 18 U.S.C. § 2510(5)).
84. *Id.* at *8–10.
85. *Id.* at *9 (quoting the TOS).
86. *Id.*
87. *Id.* at *10–11.
88. *Id.* at *10 (interpreting Cal. Penal Code § 631).
89. *Id.* at *11 (interpreting Cal. Penal Code § 632).
90. *Id.* (applying People v. Nakai, 107 Cal. Rptr. 3d 402 (Ct. App. 2010)).
91. *Id.* at *11–12 (interpreting Cal. Bus. & Prof. Code § 17200).
92. 750 F.3d 1098 (9th Cir. 2014).

a class action claiming that Zynga and Facebook violated the Electronic Communications Privacy Act of 1986 (ECPA)[93] through automatic transmissions of user data from Zynga to Facebook. Zynga's apps used "referer headers"[94] that transmitted to Facebook two pieces of information in response to the user clicking on a Facebook web page: "the user's Facebook ID and the address of the Facebook webpage the user was viewing when the user clicked the link."[95] The information enabled third parties to target their advertising to Facebook's users.[96] The Ninth Circuit affirmed the district court's dismissal of the claims.[97] It explained that plaintiffs' claims could succeed only if the defendants had divulged the "contents of any communication," and held that the two pieces of information in question did not constitute "contents" but rather "record information."[98] The court drew a clear distinction between the two categories of communications, holding that "under the ECPA, the term 'contents' refers to the intended message conveyed by the communication and does not include record information regarding the characteristics of the message that is generated in the course of the communication."[99]

B. LinkedIn

In *Perkins v. LinkedIn Corp.*, plaintiffs filed a complaint alleging that LinkedIn violated several state and federal laws by "harvesting email addresses from the contact lists of email accounts associated with Plaintiffs' LinkedIn accounts and by sending repeated invitations to join LinkedIn to the harvested email addresses."[100] Upon receiving a member's authorization, LinkedIn would send an invitation email to the member's contacts who were not already LinkedIn members.[101] If a recipient did not respond within a week, LinkedIn sent a second e-mail with the same message, and after another week, LinkedIn sent a third such message.[102] LinkedIn moved to dismiss.[103]

93. While Title I of the ECPA amended the Wiretap Act, Title II of the ECPA set forth the Stored Communications Act. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201–202, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2710 ((2012)).

94. A "referer header" is a component of the HTTP specification that allows a user's computer to transmit information to the server hosting a website. *Zynga*, 750 F.3d at 1102 & n.3.

95. *Id.* at 1102–03.

96. *See id.* at 1102.

97. *Id.* at 1100.

98. *Id.* at 1103–06 (interpreting 18 U.S.C. §2511(3)(a) (2012) (prohibiting any person from intentionally divulging the "contents of any communication" to anyone other than the intended addressee); 18 U.S.C. § 2702 (2012) (prohibiting a service provider from divulging "record or other information" pertaining to a customer *to any governmental entity*, while prohibiting any such provider from divulging the "contents of a communication" *to any person*), *amended by* Pub. L. No. 114-23, § 602(d), 129 Stat. 268, 295 (2015)).

99. *Id.* at 1106.

100. 53 F. Supp. 3d 1190, 1195 (N.D. Cal. 2014).

101. *Id.* at 1198–99.

102. *Id.* at 1199–200.

103. *Id.* at 1195.

The district court denied the motion in part, and granted it in part.[104] The court noted at the outset of its analysis that plaintiffs challenged two steps in LinkedIn's processes: (1) the collection of e-mail addresses from users' contacts, and (2) the use of those e-mails in sending out endorsements with the users' names included.[105] The court concluded, based on screenshots of the LinkedIn signup process, that users consented to both the collection and the use of the data.[106] Thus, the court granted the motion to dismiss the claims brought under the ECPA.[107]

The court next addressed the common law right of publicity claim, which could succeed only if plaintiffs demonstrated their "lack of consent" to the e-mails.[108] The court found that plaintiffs had consented to the sending of an initial invitation e-mail to each of their contacts, including the implied endorsement of LinkedIn.[109] However, the court held "that Plaintiffs have plausibly alleged that they did not consent to the second and third reminder endorsement emails."[110] The court further found that plaintiffs had sufficiently pled that the sending of the reminder e-mails caused them injury, another element of the claim.[111] As the court explained, the sending of these messages "could injure users' reputations by allowing contacts to think that the users are the types of people who spam their contacts or are unable to take the hint that their contacts do not want to join their LinkedIn network."[112]

In a subsequent opinion in the same case, the district court denied LinkedIn's First Amendment defense, finding that the reminder messages constituted commercial speech.[113]

C. Snapchat

In December 2014, the Federal Trade Commission (FTC) gave final approval to a settlement of its charges against Snapchat.[114] The FTC had alleged, *inter alia,* that Snapchat made false promises about the disappearing nature of the images sent through the service, falsely stated that it did not collect users' location information, and misrepresented the security measures it took to protect users' data from disclosure.[115] The failure to use reasonable security measures allegedly allowed hackers "to compile a database of 4.6 million Snapchat usernames

104. *Id.*
105. *Id.* at 1206.
106. *Id.* at 1211–14.
107. *Id.* at 1214.
108. *Id.* at 1214–17.
109. *Id.* at 1217.
110. *Id.* at 1216.
111. *Id.* at 1214, 1216.
112. *Id.* at 1216.
113. Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1222, 1249–54 (N.D. Cal. 2014).
114. *In re* Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014) (decision and order) [hereinafter FTC Decision and Order], *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.
115. Complaint at 2–9, *In re* Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

and the associated mobile phone numbers . . . [which] . . . could lead to costly spam, phishing, and other unsolicited communications."[116] The settlement prohibits Snapchat from misrepresenting the extent to which it protects the privacy, security, or confidentiality of users' information.[117] It also requires Snapchat to implement a comprehensive privacy program to be monitored by an independent privacy professional for twenty years.[118]

Likewise, Snapchat entered into a settlement with the Maryland Attorney General following claims that the company misled users about the ephemeral and private nature of their use of the app.[119] Snapchat's settlement with Maryland is similar to its settlement with the FTC, but the former requires Snapchat to make affirmative disclosures to its users that recipients of their messages may copy or capture those messages.[120] The settlement also requires Snapchat to get affirmative consent before collecting information from users' address books, and, for ten years, to take steps to ensure children under the age of thirteen are not using the app.[121] Finally, it requires Snapchat to make a $100,000 payment to the state.[122]

D. Legislation on Employer Access to Employee Social Media Accounts

In May 2015, Connecticut became the twenty-first state to enact a law banning (with some exceptions) employers from requiring their employees to provide them with the username or password necessary to access the employee's social media account.[123] The first such law was enacted by Maryland in 2012.[124] Some of these laws apply similar restrictions to schools and landlords.[125] Employers in a growing number of states should take heed of these restrictions when seeking methods to oversee the behavior of their employees.

116. *Id.* at 8.

117. FTC Decision and Order, *supra* note 114, at 2.

118. *Id.* at 3–4.

119. *See* Press Release, Office of the Md. Att'y Gen., Attorney General Gansler Secures Settlement from Snapchat, Inc. (June 12, 2014), http://www.oag.state.md.us/Press/2014/061214.html.

120. Jeff Clabaugh, *Snapchat Pays Maryland $100K in Settlement*, Wash. Bus. J. (June 13, 2014), http://www.bizjournals.com/washington/news/2014/06/12/snapchat-pays-maryland-100k-in-settlement.html.

121. *See* Press Release, Office of the Md. Att'y Gen., *supra* note 119.

122. *Id.*

123. Bruce H. Raymond, *Keeping Your Online Accounts Private—Can Employers Request Access to Your Facebook?,* Nat'l L. Rev. (June 22, 2015), 2015 WLNR 18347459. For the current status of such legislation, see *Access to Social Media Usernames and Passwords,* Nat'l Conf. St. Legislatures (July 9, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx [hereinafter *Access to Social Media*].

124. *See Access to Social Media*, *supra* note 123 (referencing Md. Code Ann., Lab. & Empl. § 3-712).

125. *See id.*

IV. Misappropriation

In *Mattocks v. Black Entertainment Television LLC*, a novel case out of the Southern District of Florida, the court was asked to consider whether a user has an ownership interest in a Facebook "like."[126] Mattocks created a Facebook fan page about a television series on the CW Network.[127] Black Entertainment Television LLC (BET) later acquired rights to the series and hired Mattocks to manage the fan page.[128] During that time, the number of likes grew from two to six million.[129] After a dispute arose, Mattocks reduced BET's administrative rights on the page, preventing BET from posting on the page.[130] BET responded by asking Facebook to migrate the "likes" from the fan page to an official BET page, and Facebook did so.[131] BET also persuaded Twitter to disable the account that Mattocks had used to promote the series.[132]

Mattocks sued BET alleging, *inter alia,* that BET tortiously interfered with her contracts with Facebook and Twitter, and that it converted a business interest she had in the page.[133] The district court granted BET summary judgment on the claims.[134]

The court reasoned that the tortious interference claim must fail because BET was not "a stranger to the business relationship" between Mattocks and the social networks, given its control over Mattocks' use of the accounts.[135] BET's contacts with Facebook and Twitter were therefore justified and not tortious.[136] The conversion claim failed because Mattocks could not establish a property interest in the "likes."[137] The court explained:

> "[L]iking" a Facebook Page simply means that the user is expressing his or her enjoyment or approval of the content. At any time, moreover, the user is free to revoke the "like" by clicking an "unlike" button. So if anyone can be deemed to own the "likes" on a Page, it is the individual users responsible for them. . . . Given the tenuous relationship between "likes" on a Facebook Page and the creator of the Page, the "likes" cannot be converted in the same manner as goodwill or other intangible business interests.[138]

Mattocks' appeal to the Eleventh Circuit is currently pending.[139] Depending on the outcome of the appeal, going forward, Facebook and LinkedIn "likes," Twit-

126. Mattocks v. Black Entm't Television LLC, 43 F. Supp. 3d 1311 (S.D. Fla. 2014).
127. *Id.* at 1315.
128. *Id.* at 1314–16.
129. *Id*. at 1316.
130. *Id.*
131. *Id*. at 1316–17.
132. *Id.* at 1317.
133. *Id.*
134. *Id*. at 1321.
135. *Id*. at 1319 ("For interference with a contract to be *un*justified, the interfering defendant must be a third party, a stranger to the business relationship." (internal quotations omitted)).
136. *Id.* at 1318–19.
137. *Id*. at 1321.
138. *Id.*
139. Notice of Appeal, Mattocks v. Black Entm't Television LLC, No. 14-14238 (11th Cir. Sept. 19, 2014).

ter "favorites," and similar endorsements may be treated as transient, fleeting speech, rather than intangible property. By contrast, individual or business social media *accounts* have been treated as property.[140]

V. Revenge Pornography

In the past year, legislatures and courts around the country have responded to the increased incidence of "revenge porn."[141]

In what may be the first conviction of the operator of a revenge porn website, Kevin Bollaert, who operated a website that allowed postings of revenge porn images, and who charged the victims $250 to $350 to take down the images, was convicted by a California jury of extortion and identity theft.[142] He was sentenced to eighteen years in prison.[143] In a similar case, the FTC agreed to settle claims under the FTC Act against Craig Brittain for soliciting nude photographs which he posted on the website isanybodydown.com, and then charging the victims money to remove the photographs.[144]

In 2013, California enacted the first law specifically addressing revenge porn, and by one count, twenty-four additional states now have such a law.[145] As in the Bollaert prosecution, existing laws of more general applicability may also criminalize the conduct associated with revenge porn. For example, the Supreme Court of Maine upheld an order, issued pursuant to a "protection from abuse" law, prohibiting a defendant from carrying out a threat to post nude photographs of plaintiff on a website he created in her name.[146]

---

140. *See, e.g.*, *In re* CTLI, LLC, 528 B.R. 359, 366–67 (Bankr. S.D. Tex. 2015) (holding that the social media accounts of a debtor limited liability company were the property of the bankruptcy estate).

141. Revenge porn

> involves the distribution of nude or sexually explicit photographs or videos of an individual without that individual's consent. These sexually explicit images include photographs and videos taken by the victim, as well as images taken by the poster or another. Though hackers sometimes obtain and distribute the images, the photos often surface after a romantic relationship.

Amanda L. Cecil, Note, *Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography*, 71 Wash. & Lee L. Rev. 2513, 2520 (2014) (footnotes omitted).

142. Press Release, Office of the Att'y Gen. of Cal., Attorney General Kamala D. Harris Announces 18 Year Prison Sentence for Cyber-Exploitation Website Operator (Apr. 3, 2015), https://www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-18-year-prison-sentence-cyber; *see* Complaint, People v. Bollaert, No. SCD252338 (Cal. Super. Ct. Dec. 10, 2013), *available at* https://www.oag.ca.gov/system/files/attachments/press_releases/Complaint_3.pdf.

143. Steve Almasy, *"Revenge Porn" Operator Gets 18 Years in Prison*, CNN (Apr. 4, 2015, 10:12 AM), http://www.cnn.com/2015/04/03/us/califomia-revenge-porn-sentence/.

144. Agreement Containing Consent Order, *In re* Brittain, No. 132-3120 (F.T.C. Jan. 29, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150129craigbrittainagree.pdf; *see* Complaint, *In re* Brittain, No. 132-3120 (F.T.C. Jan. 29, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150129craigbrittaincmpt.pdf.

145. *25 States Have Revenge Porn Laws*, End Revenge Porn, http://www.endrevengeporn.org/revenge-porn-laws/ (last visited Aug. 5, 2015) (referencing Cal. Penal Code § 647(j)(4)).

146. Clark v. McLane, 86 A.3d 655 (Me. 2014) (interpreting "abuse" under Me. Rev. Stat. Ann. tit. 19-A, § 4002).

As restrictions of speech, such laws are subject to challenge on First Amendment grounds. The U.S. Court of Appeals for the First Circuit upheld a conviction under a federal law criminalizing cyberstalking, where the defendant posted sexually explicit videos of a victim on pornography websites without her permission, against a First Amendment challenge.[147] The court decided that the statute was not unconstitutionally overbroad, and that defendant had waived any argument that it was impermissibly vague.[148]

VI. Conclusion

Social media continues to develop and businesses continue to innovate new ways to communicate. Legislatures and courts will need to address the issues these new technologies present. As evidenced by the developments discussed in this survey, lawmakers may struggle to catch up to the pace of innovation. Practitioners should work to stay abreast of changes in the law, but should also consider the potential legal consequences of new technologies as they emerge in the marketplace.

147. United States v. Sayer, 748 F.3d 425, 427–28 (1st Cir. 2014) (interpreting 18 U.S.C. § 2261A(2)(A)).

148. *Id*. at 435–36. The Ninth Circuit upheld the same statute against both overbreadth and vagueness challenges. United States v. Osinger, 753 F.3d 939, 940–41 (9th Cir. 2014).