The Computer & Internet Lawyer

Volume 36 ▲ Number 5 ▲ MAY 2019

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

The (Social) Media Is the Message: *Navigating Legal and Reputational Risks Associated with Employee Social Media Use*

By James A. Sherer, Melinda L. McLellan & Brittany A. Yantis

Defining the World of Social Media Interactions

This discussion of the risks associated with social media begins with a common definition that should be helpful for those executives who "aren't familiar with social media" or associate it with "fear."[1] To distill it to a "tweet,"[2] Google's suggestion is as good as any: "Web sites and applications that enable users to create and share content or to participate in social networking."[3] But a broad focus on "social media" is little help for organizations that want to—or are required to[4]—be active participants in its use. In order to engage in affirmative practices, and to carefully consider actual risks and benefits to an organization, that organization and its practitioners must start with the social media outlets the organization and its employees already use or are likely to use in the future, and subsequently, address what populations of individuals, both within and without the organization, are going to be engaged. This will define the actual universe of social media quarry the organization is targeting and will lead to better results with less tail-chasing.

This consideration begins with the platform. There are plenty, but even within a single branded platform, there may be markedly different lines of service and still more varied ways of using those, depending on the audience and the technology. In broad strokes, then, many practitioners break down the marketplace into different segments comprised of such ideas as "online communities"[5] which include the social networking sites, or even dating sites. These online communities may also be built into existing commercial applications, such as the feedback most online platforms offer to customers when browsing merchandise; Amazon's extensive use of customer ratings[6] is a prime example. Other sites may be considered microblogs, where the involvement—at least from post to post—is much less involved. Examples may

James A. Sherer and **Melinda L. McLellan** both serve as partners and **Brittany A. Yantis** as an associate at BakerHostetler. The views expressed herein are solely those of the authors; they should not be attributed to their places of employment, colleagues, or clients; and they do not constitute solicitation or the provision of legal advice. This article revisits and refreshes the subject matter originally covered in J. Sherer & M. McLellan, "Like *This*, Not *That* – Mitigating Corporate Social Media Engagement Risks," *The Computer & Internet Lawyer*, Vol. 32 No. 8 (2015).

include communication sites such as Twitter; video and picture-sharing applications; virtual worlds and social gaming sites;[7] dating sites; now-integrated platforms such as Yammer or Slack;[8] or even more focused sites such as Prezi,[9] which itself hosts a number of presentations on the phenomenon of social media,[10] or Discord, which focuses on Gamers.[11]

Using these groupings of technologies and audiences, the organization should first get to know and then build out policies for its selected platforms. Part of that knowledge will come from a careful consideration of what seems to integrate well with the organization's mission and its operation, but that presupposes a good articulation of what the organization wishes to accomplish on social media. There is still another set of considerations wrapped up in what is already happening on social media for most operations: Any baseline must start with considerations of what is already happening with the organization's presence, its brand, and its customers and employees. A true strategy needs to incorporate both; a responsible policy will do so as well.

Social Media Is an Organic Phenomenon and Stuff

Nearly every organization of every size already uses these platforms whether they know it or not. With seven out of 10 Americans using social media,[12] links between organizations and their employees and customers, regardless of whether intentionally planned, are immediate, widespread, and represent opportunity and risk bundled together in a potent package. Summed up in a story, when Chevrolet regional zone manager Rikk Wilde presented the World Series MVP award live on television and stated that the Chevy Colorado had "technology and stuff,"[13] Wilde became a short-lived legend. Wilde's comment was immediately picked up by Twitter users, and Chevrolet, closely following the (loosely defined) discourse, embraced the concept, engaged the #ChevyGuy and #TechnologyAndStuff Twitter hashtags,[14] and reaped, according to some estimates, around $5 million in free advertising before retiring the concept.[15]

"Buyer" Beware

The Wilde story shows how a potentially embarrassing situation for Chevrolet was transfigured into a windfall, but this is an exception to the rule. These sites have risk built into them as a design component for every user, including organizations, their employees, and their customers. Social media sites are not a public good that sprang out of the ether to be used with impunity. They are not *for* their users—they are *about* them. Users, including organizations, must be mindful of the adage that "if you're not paying for a product, then by default you are the product,"[16] and the caution that "the social media sites and data mining industry study online behavior and build manipulation machines designed to entice you to remain engaged and to divulge information."[17] As made clear by the recent scandals over the misuse of social media user data, the interests of mass media may not be the same as those of everyone else. These sites are set up to elicit rapid-fire responses and emotional reactions, and move to disseminate those, permanently and as quickly as possible, to a worldwide audience. This is a high-risk environment, and organizations have the burden of dealing with both first-instance (their own profiles, advertising efforts, and direct customer interaction) and second-instance (employees, customers, and third-party postings) issues in a rapidly developing space without a lot of history, case law, or direct analogues.

Employee Use of Social Media

There is an incredible breadth to the mischief employees can cause on social media platforms designed to record and amplify questionable decisions. A highly visible concern involves the ownership issues associated with sharing information online—and the incredible ease by which an employee can copy, sometimes edit, and then share a high-quality image or short (or lengthy) piece of writing with the world without a second thought. These actions may include sharing confidential information belonging to one's employer, ranging from proprietary diagrams to sales figures, from leaked product news and photographs to internal emails, thereby losing the protections associated with that information.[18] And depending on the considerations, this has encompassed material, inside information relevant to potential corporate deals or the movement of stocks.[19] This may be most evident in the public sphere, where public employees or officials, who are engaged in very serious matters on a daily basis but are still accustomed to using social media (such as Twitter) regularly to communicate with "friends" or "followers," often post material with little or no consideration as to who may have access to it or how it may be shared, following the "post first and think later" maxim.[20] Or it can even implicate national security, as then US Rep. Peter Hoekstra (R. MI) demonstrated when tweeting his "secret" trip to Iraq in early 2009.[21] Organizations contemplating similar concerns must be creative when considering exactly what employees might be up to, or should hedge their bets by implementing policies broad enough to cover otherwise unthinkable actions.

Intentional Social Media Use and Related Considerations

Some industries faced these issues sooner than others. A number of organizations are "required by statute to monitor employees' social media communications," and there are specific exemptions to some qualifiers regarding organizations' control over employees' use of social media in "the financial services sector," where many organizations in "banking, securities sales, and insurance are required to monitor certain employee's correspondence of all types with customers or prospective customers."[22] Others, such as General Motors,[23] are proactively engaged across the platforms and actively monitor mentions of their brands by their employees and the general public. But for every General Motors, there are many other organizations where social media considerations face challenges with active management and eschew a nuanced approach.[24]

Organizational social media adoption has proceeded at a slower pace than the viral growth seen in personal adoption figures. Even where tools such as Yammer are crafted specifically for internal consumption, they are used differently by individuals when employees are conscripted into their ranks and forced to adopt them.[25] These prior habits represent additional risk for an organization giving new sets of direction for the tools' use. An organization regulating social media use must be careful about how these adoptions are enforced and maintained, as evident by a wave of legislation that swept the United States beginning in 2013. Today, a total of 27 states and the District of Columbia[26] prohibit or restrict "employers from requesting access to an employee's private social media account."[27] Many of the laws overlap, with most of them prohibiting employers from seeking employees' social media account login information.[28] And two states, California[29] and New Jersey, prohibit employers from "shoulder surfing" or "making an employee access a personal account while management watches, from requiring an applicant or employee to change the privacy settings on a restricted account to a less-restrictive setting so that the employer can access it, or from forcing the employee to accept an employer's 'friend' request."[30]

Intentional uses also carry other attendant risks. Among them are organizational concerns regarding the ownership of their content—or content developed as part of a worker's employment with the organization—where the line between the organization, the worker posting the material, the worker's personality as an individual,[31] and the site on which the material is posted is blurred. These considerations may include the ownership of the social networking page itself,[32] as well as value developed from the use of social media, where the ownership of "contacts developed through the employee's use of social media" may be a matter of dispute after the employment relationship ends.[33] Finally, the organization must also worry about the other party to the social media interaction and how the organization's content, as disseminated to the world at large, may entertain the possibility of "genericide"—those instances when the brand name becomes the synonym for an entire class of product or service (think Xerox, Aspirin, or Zipper).[34]

Organic Organizational Social Media Use and Related Considerations

After safeguarding their own property, organizations must consider what their employees are doing with others' protected content or information. Just as employees can copy and share the organizations' information, they can do the same with others' data. These concerns may range from a disclosure of confidential information belonging to a joint venture partner or an unauthorized use of trademarks or copyright-protected works,[35] and may violate copyright law to the tune of treble damages and attorneys' fees.[36] There may be a disclosure of customer information—where posting or tweeting photos or videos of people (regardless of whether they are famous or private)[37] without permission can be a breach of privacy rights.[38] Even comments made regarding the organization posting the information may impact the copyright inherent in the authorship of the statements (as well as the manner in which the data is collected and its related consents).[39]

These concerns are not just with naive users; often marketers, who do have the most opportunity to work within these spaces at the direction or in the service of the organization, may be to blame when they "forget that the same laws and restrictions that apply to traditional advertising and promotion also apply to these new forms of promotion."[40] There may be a limited defense to these types of actions, however, if the Web site or service where copyright infringing material is posted offers a mechanism by which the copyright owner can request a "takedown" of the material under Section 512(c) of the Digital Millennium Copyright Act. The Web site asserting a defense under Section 512(c) must also avoid receiving a financial benefit attributable to the infringing material.[41]

Organic Employee Social Media Use and Related Considerations

Even if organizations are slow on the uptake at a corporate level, organic and individual-by-individual

uses of certain social media sites for work purposes are not. But these secondary uses of social media still carry requirements for proper use, especially in those instances where, instead of putting out a message on the platform, organizations are taking information in, relying on social media to make employment decisions (so-called cybervetting), or creating comprehensive background investigations that include the use of social media and other online resources.[42] This process has only accelerated with candidates' and applicants' use of LinkedIn or other similar sites.[43] Extensive sets of personal information for potential employees are only a click away. The ultimate implications for taking social networking information into account when making a hiring or firing decision are still unknown.[44] Concerns with these practices may implicate the use of "social media sites to discriminate against employees or potential employees."[45] Organizations must be aware of such concerns when recruiting employees through the use of targeted advertising and social media background checks, and should consider confining their searches to publicly available information, as more states are enacting laws to prohibit employers from requesting username and password information.[46] While there is no obvious solution to addressing these issues, it is clear that having no policy and no considerations is not going to provide a defense to related claims.

Within the strict business concerns associated with mobile applications for social media, for those organizations that are directing more of their customers to interact with them—or even pay for goods and services—across social media, those organizations must work to ensure interoperability across a variety of devices to first make sure their customers can use those platforms, and second, that ease of access across those platforms is a uniform experience. These can also implicate concerns regarding access for the disabled to the digital world, where commentators are beginning to look at the application of the Americans with Disabilities Act (ADA).[47] These arguments were first promoted in the world of the Internet; an early First Circuit decision, *Carparts Distribution Center*,[48] found that a "place" of public accommodation under Title III of the ADA did need not be a physical place, and in *National Federation of the Blind*,[49] the court found that there was a nexus between Target's stores and its Web site that obligated Target to make certain portions of its Web site accessible. However, guidance remains unclear, with the Ninth Circuit's 2015 unpublished opinion ruling that Netflix is not subject to the ADA because it has no physical place of business as an online video streaming service.[50]

A Special Note on Social Media-Based Threats

There are threats *from* or *associated with* social media writ broadly that we have discussed above, and then there are threats *on* social media with a smaller, but perhaps more serious, footprint. Within those practices or those instances where employees and managers make "discriminatory comments or use social media to harass employees," there may be organizational liability.[51] This is tricky, as defamatory content is often posted without a second thought,[52] and where with the click of a button, an insulting statement might instead live on in infamy instead of being relegated to the graveyard of bad decisions. Here, there may be a defense under Section 230 of the Communications Decency Act, where a Web site may be immune from the publication of information by a user—usually in the context of defamation, privacy, negligence, and other tort claims.[53] Posters beware, however; unlike those granted to social networking sites, there are no immunities afforded to users making inappropriate posts, and such users will face liability under laws associated with defamation and infringement.[54]

These threats can get quite serious, yet the law remains unclear what exactly comprises a threat conveyed across social media. In the 2015 *Elonis v. United States* case,[55] the Supreme Court addressed the questions of whether it was enough to show that a "reasonable person" would regard the statement as threatening, and whether a conviction of threatening another person under the appropriate federal rule[56] required proof of Elonis's subjective intent to threaten through his Facebook posts.

Both sides of the *Elonis* case presented compelling, modern arguments in the face of these new technologies. "Internet users may give vent to emotions on which they have no intention of acting, memorializing expressions of momentary anger or exasperation that once were communicated face-to-face among friends and dissipated harmlessly," read a brief filed on Elonis's behalf by the Student Press Law Center, the Electronic Frontier Foundation, and the writers' organization PEN.[57] In contrast, a brief filed by the National Network to End Domestic Violence highlighted individuals who "have experienced real-life terror caused by increasingly graphic and public posts to social media sites – terror that is exacerbated precisely because abusers now harness the power of technology, 'enabling them to reach their victims' everyday lives at the click of a mouse or the touch of a screen.'"[58]

Avoiding the potential First Amendment ramifications, the Court held as a matter of statutory interpretation that a conviction of threatening another person under the appropriate federal rule[59] required proof of

Elonis's subjective intent to threaten.[60] The Court further found that an objective standard would risk convicting innocent actors because the crucial element of this criminal behavior is the threat itself, not merely the posting of it.[61]

For organizations, the link to Elonis's behavior and other so-called cyberbullying issues (which include threats of violence; sending sexually explicit messages or photos; taking photos or videos of people in places where they would expect privacy; and stalking and hate crimes[62]) may not seem immediately evident. But when an organization's employee uses the organization's platform for a questionable and arguably threatening purpose, the line between the organization's profile and the employee's behavior may blur. There may be no agency on the part of the organization involved at all; at least one vendor has compiled data that indicates organizations' social media accounts, including those of the Fortune 100, are compromised every day.[63] But while it's unlikely that an organization would be held criminally liable for actions taken on its social media platforms, there may be civil remedies available for negligent monitoring (similar to the issues associated with genericide we discuss above), and there is certainly good reason for an organization to include terms of use and policies associated with threats and to keep an active watch for similar activity intentionally or accidentally placed on social media platforms in ways directly attributable or linked to the organization.

Summed and Additional Considerations for Organizational Social Media Policies

Policy considerations should begin with the points above and include the intent of the organization, the platforms it wishes to employ and a realization of what is already happening in the social media marketplace.[64] The additional policy considerations discussed above and outlined below can then be mapped, as applicable, to the different platforms and the types of engagement the organization makes plans for—understanding that flexibility should be key given the rapid and often exaggerated advances seen in the technologies.[65] This is by no means an exhaustive list, but it should spur discussion within the organization and encourage stakeholders to be more specific about how social media is currently, or could be, used for their divisions or parts of the organization and on organizational and employee devices:[66]

- Conduct a comprehensive preliminary assessment to determine every social media platform featuring representations of the organization or its brand and continue to evaluate and update at regular intervals;[67]
- Define what social media means for the organization, both in aspiration (the plan) and reality (what's already happening organically);
    - o Consider the use of internal social media platforms, such as Yammer or Slack, but understand that even "bulletin board-type" services may fall within certain policy definitions and should be evaluated, monitored, and directed accordingly.
    - o Educate executives and designate an executive-level "champion" for the inevitable reconsideration of the policy and the technology it encompasses.
- Determine who within the organization is responsible for monitoring social media as well as the intake of concerns (*e.g.*, marketing outreach opportunities; employee, customer, or third-party complaints);
    - o Determine a strategy to avoid genericide and related copyright considerations.
    - o Create an escalation path for certain types of sensitive inquiries and disclosures.
    - o Create an "after hours" protocol to address the inevitable night/weekend/holiday social media crises.[68]
- Determine who is responsible for maintaining social media under the organization's control;
    - o Define a policy on ownership.[69]
    - o Consider application of the Digital Millennium Copyright Act.[70]
    - o Consider application of the Americans with Disabilities Act.
    - o Consider industry-specific requirements for use and retention. Electronic discovery concerns have been a part of this system for nearly as long as social media has been available as a sharing mechanism. While court rules and practices "generally lag behind the actual technology employed,"[71] social media is an active part of current electronic discovery requests.
    - o Consider attribution disclaimers, the review of all content before its release, screening of

third-party content for copyright permission issues and obtaining appropriate releases.[72]

- o If photographs or descriptions of identifiable individuals are used, consider how social media use of these likenesses without permission may infringe privacy rights.[73]

- o Consider endorsements, where the Federal Trade Commission (FTC) may require the disclosure of any payments or consideration regarding specific types of information.[74] The FTC has provided some guidance on these points through its Fair Information Practice Principles,[75] as well as some information on the use of endorsements and testimonials.[76]

- Determine how employees must or may use social media in reference to the organization; and

  - o Consider jurisdictional prohibitions against control by the organization where it may impinge on union, contract, free speech or other considerations.

  - o Consider addressing the issue of whether an employee is making statements in his or her capacity as an employee or agent for the organization or as a private citizen, which may be especially concerning in instances where the employer is a government agency.[77]

  - o Consider simple rules of thumb well, such as "if it has anything to do with [individuals'] medical, financial or sex lives, don't talk about it on social media."[78]

- Determine how employees may use social media in service to the organization.

  - o Discuss cybervetting and its related behaviors.

  - o Don't use location features or "check-ins" if it could compromise employee safety and privacy, whether dropping off money after hours or traveling to remote locations.[79]

Notes

1. B. Rathjens, Top Reasons Hospitals & Healthcare Organizations Are Slow to Social Media Adoption, Afia Health (Aug. 25, 2014).
2. Twitter, *New user FAQs*, *see https://help.twitter.com/en/new-user-faq* ("What's a Tweet? A Tweet is any message posted to Twitter which may contain photos, videos, links and text.").
3. Google, *so•cial me•di•a*, *see https://www.google.com/#q=social+media+definition*.
4. Federal Depository Trust Corporation, *Social media – Consumer Compliance Risk Management Guidance*, FIL-56-2013 (Dec.11, 2013), *see https://www.fdic.gov/news/news/financial/2013/fil13056.html#cont*.
5. K. L. Ossian, *Legal Issues in Social Networking*, Institute of Continuing Legal Education (May 2009).
6. About Comments, Feedback, & Ratings, *see https://www.amazon.com/gp/help/customer/display.html?nodeId=537806* (last visited Nov. 26, 2018).
7. Federal Depository Trust Corporation, *supra* n.4.
8. K. Shelton, *Workplace by Facebook, Slack, or Yammer: What Is the Best Office Collaboration Tool*? Social Media Week (July 2, 2018); S. Rosenbush & C. Boulton, "As Facebook Goes Parabolic, Social Media Adoption at Work Is Slower Affair," *The Wall Street Journal – CIO Journal* (July 24, 2014), *see http://blogs.wsj.com/cio/2014/07/24/as-facebook-goes-parabolic-social-media-adoption-at-work-is-slower-affair*; J. Sherer, A. Singer & S.B. Barnes, *Picking Up the Slack – Legal and Information Governance Considerations for New(er) Technologies*, Capstone Legal Conference on E-Discovery – National Law School of India University, Bangalore (Dec. 1, 2018).
9. A. Levy, "Trial by Twitter," *The New Yorker* (Aug. 5, 2013).
10. C. Conway, *Ins & Outs of Social Media*, Prezi (Dec. 1, 2014), *see https://prezi.com/jjgvq1gattpt/ins-outs-of-social-media*.
11. Discord, We built Discord to bring gamers together (undated), *see https://discordapp.com/company*.
12. Pew Research Center, *Social Media Fact Sheet* (Feb. 5, 2018), *see http://www.pewinternet.org/fact-sheet/social-media/*.
13. B. Shea, "Social Media Key Tools for Building Brands, but Companies Must Exercise Caution," *Crain's Detroit Business* (Dec. 21, 2014), *see http://www.crainsdetroit.com/article/20141214/NEWS/312149985/social-media-key-tools-for-building-brands-but-companies-must*.
14. Wikipedia, *Hashtag* ("A type of metadata tag used on social networks such as Twitter and other microblogging services, allowing users to apply dynamic, user-generated tagging, which makes it possible for others to easily find messages with a specific theme or content. Users create and use hashtags by placing the number sign or pound sign "#" – usually in front of a word or phrase…"), *see http://en.wikipedia.org/wiki/Hashtag* (last visited Nov. 26, 2018).
15. M. Colias, "Chevy Retires 'Technology and Stuff' after Reaping Publicity Windfall," *Automotive News* (Nov. 7, 2014), *see http://www.autonews.com/article/20141107/RETAIL03/141109854/chevy-retires-technology-and-stuff-after-reaping-publicity-windfall*.
16. B. Kepes, "Google Users – You're The Product, Not The Customer," *Forbes Tech* (Dec. 4, 2013, 3:19PM), *see http://www.forbes.com/sites/benkepes/2013/12/04/google-users-*

youre-the-product-not-the-customer/; *see In re Google, Inc. Privacy Policy Litig.*, No. 12-CV-01382, 2013 WL 6248499, at *2 (N.D. Cal. Dec. 3, 2013) (Mag. J. P.S. Grewal) (finding "Google still manages to turn a healthy profit by selling advertisements within its products that rely in substantial part on users' personal identification information […]. As some before have observed, in this model, the users are the real product.").

17. T.F. Claypoole, "Privacy and Social Media," American Bar Association, *Business Law Today* (2013).
18. B. Shea, *supra* n.12.
19. Neal & McDevitt, *Top 10 Legal Issues in Social Media*, Intellectual Property & Marketing Attorneys (2010).
20. M. Pettry, "Social Media – Legal Challenges and Pitfalls for Law Enforcement Agencies," *FBI Law Enforcement Bulletin* (Dec. 9, 2014), *see http://leb.fbi.gov/2014/december/legal-digest-social-media-legal-challenges-and-pitfalls-for-law-enforcement*.
21. R. Needleman, *Congressman twitters secret trip to Iraq*, CNET (Feb. 11, 2009), *see http://www.cnet.com/news/congressman-twitters-secret-trip-to-iraq/*.
22. Claypoole, *supra* n.16; see also Federal Depository Trust Corporation, *supra* n.4.
23. V. Goel, "G.M. Uses Social Media to Manage Customers and Its Reputation," *The New York Times* (Mar. 23, 2014), *see http://www.nytimes.com/2014/03/24/business/after-huge-recall-gm-speaks-to-customers-through-social-media.html?_r=0* ("G.M. has a team of about 20 people based in Detroit that manages its social media presence – including monitoring about 100 independent auto forums.").
24. VMTyler, *Why Your Company Sucks at Social Media*, VMTyler.com (Sept. 22, 2014), *see https://vmtyler.com/why-your-company-sucks-at-social-media/*.
25. Rosenbush and Boulton, *supra* n.8.
26. *State Social Media Privacy Laws*, National Conference of State Legislatures (Nov. 6, 2018), *see http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx*.
27. T. Traylor-Notaro, "Workplace Privacy in the Age of Social Media," 7 *Global Bus. L. Rev*. 133, 134 (2018).
28. *Id*. at 143.
29. *Id*. at 145.
30. Claypoole, *supra* n.16.
31. See *PhoneDog LLC v. Noah Kravitz*, No. C 11-03474, 2011 WL 5415612, (N.D. Cal. July 15, 2011).
32. Ossian, *supra* n.5.
33. H. Bussing, "Social Media's Real Legal Issues," *HRExaminer* (Mar. 25, 2013), *see http://www.hrexaminer.com/social-medias-real-legal-issues/*.
34. D. Klemchuk, *Navigating the Legal Issues Surrounding Social Media*, Klemchuk Kubasta LLP, (2012), *see http://www.kk-llp.com/133-Navigating-the-Legal-Issues-Surrounding-Social-Media*.
35. Neal & McDevitt, *supra* n.18.
36. US Copyright Act, 17 U.S.C. Section 101, et. seq., *see https://www.copyright.gov/title17/* (last visited Nov. 26, 2018).
37. A. Lustigman & S. Anand, *Legal pitfalls in utilizing intellectual property in social media*, InsideCounsel (Dec. 9, 2014); see also *Heigl v. Duane Reade, Inc.*, 14 C.V. 2502 (S.D.N.Y. complaint filed Apr. 9, 2014) (April 2014 incident in which Duane Reade posted a photo of Katherine Heigl leaving a Duane Reade and was promptly sued).
38. Ossian, *supra* n.5.
39. *Id*.
40. Lustigman and Anand, *supra* n.36.
41. K. Fayle, *Understanding the Legal Issues for Social Networking Sites and Their Users*, FindLaw (Mar. 11, 2014), *see http://technology.findlaw.com/modern-law-practice/understanding-the-legal-issues-for-social-networking-sites-and.html*.
42. Pettry, *supra* n.19.
43. Neal & McDevitt, *supra* n.18.
44. Ossian, *supra* n.5.
45. Klemchuk, *supra* n.33.
46. L. Gingeleskie, *Social Media in the Hiring Process: Pitfalls and Protections* (Mar. 20, 2018), *see https://www.law.com/njlawjournal/2018/03/20/social-media-in-the-hiring-process-pitfalls-and-protections/?slreturn=20181026171048*.
47. D. Goldstein & G. Care, *Disability Rights and Access to the Digital World*, Disability Rights Education & Defense Fund (2012), *see http://dredf.org/media-disability/disability-rights-and-access-to-the-digital-world/*.
48. *Carparts Distribution Center Inc. v. Automobile Wholesaler's Ass'n of New England Inc.*, 37 F.3d 12 (1994).
49. *Nat'l Fed. of the Blind v. Target Corp*., 452 F. Supp. 2d 946 (N.D. Cal. 2006).
50. E. Griffin, *Americans with Disabilities Act (ADA) and Web Accessibility Requirements for Video* (Jan. 4, 2018), *see https://www.3playmedia.com/2016/03/02/americans-with-disabilities-act-ada-and-web-accessibility-requirements-for-video/*; *Cullen v. Netflix, Inc.*, 2015 U.S. App. LEXIS 5257 (9th Cir. Apr. 1, 2015).
51. Bussing, *supra* n.32.
52. Neal & McDevitt, *supra* n.18.
53. Fayle, *supra* n.40.
54. *Id*.
55. *Elonis v. United States*, 135 S.Ct. 2001 (2015).
56. Interstate Communications Act, 18 U.S.C. § 875(c) (1948).
57. Student Press Law Center, the Electronic Frontier Foundation and PEN American Center, *Amicus Brief for Elonis v. United States* (Aug. 22, 2014), *see https://www.eff.org/files/2014/08/25/elonis_filed_amicus_brief.pdf*.
58. National Network to End Domestic Violence, *Amicus Brief for Elonis v. United States* (Oct. 6, 2006), *see http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/BriefsV4/13-983_resp_amcu_nnedv-etal.authcheckdam.pdf*.
59. Interstate Communications Act, 18 U.S.C. § 875(c) (1948).
60. *Elonis*, 135 S.Ct. at 2012.
61. *Id*. at 2009.

62. StopBullying.gov, Report Cyberbullying, *see http://www.stopbullying.gov/cyberbullying/how-to-report/* (last visited Nov. 26, 2018).
63. Proofpoint, *Fortune 100 Social Media Accounts Are Compromised Every Business Day, Proofpoint Research Reveals* (Dec. 10, 2014).
64. M. McLellan & J. Sherer, "Corporate Social Media Engagement – Guidelines and Strategies for Managing Unpredictability," *Bloomberg BNA – Electronic Commerce & Law Report*, Vol. 20, No. 31 (2015).
65. J. Sherer & M. McLellan, "Like This, Not That – Mitigating Corporate Social Media Engagement Risks," *The Computer & Internet Lawyer,* Vol. 32 No. 8 (2015).
66. E. Fedeles, J. Sherer & J. Selby, "Bring Your Own Device Policy Language and Considerations for HR, Legal, IT and Facilities Stakeholders," *Bloomberg BNA Digital Privacy and Security Law Report*, 15 PVLR 279 (2016).
67. McLellan and Sherer, *supra* n.63.
68. *Id.*
69. Klemchuk, *supra* n.33.
70. Pub. L. 105-304, 112 Stat. 2860 (1998).
71. Neal & McDevitt, *supra* n.18.
72. Ossian, *supra* n.5.
73. McLellan and Sherer, *supra* n.63.
74. Neal & McDevitt, *supra* n.18.
75. Fair Information Practice Principles, FTC, *see http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.*
76. FTC Guidelines Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.
77. Pettry, *supra* n.19.
78. Bussing, *supra* n.32.
79. *Id.*