2

Social Media's Not For You—It's About You: Risk Considerations for Organizations and Practitioners in Yet Another Age of Uncertainty (January 2, 2015)

James A. Sherer
Melinda L. McLellan

Baker & Hostetler LLP

This paper was authored on January 2, 2015 as a submission to the Practicing Law Institute—Ethics in Social Media 2015 Seminar, March 16, 2015.

James A. Sherer & Melinda L. McLellan both serve as Counsel 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.

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 and others who "aren't familiar with social media" or even "fear" it.[1] To distill the social media universe to a "tweet,"[2] Google's description works as well as any: "websites and applications that enable users to create and share content or to participate in social networking."[3] But a broad focus on "social media" does little to help organizations that want—or are required to be[4]—actively involved in its use. Affirmatively establishing best practices that are rooted in thoughtful consideration of the actual risks and benefits to the organization starts with assessing which social media outlets the organization and its employees already use or are likely to use in the future, and determining which populations (both internal and external) will be engaged. This analysis will help the organization narrow the social media universe to specific targets, resulting in better outcomes with less tail-chasing.

The initial consideration focuses on the platform. There are plenty, but even within a single branded platform, there may also be markedly different lines of service and still more varied ways of using those products depending on the audience and the technology. To narrow the scope, many practitioners divide the marketplace into different segments comprised of conceptual frameworks such as the "online communities" of Facebook, LinkedIn, Reddit, or even dating services like Match.com or eHarmony.[5] These online communities may be built into existing commercial applications—for example, most online platforms offer customers feedback forums to facilitate online shopping; Amazon's extensive use of customer

1. B.Rathjens, *Top Reasons Hospitals & Healthcare Organizations are Slow to Social Media Adoption*, Afia Health (Aug. 25, 2014), http://www.afiahealth.com/healthcare-is-slow-to-social-media-adoption/.
2. Twitter, *New user FAQs*, https://support.twitter.com/articles/13920-new-user-faqs# ("What's a Tweet? A Tweet is any message posted to Twitter which may contain photos, videos, links and up to 140 characters of text.").
3. Google, *so•cial me•di•a*, 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) 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) http://0384058.netsolhost.com/wp-content/uploads/2013/10/Legal-Risks-of-Social-Media.pdf.

ratings[6] is a prime example. The services offered by other social media sites often are referred to as "microblogs,"[7] where the time investment—at least from post-to-post—is much less extensive. Examples may include sites like Twitter; video and picture sharing applications like YouTube, Instagram, Pintrest, Tumblr, FourSquare, Vine, and Flickr; "quicker" dating sites like Tinder, HowAboutWe and Hinge; now-integrated platforms like Yammer;[8] or even more focused sites like Prezi,[9] which itself hosts a number of presentations on various Social Media phenomena.[10] On the opposite side of the spectrum are virtual worlds like SecondLife and social gaming sites such as FarmVille (that may absorb significant amounts of user engagement).[11]

Using these groupings of technologies and audiences, the organization should educate itself before building out policies for the relevant platforms. Part of that process must involve careful consideration of what integrates well with the organization's mission and its operations, but the first step is clearly articulating what the organization seeks to accomplish through its use of social media. Yet another set of considerations must take into account what is already happening with the organization in terms of its social media presence with respect to its brand, its customers, and its employees. An effective strategy needs to incorporate both; a responsible policy will as well.

SOCIAL MEDIA IS AN ORGANIC PHENOMENON – AND STUFF

Nearly every organization of every size uses social media platforms whether the organization is aware of its involvement or not. With nearly

6. Amazon Seller Rating Help, http://www.amazon.com/gp/help/customer/display.html/ref=sm_xx__xx?ie =UTF8&nodeId=201066530 (last visited Jan. 2 ,2015).
7. J.M. Brody & S.A. Shah, *Navigating legal Issues in the Twittersphere*, Manatt Digital Media (Nov. 18, 2014) http://www.manattdigitalmedia.com/navigating-legal-issues-in-the-twittersphere/#sthash.2QggD8QJ.dpbs.
8. 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) http://blogs.wsj.com/cio/2014/07/24/as-facebook-goes-parabolic-social-media-adoption-at-work-is-slower-affair/.
9. A. Levy, *Trial by Twitter*, The New Yorker (Aug. 5, 2013) http://www.newyorker.com/magazine/2013/08/05/trial-by-twitter.
10. C. Conway, *Ins & Outs of Social Media*, Prezi (Dec. 1, 2014) https://prezi.com/jjgvq1gattpt/ins-outs-of-social-media/.
11. Federal Depository Trust Corporation, Social media – *Consumer Compliance Risk Management Guidance*, FIL-56-2013 (Dec. 11, 2013) https://www.fdic.gov/news/news/financial/2013/fil13056.html#cont.

75% of adults 18 or older in the United States using some form of social media,[12] links between organizations and their employees and customers, regardless of intentionality, are immediate, widespread, and represent both opportunity and risk bundled together in a potent package. To offer but one relevant anecdote, when Chevrolet regional zone manager Rikk Wilde presented the MLB 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 snarky Twitter users, but Chevrolet, closely following the (loosely defined) discourse, embraced the attention and promoted engagement with the #ChevyGuy and #TechnologyAndStuff Twitter hashtags,[14] reaping, 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 turned into a windfall, but such good fortune is an exception to the rule. Social media sites have risk built into them as a design component for every user, including organizations, their employees, and their customers. They are not a public good that sprang out of the ether to be used with impunity. These sites 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 caveat that, "the social media sites and data mining

12. M. Duggan and A. Smith, Pew Research Center, *Social Media Update 2013* (Dec. 30 2013), http://pewinternet.org/Reports/2013/Social-Media-Update.aspx.
13. B. Shea, *Social media key tools for building brands, but companies must exercise caution*, Crain's Detroit Business (Dec. 21, 2014) http://www.crainsdetroit.com/article/20141214/NEWS/312149985/social-media-key-tools-for-building-brands-but-companies-must.
14. Wikipedia, *Hashtag* (Hashtags in the Twitter context are words or unspaced phrases prefixed with a "#" to form a metadata tag) http://en.wikipedia.org/wiki/Hashtag (last visited Jan. 1, 2014).
15. M. Colias, *Chevy retires 'technology and stuff' after reaping publicity windfall*, Automotive News (Nov. 7, 2014)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) http://www.forbes.com/sites/benkepes/2013/12/04/google-users-youre-the-product-not-the-customer/. *See also In re Google, Inc. Privacy Policy Litig.*, No. 12-CV-01382, 2013 WL 6248499, at *2 (N.D. Cal. Dec. 3, 2013) (Mag. J.

industry study online behavior and build manipulation machines designed to entice you to remain engaged and to divulge information."[17] These sites are set up to elicit rapid fire responses and emotional firestorms, and then disseminate those reactions quickly and permanently to a world-wide audience. This is not a low-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 constantly-evolving space that offers very little in the way 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 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, from proprietary diagrams to sales figures, from leaked product news and photographs to internal emails, and 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 law enforcement employees, who are engaged in very serious matters on a daily basis but are still accustomed to using social media 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

---

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) http://www.americanbar.org/publications/blt/2014/01/03a_claypoole.html.
18. Shea, *supra*. note 13.
19. Neal & McDevitt, *Top 10 Legal Issues in Social Media*, Intellectual Property & Marketing Attorneys (2010) http://www.nealmcdevitt.com/assets/news/Top_10_Social_Media_Legal_Issues_FINAL.PDF.

the "post first and think later" maxim.[20] Or it can even implicate national security, as U.S. Representative Peter Hoekstra 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 and were forced to adapt. These included organizations that are "required by statute to monitor employees' social media communications." Where there are laws regarding social media use, there are requirements for organizational control over employees' use of social media, such as 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] For others, such as General Motors,[23] the lines are blurrier, and approaches to proactive engagement across social media platforms and active monitoring of mentions of brands by their employees and the general public can vary. And there is a third category, where for every General Motors, there are many other organizations without a consistent or nuanced approach that engage in *ad hoc* or reactionary strategies.[24]

This reactionary approach can happen both quicker and slower than an organization might like. Certainly organizational social media adop-

---

20. M. Pettry, *Social Media – Legal Challenges and Pitfalls for Law Enforcement Agencies*, FBI Law Enforcement Bulletin (Dec. 9, 2014) 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) http://www.cnet.com/news/congressman-twitters-secret-trip-to-iraq/.
22. Claypoole, *supra*. note 17; *see also* Federal Depository Trust Corporation, *Social media – Consumer Compliance Risk Management Guidance*, FIL-56-2013 (Dec. 11, 2013) https://www.fdic.gov/news/news/financial/2013/fil13056.html#cont.
23. V. Goel, *G.M. Uses Social Media to Manage Customers and Its Reputation*, The New York Times (Mar. 23, 2014) 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) https://vmtyler.com/why-your-company-sucks-at-social-media/.

tion has proceeded at a slower pace than the viral growth seen in personal adoption figures. Even where tools like Yammer are crafted specifically for internal consumption, they are used differently by employees when used as part of a forced adoption of executive policy.[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 or continuations of use are enforced and maintained, as evident by a wave of legislature that swept the United States in 2013, prohibiting or restricting "employers from demanding access to their employees' social media sites when those sites are not fully public."

At least one state, New Jersey, already prohibits 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 by forcing the employee to accept an employer's 'friend' request."[26] This trend continued into 2014, with additional regulations addressing "what social media information current and prospective employees should be required to give employers."[27] Organizations should not be surprised if unions or other contractual partners demand further autonomy in this space in the very near future.

Intentional uses also carry other attendant risks. Among them are concerns regarding the ownership of the organization's content—or content developed as part of a worker's employment with the organization where the lines between the organization, the worker posting the material, the worker's personality as an individual,[28] and the site on which the material is posted, are blurred. These considerations may include the ownership of the social networking page itself,[29] as well as the value developed from the use of social media. The ownership of "contacts developed through the employee's use of social media" may be disputed after the employment relationship ends.[30] The organization must also

25. Rosenbush & Boulton, *supra*. note 9.
26. Claypoole, *supra*. note 17.
27. B. Luschen, *New Law Protects Privacy of Employee Social Media*, KGOU NPR Network (Nov. 11, 2014) http://kgou.org/post/new-law-protects-privacy-employee-social-media.
28. *See PhoneDog LLC v. Noah Kravitz*, No. C 11-03474, 2011 WL 5415612, (N.D. Cal. July 15, 2011).
29. Ossian, *supra*. note 5.
30. H. Bussing, *Social Media's Real Legal Issues*, HRExaminer (Mar. 25, 2013) http://www.hrexaminer.com/social-medias-real-legal-issues/.

contemplate other participants on the social media platform 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).[31]

ORGANIC ORGANIZATIONAL SOCIAL MEDIA USE AND RELATED CONSIDERATIONS

After safeguarding its own property, an organization must consider what its 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'. These concerns may include a disclosure of confidential information belonging to a joint venture partner or an unauthorized use of trademarks or copyright-protected works,[32] and may violate copyright law to the tune of treble damages and attorneys' fees.[33] 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)[34] without permission can breach of privacy rights.[35] Even posting comments made regarding the organization may impact the copyright inherent in the authorship of the comments (as well as the manner in which the data is collected and its related consents).[36]

These concerns are not unique to naïve 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

---

31. D. Klemchuk, *Navigating the Legal Issues Surrounding Social Media*, Klemchuk Kubasta LLP, (2012) http://www.kk-llp.com/133-Navigating-the-Legal-Issues-Surrounding-Social-Media.
32. Neal & McDevitt, *supra.* note 19.
33. U.S. Copyright Act, 17 U.S.C. Section 101, et. seq. http://www.copyright.gov/title17/ (last visited Jan. 2, 2015).
34. A. Lustigman & S. Anand, *Legal pitfalls in utilizing intellectual property in social media*, InsideCounsel (Dec. 9, 2014) http://www.insidecounsel.com/2014/12/09/legal-pitfalls-in-utilizing-intellectual-property. *See also Heigl v. Duane Reade, Inc.*, 14 C.V. 2502 (S.D.N.Y. complaint filed Apr. 9, 2014) (April, 2014 incident where Duane Reade posted a photo of Katherine Heigl leaving a Duane Reade and was promptly sued).
35. Ossian, *supra*. note 5.
36. *Id.*

and promotion also apply to these new forms of promotion."[37] There may be a limited defense to these types of action, however, if the website 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 website asserting a defense under 512 (c) must also avoid receiving a financial benefit attributable to the infringing material.[38]

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 releasing a message on the platform, organizations are absorbing information by 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 on-line resources.[39] This process has only accelerated with candidates' and applicants' use of LinkedIn, Monster, or other similar sites.[40] The ultimate implications of considering social networking information when making a hiring or firing decision are still unknown.[41] But concerns with these practices have referenced the use of "social media sites to discriminate against employees or potential employees."[42] Although there is no obvious solution to addressing these issues, it is clear that having no policy or guidelines in place is unlikely to provide a defense to related claims.

Within the strict business concerns associated with mobile applications for social media, for those organizations who 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

37. Lustigman & Anand, *supra*. note 34.
38. K. Fayle, *Understanding the Legal Issues for Social Networking Sites and Their Users*, FindLaw (Mar. 11, 2014) http://technology.findlaw.com/modern-law-practice/understanding-the-legal-issues-for-social-networking-sites-and.html.
39. Pettry, *supra*, note 20.
40. Neal & McDevitt, *supra.* note 19.
41. Ossian, *supra*. note 5.
42. Klemchuk, *supra*. note 31.

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").[43] These arguments were first promoted in the world of the internet; an early First Circuit decision, *Carparts Distribution Center*,[44] 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*,[45] the court found that there was a nexus between Target's stores and its website that obligated Target to make certain portions of its website accessible.

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.[46] This is tricky, as defamatory content is often posted without a second thought,[47] 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 website may be immune from the publication of information by a user—usually in the context of defamation, privacy, negligence, and other tort claims.[48] Posters should 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.[49]

---

43. D. Goldstein & G. Care, *Disability Rights and Access to the Digital World*, Disability Rights Education & Defense Fund (2012) http://dredf.org/media-disability/disability-rights-and-access-to-the-digital-world/.
44. *Carparts Distribution Center Inc. v. Automobile Wholesaler's Ass'n of New England Inc.*, 37 F.3d 12 (1994).
45. *Nat'l Fed. of the Blind v. Target Corp*., 452 F. Supp. 2d 946 (N.D. Cal. 2006).
46. Bussing, *supra*. note 30.
47. Neal & McDevitt, *supra.* note 19.
48. Fayle, *supra*. note 38.
49. *Id.*

These threats can get quite serious, and the United States Supreme Court is considering exactly what comprises a threat conveyed across social media through the a 3rd Circuit case *Elonis v. United States*.[50] Here, the Supreme Court Justices considered whether convicting Elonis of threatening another person required proof of Elonis's *subjective* intent to threaten through his Facebook posts, or whether it was enough to show that a "reasonable person" would regard the statement as threatening; and whether, as a matter of statutory interpretation, a conviction of threatening another person under the appropriate federal rule[51] required proof of Elonis's subjective intent to threaten.

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.[52] 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 Facebook and other 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.'"[53] The Supreme Court heard arguments in December of 2014, and will decide whether to uphold Elonis's conviction sometime in 2015.

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 a places where they would expect privacy; and stalking and hate crimes[54]) may not seem immediately evident. But when an organization's employee uses the organization's platform for a questionable and arguably threatening

---

50. *Elonis v. United States*, 134 S.Ct. 2819 (2014).
51. Interstate Communications Act, 18 U.S.C. § 875(c) (1948).
52. Student Press Law Center, the Electronic Frontier Foundation and PEN American Center, *Amicus Brief for Elonis v. United States* (Aug. 22, 2014) https://www.eff.org/files/2014/08/25/elonis_filed_amicus_brief.pdf.
53. National Network to End Domestic Violence, *Amicus Brief for Elonis v. United States* (Oct. 6, 2006) http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/BriefsV4/13-983_resp_amcu_nnedv-etal.authcheckdam.pdf.
54. StopBullying.gov, Report Cyberbullying, http://www.stopbullying.gov/cyberbullying/how-to-report/ (last visited Jan. 2, 2015).

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.[55] But although it is 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" discussed above) and there is certainly good reason for an organization to include terms of use and policies associated with threats, and to be vigilant about monitoring for similar activity that may, intentionally or accidentally, show up on social media platforms in a manner that is either directly attributable to, or otherwise linked with 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 an appreciation of its current state of social media engagement. 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 is contemplating—understanding that flexibility should be key given the rapid and often unpredictable advances in these types of technologies. This list 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.

- Define what social media means for the organization, both in aspiration (the plan) and reality (what's already happening organically).
    - Consider the use of internal social media platforms, such as Yammer, but understand that even "bulletin board" type services may fall within certain policy definitions and should be evaluated, monitored, and directed accordingly.

55. Proofpoint, *Fortune 100 Social Media Accounts Are Compromised Every Business Day, Proofpoint Research Reveals* (Dec. 10, 2014) http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=887048.

- 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).
  - Determine a strategy to avoid "genericide" and related copyright considerations.
  - Create an escalation path for certain types of sensitive inquiries and disclosures.
- Determine who is responsible for maintaining social media under the organization's control
  - Define a policy on ownership.[56]
  - Consider application of the Digital Millennium Copyright Act.[57]
  - Consider application of the Americans with Disabilities Act.
  - 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,"[58] social media is an active part of current electronic discovery requests.
  - Consider attribution disclaimers, the review of all content before its release, screening of third party content for copyright permission issues and obtaining appropriate releases.[59]
  - Consider endorsements, where the FTC may require the disclosure of any payments or consideration regarding specific types of information.[60] The FTC has provided some guidance

56. Klemchuk, *supra*. note 31.
57. Pub. L. 105-304, 112 Stat. 2860 (1998).
58. Neal & McDevitt, *supra.* note 19.
59. Ossian, *supra*. note 5.
60. Neal & McDevitt, *supra.* note 19.

on these points through its Fair Information Practice Principles,[61] as well as some information on the use of endorsements and testimonials.[62]

- Determine how employees must or may use social media in reference to the organization.
  - Consider jurisdictional prohibitions against control by the organization where it may impinge on union, contract, free speech, or other considerations.
  - Consider addressing the issue of whether an employee is making statements in their 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.[63]
  - 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."[64]
- Determine how employees may use social media in service to the organization.
  - Discuss "cybervetting" and its related behaviors.
  - Don't use location features or "check-ins" unless there are clearly-defined reasons for doing so, especially if they could compromise employee safety, whether dropping off money after hours, or traveling to remote locations.[65]

---

61. Fair Information Practice Principles, FTC, available at http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.
62. FTC Guidelines Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.
63. Pettry, *supra*, note 20.
64. Bussing, *supra*. note 30.
65. *Id.*