Marketing Through Social Networks: Business Considerations--From Brand to Privacy

Katheryn A. Andresen

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation
Available at: http://open.mitchellhamline.edu/wmlr/vol38/iss1/10
MARKETING THROUGH SOCIAL NETWORKS:
BUSINESS CONSIDERATIONS—
FROM BRAND TO PRIVACY

Katheryn A. Andresen†

I. INTRODUCTION .............................................................. 291
II. THE EXPANSION OF SOCIAL NETWORKS ......................... 293
   A. From Playground to Credible Business .................... 293
   B. Target Market Expansion ..................................... 296
III. THE APPLICATION OF SOCIAL NETWORKS TO BUSINESS
     (I.E., MARKETING ALTERNATIVES) .......................... 297
     A. Business Identification of Market Opportunities .......... 298
     B. Application Development .................................. 300
     C. Expansion of Business Through Social Networks ....... 302
        1. Target Marketing .......................................... 302
        2. Expansion of Companies’ Goods/Services ............... 304
IV. RISKS ASSOCIATED WITH MARKETING THROUGH SOCIAL
    NETWORKS ................................................................. 305
    A. Business Risks and Strategies to Avoid Such Risks ....... 306
       1. Effect on Brand .............................................. 306
       2. Control of Company Image/Position ...................... 309
       3. Premature Release of New Products/Services .......... 310
    B. Legal Risks ....................................................... 311
       1. Compliance Consideration with Company Policies .... 311
       2. Loss of Intellectual Property ............................... 313
       3. Liability Issues .............................................. 314
V. PRIVACY IMPLICATIONS FOR BUSINESSES DUE TO SOCIAL

† Katheryn A. Andresen is a partner at Hellmuth & Johnson, PLLC, in the Information Technology and Ecommerce Practice Group. Ms. Andresen is an experienced transactional attorney, with a practice emphasis on technology and intellectual property considerations. She is a frequent author and guest speaker—both nationally and internationally—on technology law related matters. Ms. Andresen authored THE LAW AND BUSINESS OF COMPUTER SOFTWARE (2d ed. 2011).
I. INTRODUCTION

With the advent of social networks, the Internet has been transfigured from silos of use (e.g., game sites, business applications, and company sites) into potential streams of information merged through social network sites. The Internet may have originally been designed to allow professors in a university setting to share files and information, but it would have been impossible for anyone to conceive of the total integration of such information access into all areas of life. The Internet can now be used for an extremely broad range of uses: family/social communication, business marketing/applications/communication, personal interests (e.g., gaming, pornography, hobbies, etc.), and information resources.

Business use of the Internet was originally limited to basic company websites, streamlined communication via e-mail and sharing of documents electronically, and marketing through domain name and search engine keywords; few businesses initially understood the benefit or impact of a well-designed company

---


2. Barry M. Leiner et al., A Brief History of the Internet, INTERNET SOCY, http://www.isoc.org/internet/history/brief.shtml (last visited Oct. 20, 2011) (“[T]hese early networks (including ARPANET) were purpose-built—i.e., they were intended for, and largely restricted to, closed communities of scholars . . . .”).

website. In the late 1990s, technology companies broadened the reach of their software through the development of the Internet-based application that was licensed under an Application Service Provider (ASP) or Software-as-a-Service arrangement. In addition, businesses developed electronic versions of licenses now labeled as “click-wraps” or “browse-wraps” and utilized new marketing tools through a variety of company sites, industry sites, search engines, and other tools (e.g., cookies, bots, and spyders). With the advent of social networks, businesses now have the option of expanding their service/product offerings or marketing options through this new media. Businesses, however, should assess the benefits and risks associated with the utilization of social networks.

This article reviews the expansion of social networks and the impact of that expansion on business. It then explores the application of social networks to business through marketing and expansion of services. Next, it identifies both the business and legal risks in conducting business through social networks. Finally, it reviews the privacy implications to business due to social networks, providing a separate analysis of such privacy considerations for regulated entities under the Gramm-Leach-Bliley Act (GLB Act) or the Health Information Portability and Accountability Act (HIPAA). It also identifies some specific risks to individuals—especially those subject to ethical obligations—such as doctors or lawyers. It concludes that social networks are now an inherent part of conducting business; and, as such, businesses

4. See Roy Rosenzweig, Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet, 103 AM. HIST. REV. 1530, 1543 (1998); see also Leiner et al., supra note 2.
7. See infra Part III.
8. See infra Part II.
9. See infra Part III.
10. See infra Part III.
11. See infra Part IV.
12. See infra Part V.
13. See infra Part V.B.
14. See infra Part V.C.
need to develop policies and practices to reduce business and legal risks, in addition to refining business strategies to maximize benefits under marketing and expansion of services.\(^\text{15}\)

II. THE EXPANSION OF SOCIAL NETWORKS

The concept of a social network was originally developed as a simple application allowing “members” to join for free (thereby creating a member account and member page on the website).\(^\text{16}\) Members were then permitted to customize their member page by adding text, photos, and graphics. As the volume of members grew, the concept of associating commercial value through that “member access” market developed.\(^\text{17}\) As this article will discuss in greater detail, this focus on associating commercial value through member access implicates a number of possible privacy considerations.

A. From Playground to Credible Business

When the creators of MySpace launched their site in 2003, it was aimed at young members of Generation Y who could create custom pages with pictures and text to share ideas and favorite music and other activities with friends.\(^\text{18}\) The company envisioned advertising targeted at this group for specific music groups, movies, and TV shows.\(^\text{19}\) Around the same time, the creators of Facebook developed their own site, initially targeting college students, with the aim of making it easier to set up a profile page and to communicate with linked friends, both in messages and pictures.\(^\text{20}\) Social networking sites offer free services, but their value is based on the concept of profitability through advertising revenue based

---

15. See infra Part VI.
17. See id.
19. See Williams, supra note 18 (discussing the roots and early successes of MySpace).
on the number of subscribers. 21

Within weeks of launching, both sites had one million users, and by summer of 2011, Facebook had over 750 million users. 22 With advertisers paying per click, and with bumps in payments for one million-plus users, it is easy to understand how a site that is free to users could be extremely profitable. Although LinkedIn launched prior to MySpace and Facebook, 23 it has grown at a slower rate. 24 This professional-connection site is accessed less frequently by its users than the other social networks, but it expressly targets companies as users. 25

Along with the tremendous growth of social networks, the companies running the sites had to learn and grow, often with painful, public outrages over company policies or changes in site options. 26 Facebook settled a class action lawsuit based on its Beacon program—after users alleged violations of users’ privacy—for $9.5 million. 27 A consistent concern with these sites has been the privacy protections (or lack thereof) and the risks associated with the sites’ privacy policies. 28 There have been numerous studies

---


24. Id. (claiming more than 120 million users as of August 2011).

25. See id. (“More than 2 million companies have LinkedIn company pages.”).


and cases of individuals losing their jobs or losing out on job possibilities based on personal postings on a social network site.\textsuperscript{29}

The obligation to assume corporate responsibility for an individual’s privacy concerns was previously focused on key industries, such as financial institutions and healthcare providers.\textsuperscript{30} Consumer privacy protections have been escalated through Federal Trade Commission (FTC) actions bringing section 5 claims against social networking sites, leading to orders or settlements requiring the sites to change corporate policies.\textsuperscript{31} For example, an order against Google required Google to: (1) not misrepresent its privacy policies; (2) give users clear notice and obtain consent before use of user information; (3) establish and maintain a comprehensive privacy policy; and (4) allow for a neutral auditor to audit for compliance for a twenty-year period.\textsuperscript{32} Similarly, a ruling against Twitter also obligated a twenty-year audit right.\textsuperscript{33} In fact, Congress has now introduced privacy bills aimed at creating a federal baseline of privacy protections from business and social networks.\textsuperscript{34}

The European Union created its regulation on privacy years ago, obligating individual protections and limiting business access and

\begin{flushright}
\textsuperscript{29}. See infra Part V.C.
\textsuperscript{30}. See \textit{cf} ANDRESEN, supra note 6, § 6 (detailing the Gramm-Leach-Bliley Act, applicable to financial institutions, and the Health Information Portability and Accountability Act, applicable to healthcare providers).
\textsuperscript{33}. \textit{In re} Twitter, Inc., 2011 WL 914034, at *4.
\end{flushright}
use of private information without express consent. Even if the United States enacts a privacy statute, it likely will permit business to continue with its current marketing and information uses, provided that an individual has the right to opt out of such use.

B. Target Market Expansion

Besides social networks, the concept of using free social access focused on meeting an individual need has expanded into alternative business and referral models. Craigslist was developed in base form in the 1990s. By the early 2000s it had expanded to a national model focused on offering local advertising for personal sales. The concept behind Craigslist was not new; individuals have advertised their personal items for sale or offered services for centuries via traditional print media. Instead, the use of the Internet made such ads easier to search and find. Although Craigslist is now available around the globe, and eBay even bought twenty-five percent of Craigslist’s equity in 2004, it still does not have the polish and sophistication of other social networks. The website is still coded in Perl and has limited customization by users. The lack of sophistication is most obvious in the limited keyword obligations and various types of search capabilities. The ads on Craigslist are presented in reverse chronological order, and the search engine tools are basic. The Craigslist site lacks the look and feel of a professional business site.

---


36. See generally About Craigslist Factsheet, CRAIGSLIST (Nov. 9, 2010, 1:20 PM), http://www.craigslist.org/about/factsheet (listing and answering frequently asked questions about Craigslist and its services).


38. See About Craigslist Factsheet, supra note 36.

39. Id.


42. Id. For example, a professional business site should allow for easy and logical search of the ads.
There are also numerous referral sites based on free social access (e.g., Angie’s List, Service Magic, or even the advertising options on search engines like Google or Yahoo).

These referral sources are designed to allow individuals to provide references or feedback on service providers. This personalized referral source lends credibility to the service provider, but, depending on the site’s terms and conditions, it may be possible for a business to enter its own “review,” thereby skewing the apparent neutrality of the referral source. Selling advertisements on such sites may also reduce the ability to trust the objectivity of the site’s reviews.

III. THE APPLICATION OF SOCIAL NETWORKS TO BUSINESS (I.E., MARKETING ALTERNATIVES)

Social networks created a new pool of potential customers through the sheer volume of users that voluntarily created accounts. In addition, the true social networks like Facebook, MySpace, and LinkedIn also created access points likely to be viewed frequently by users. In a 2010 survey, social network sites accounted for twelve percent of all online use. Even though social networks may have started as a communication tool for young people in school, the average age of users of a major social networking site is now forty years old. Along with ease of use and popularity, social networking sites also require businesses to consider issues related to security, privacy, terms of use, employee policies, and brand or other intellectual property protection. However, in addition to the concerns associated with social networks, companies have also recognized new market


44. ANGIE’S LIST, supra note 43; SERVICEMAGIC.COM, supra note 43.


opportunities through these networks of voluntary users. Of the Fortune Global 100 companies, 65% have active Twitter accounts, 54% have Facebook fan pages, 50% have YouTube video channels and 33% have corporate blogs. Even governments have worked to establish a social media presence. The National Association of State Chief Information Officers (NASCIO) conducted a survey of social media use in 2010. Forty-three states participated, representing approximately seventy-nine percent of the U.S. population.

A. Business Identification of Market Opportunities

One of the first sources of marketing opportunities via the Internet outside of a company’s own website was through either search engine placement or search engine advertising. Although search engines have millions of users, there is no way to guarantee what search criteria would be entered in order to gain access to such users. In the social network environment, users are easier to access in the sense that their “address” (i.e., their profile page) is knowable. In addition, just as the depth of information about a company’s own clients is developed over time, the type of information associated with an individual user on a social networking site becomes increasingly more comprehensive as the user updates and adds to his or her profile. The network

50. Id. at 2.
52. Generally, using a competitor’s keyword for paid advertising is a “likelihood of confusion” trademark infringement. See Network Automation, Inc. v. Advanced Sys. Concepts, Inc., 638 F.3d 1137, 1154 (9th Cir. 2011) (holding that the “Internet ‘troika’” factors are not controlling and that courts should instead consider traditional factors in assessing consumers’ likelihood of confusion).
54. See generally Personalized Marketing Brings Rewards and Challenges, eMARKETER (June 2, 2011), http://www.emarketer.tv/Article.aspx?R=1008417 (discussing the efficiency of personalized marketing and surveying respondents to conclude that companies will use personalized marketing more in the future).
approach through personal contacts also takes advantage of “social capital.”

Beyond the popular social networks like Facebook and LinkedIn, there are now a multitude of private-branded network sites and company- or industry-specific “community” sites designed to capture the benefits of a social network.\(^\text{57}\) For example:

A new national survey by the Pew Research Center’s Internet & American Life Project has found that 75% of all American adults are active in some kind of voluntary group or organization and internet users are more likely than others to be active . . . . And social media users are even more likely to be active: 82% of social network users and 85% of Twitter users are group participants.\(^\text{58}\)

There are also professional sites—such as that run by the International Technology Law Association\(^\text{59}\)—that allow for some portions of their site to be accessed by the public, but which have custom sections on the site limited to actual members.\(^\text{60}\) Even the International Association of Machinists—started in 1888,\(^\text{61}\) well before the development of the computer, the Internet, or social networking sites—now has a website that acts as a union vision statement, online lobby, and information distribution point and allows members of the union to connect with each other through the members section.\(^\text{62}\)

---


57. See Andrea Kavanaugh et al., Community Networks: Where Offline Communities Meet Online, 10 J. COMPUTER-MEDIATED COMM. (2005), http://jcmc.indiana.edu/vol10/issue4/kavanaugh.html, for a statistical analysis on community networks.


60. See, e.g., Member Center Login, INT’L TECH. L. Ass’N, http://www.itechlaw.org/members.htm (last visited Oct. 20, 2011) (requiring a username and password for access to member-only content).


B. Application Development

As the volume of members in social networks grew, the financial incentive for other companies to develop related applications also grew. The business models of the most successful social network companies encouraged the development of third-party applications that might be of interest to the site’s users. To that extent, the ability to access an interface code (e.g., application programming interface or “API”) or to use the social network’s development platform requires strict compliance with the social network’s standards. A business that offered a transportable service (e.g., horoscopes, weather, or search engines) could develop a social network version application that extended the reach of such services to the users of the social networks within the social network environment. These applications are voluntarily selected by users but are also viral because a user’s friends and family connections are shared as links allowing an application download or link to that new user’s profile. Most social networks require user permission for this viral sharing. For example, Facebook’s developer site states: “In order to gain access to all the user information available to your app by default (like the user’s Facebook ID), the user must authorize your app.”

Some companies were started for the express purpose of developing custom social networks, custom games, or other

---

63. See, e.g., Apps on Facebook.com, FACEBOOK, http://developers.facebook.com/docs/guides/canvas (last updated Oct. 6, 2011) (“Building an app on Facebook gives you the opportunity to deeply integrate into the core Facebook experience. Your app can integrate with many aspects of Facebook.com . . . .”).

64. See, e.g., Facebook Platform Policies, FACEBOOK, http://developers.facebook.com/policy (last updated Oct. 7, 2011) (requiring platform applications and developers to comply with Facebook’s statement of rights and responsibilities, principles, and policies, each of which is outlined in great detail).

65. For example, see Apps on Facebook.com, supra note 63, for information on developing a Facebook version of an application.

66. See, e.g., Social Channels, FACEBOOK, http://developers.facebook.com/docs/channels (last updated June 11, 2011) (“Apps on Facebook.com have the opportunity to appear on one of two dashboards—the Apps Dashboard and the Games Dashboard. Dashboards appear as bookmarked links on Facebook’s homepage and shows [sic] users [sic] outstanding requests, apps they’ve recently used and apps their friends have recently used.”).


69. See, e.g., Dustin Betonio, 25 Best Social Networking Platforms to Start Your Own Service, TRIPWIRE MAG. (July 10, 2010), http://www.tripwiremagazine.com
applications to be run in a social network environment, or even generating response or data collection information and statistics from social network users. Whole new industries have also been created such as search engine optimization services. Gaming, as an industry, had to shift and redesign its development model to account for social networks. The advent of social networks created its own industry of technology companies providing content, analyzing content, or analyzing the use of such content. Some examples of these companies include:

- Microsoft’s Sharepoint, which allows “your people [to] set up Web sites to share information with others, manage documents from start to finish, and publish reports to help everyone make better decisions.”
- Select Minds, which allows a company to create a corporate “alumni” network application.
- Joomla!, which is an open-source content management system (CMS).
- Communispace, which designs customer feedback applications.
- Passenger, which also creates customer community sites so companies get clear feedback on their services and goods.


C. Expansion of Business Through Social Networks

In addition to targeted advertising, social networks allow a business to think outside the box by creating games or applications intended to gather user information, as well as other data. These games or applications are spread virally (i.e., from user to user) as a user invites or attempts to play with a social network “friend,” which obligates the “friend” to also become a member in order to play.\(^{78}\) The marketing could be incorporated into a game or other application, but the key element is the acquisition of user data, including usage, connections, and—depending on the type of cookies, bots, or other tools utilized—information on the next pages or sites visited by the user.\(^{79}\) But the specific type of user data that is captured may be vastly different depending on the purpose for which the user data is captured. For example, while it may be significant for a company that sells goods to know if a site visitor immediately searches for or visits a competitor’s site (presumably to compare goods or pricing), this level of detail may not be relevant for other companies using user data for other purposes. If a site does not sell commercial products, the need for commercial competitiveness data is likely irrelevant and not worth the cost of tracking and monitoring. The biggest impact of social networks, however, is the sheer volume of users and daily access to these users.\(^{80}\)

1. Target Marketing

The concept of social networks led to the development of new services and applications that permit target marketing by knowing

\(\text{white label community vendor} \) that helps brands develop “through ongoing customer collaboration”).


in advance what an individual user’s preferences are. Such knowledge is gained, in part, by assessing keyword usage in a user profile. For example, a user who supports a diabetes group in a social network environment may be interested in drugs and treatments for diabetics. Just as search engines could use the keyword used for the search to return appropriate links, associating keywords with a specific user allows companies to send marketing information regarding what is likely to be more interesting or relevant to that user. Targeted marketing may also have a strong viral component to it. As one study noted, “[w]e’ve also discovered that 44% of users readily share brand-related information with others. And, as action speaks louder than words, 48% of those who came into contact with a brand name on Twitter and 34% on other social networks went on to search for additional information on search engines.”

In addition, many social networks have categorical information related to users, such as age range, geographical location, and affiliation (with companies or schools). This type of information not only permits businesses to identify target markets for their ads, but also provides both specific companies and educational institutions access to alumni communities for sharing information or targeting advertising. Just as AARP became the perfect target market opportunity for companies offering goods and services for

---


82. See id.


baby boomers, social networking sites allow companies to offer goods and services to target markets based on any number of data criteria. In addition to marketing a company’s own goods, a company has the option to market its goods whenever a related good or service is searched or identified by keywords associated with a user’s profile. However, a company should consider the risks these keywords have, which led to a large volume of cases cited based on keywords in search engine ads.

2. Expansion of Companies’ Goods/Services

Social networks, and the concepts associated with such networking, create new service opportunities for various industries. Data analysis and data integration companies have new resources and new types of data through social network users’ information. These new data elements have permitted new types of statistical analysis on market penetration, average user profile, as well as geographical and other custom variations. For example, it is entirely plausible that a company could assess the buying habits of a social network user and also determine if fans of certain music are more likely to purchase similar products or services. The ability to then identify new or related goods and services is strengthened by this built-in market analysis information.

On the community sites, actual customers not only provide feedback but are also just as likely to offer suggestions as to improvements or indicate related items they typically buy to supplement their purchase. This information is then reported back to the company for use in its product development process.

89. See infra notes 102–106.
90. See Boorman, supra note 87.
93. Id.
For example, if many users comment on the best place to purchase cool futon covers, a company that sells futons may elect to become an authorized reseller of those covers—or may elect to create a competitive product to augment its futon sales.

IV. RISKS ASSOCIATED WITH MARKETING THROUGH SOCIAL NETWORKS

The viral nature of social networks needs to be both understood and accounted for in a decision to market through a particular network. If a company creates an ad campaign that has an unintended negative effect in the traditional marketing realm, the ad pieces could be pulled from circulation and destroyed. In an online social network environment, replacing an ad may be too late—a posting is likely to have been passed from user to user and may potentially even be cached and stored in multiple locations on the web. Just as work professionals had to relearn the art of communication when switching from letters to e-mails, companies need to relearn the art of conducting business on social networks.  

A glossy tri-fold marketing piece, when uploaded to an online environment, oftentimes loses its effectiveness as the graphic capabilities vary from browser to browser and the hardware hosting the browser may have more or less random access memory (or “RAM”). If a graphic does not load quickly and sharply, it is likely to be viewed as a nuisance rather than as an effective advertising brochure.

A move into social media for businesses may seem like a necessary requirement in today’s marketplace, but there are both business and legal risks in doing so. The business risks include potential loss of control over target marketing or brand adherence. The legal risks include privacy considerations, impacts on intellectual property rights, possible claims for breach of contract, and tort liability. The actual impact and relevance of

---


96. See Lawrence Savell, Minimizing the Legal Risks of Using Online Social Networks, CHADBOUNRE & PARK LLP (June 28, 2010), available at http://www.chadbourne.com/publications (enter “Savell” in search field).
social media to business is likely not even fully recognized. Notwithstanding these risks, more than half of companies surveyed are using social media without any strategy.  

A. Business Risks and Strategies to Avoid Such Risks

Outside of technology considerations, marketing online requires recognition of the potential loss of control over distribution, location, and association. While the maker of an aged single malt scotch would gladly target its marketing to private clubs and upscale bars and restaurants, it would likely want to avoid marketing to pregnant women, minors, or alcoholics. In a social network environment, the ability to manage that target market may be controllable at the launch point, but that control may be lost among users of the network. If this effect is taken into consideration in the social media marketing campaign, this is not necessarily a bad thing, but a haphazard marketing strategy can have harmful business ramifications.

1. Effect on Brand

For many companies, the development of its brand is one of the critical components of a company’s intellectual property portfolio. Controlling and managing that brand is also both strategically desirable and necessary. A brand connects a company’s products or services with an image of the quality and desirability. Famous brands sell based on name alone; for example, Ralph Lauren, Coca-Cola, Apple, and Tiffany’s.  


98. Aaron Strout, The Upside of Losing Brand Control, E-COMMERCE TIMES (July 16, 2009, 4:00 AM PT), http://www.ecommercetimes.com/article/67606.html?wlc=1307377469 (“What companies need is a plan: how to engage with their customers and begin to ‘shepherd’ their brand, even if they no longer ‘own’ it.”).


100. See Adam Arvidsson, Brands: A Critical Perspective, 5 J. CONSUMER CULTURE 235, 236 (2005), available at http://www.pineforge.com/mcdonaldizationstudy5/articles/Consumption_Articles%20PDFs/Arvidsson.pdf (“For companies like McDonald’s, Coca-Cola or Nike, the most valuable asset is the public standing of their brands.”); Jonathan Mesiano Crookston, Controlling Your Brand on Social
brand, however, is in its association with consistently high quality goods and services. In a social network, the ability to control that association may be lost. For example, there have been many cases associated with search engines over the use of keywords including a protected brand where the search result is to a different company’s goods or services. Some cases have held that the use of metatags in search engines constitutes “use in commerce” and have allowed a claim under the Lanham Act, while other cases have held that metatags do not constitute “use in commerce.” Still other cases have held that, even though metatags constitute “use in commerce,” there is no “likelihood of confusion.”

In 2011, the Ninth Circuit clarified that these keyword cases do not reduce the consideration of the typical eight factors used to assess “likelihood of confusion,” and that prior case law, which referred to a three-factor “Internet troika” test, was not appropriate “[g]iven the multifaceted nature of the Internet . . . .”

Another issue can be based on technology-related problems with color standards or logo graphics. Some companies invest

---


102. See I ANDRESEN, supra note 6, §§ 5:17, 23:7.

103. Id. (citing cases such as Edina Realty, Inc. v. TheMLSonline.com, 2006 WL 737064 (D. Minn. Mar. 20, 2006) and Playboy Enters., Inc. v. Netscape Commc’n Corp., 354 F.3d 1020 (9th Cir. 2004)).


105. Id. (citing J.G. Wentworth, S.S.C. Ltd. v. Settlement Funding LLC, No. 06-0597, 2007 WL 50115, at *6 (E.D. Pa. Jan. 4, 2007) (concluding that use of a mark in Google’s AdWord program and in metatags is “use in commerce” under the Lanham Act but does not fall within “likelihood of confusion”); see also Hamzik v. Zale Corp., No. 3:06-CV-1300, 2007 WL 1174863, at *2–3 (N.D.N.Y. Apr. 19, 2007) (agreeing with the reasoning in Rescue.com Corp. but denying the motion to dismiss because a search of plaintiff’s trademark not only returned defendant’s website among the search results, but plaintiff’s trademark also appeared next to defendant’s name, demonstrating that plaintiff’s trademark could be displayed in a way indicating an association with defendant).

significantly in protecting their brand, including color elements. Online usages of the graphic components (i.e., color) of marks, however, are more difficult to manage from a strict control perspective. It is not possible to control the hardware, memory capabilities, or monitor graphics capabilities for each user. Unlike selling a software product where the company can establish baseline technology standards for use of the product, use of brands in social networks eliminates the ability to control for the end user’s actual experience of the mark.

Even without technology issues, a complex advertising campaign involving multiple pages of graphics may be quite effective in print but cumbersome or annoying once delivered electronically. When website developers discovered the flash component option for sites, it became popular to code mini-videos or streamed graphics for the opening page of the site. In the social network setting, linking to such a page can be too slow for good user response. Another example could be the balance of text and graphics to keep a user’s interest and lower the site’s “bounce rate” (i.e., the rate at which a user quickly moves on to another page). Web analytics assess many elements of a site, including technical issues.

Social network users expect an easy-to-use and logical process to access information, just like most social networks attempt to provide. Linking from this type of site onto an advertiser’s own


109. See, e.g., Varatharajan, supra note 108.


site may highlight issues or failures for a good user experience if (1) the company site is difficult to navigate, (2) the search for products is not easy and logical, or (3) the link is to a competitor or negative site.\footnote{See Danny Sullivan, \textit{Bing Terminates Relationship with Publisher Doing Tricky Home Page Switch}, \textit{Search Engine Land} (Jan. 18, 2011, 1:07 PM), http://searchengineland.com/bing-to-address-problems-with-affiliate-doing-tricky-home-page-switch-61551.}

2. \textit{Control of Company Image/Position}

In addition to issues related specifically to a company’s branding of particular products, there may also be risks associated with the organization’s image more generally. For example, in a social network, there is a fine line between the “freedom of speech” right of a user and the violation of a protected trademark right of another. While gripe or parody sites have been upheld in case law on the basis of First Amendment rights—particularly where the use is non-commercial,\footnote{See Lamparello v. Falwell, 420 F.3d 309, 318–19 (4th Cir. 2005) (noting that even amendments to the Lanham Act—the Federal Trademark Dilution Act of 1995 and the Anticybersquatting Consumer Protection Act of 1999—did not intend to limit First Amendment rights, especially for non-commercial use); \textit{see also} Nissan Motor Co. v. Nissan Computer Corp., 378 F.3d 1002, 1015–18 (9th Cir. 2004) (holding that an injunction preventing a company from placing links to disparaging remarks about another company violated the First Amendment because the speech enjoined was non-commercial); Taubman Co. v. Webfeats, 319 F.3d 770, 774–75 (6th Cir. 2003) (noting that the Lanham Act limits First Amendment protections on commercial speech but not on non-commercial speech).}—linking a purported “comment” to an advertisement for a competitive product may violate the Lanham Act or other legal rights of the brand owner.\footnote{See PBM Prods. v. Mead Johnson & Co., 639 F.3d 111, 121–22 (4th Cir. 2011).}

A company can implement a social media policy and create and manage its own social media accounts, but doing nothing may have a negative impact on a company’s key brands. In one study, professors from three countries—Sweden, the United Kingdom, and the United States—statistically assessed the impact potential of marketing through social media for luxury wine brands.\footnote{Mignon Reyneke et al., \textit{Luxury Wine Brand Visibility in Social Media: An Exploratory Study}, 23 INT’L J. WINE BUS. RES. 21, 26–31, 34–35 (2011).} The study assessed the development of the social media marketplace,\footnote{Id. at 22–24.} examples of ways to improve the user’s experience.)
identified a tool for assessing brand strength, and concluded business should understand its brand’s essence in social media (e.g., whether the brand is business-oriented and formal, or whether it is more personal, social, and informal). Brand development for Starbucks would likely fall in the latter category, and SAP would fall in the first category. The study actually used four quadrants, with the other two combinations identifying a brand as business-oriented but still informal (like the musical tones in Intel’s brand) or a personal brand that is presented in a formal manner (like Tiffany’s blue box). If a company understands its brand’s essence, then it is poised to develop both a social media policy and a campaign designed to maximize that essence. For example, Nikon’s camera campaign using Ashton Kutcher and YouTube is directly on-point for an informal or personal brand essence.

A company (or even a government agency like the Secret Service) with a brand associated simply with the concept of high professionalism or protected privacy may be negatively impacted by any “tweeting,” posting, or other social network messaging that is considered less than professional or discreet. In other contexts, a simple news story can become a corporate nightmare if it creates a negative impression that is then virally transmitted through social networks.

3. Premature Release of New Products/Services

The nature of the Internet—with its high-speed dissemination of information and the ease by which the average citizen can be a source for news—may cause risks associated with an organization’s

117. Id. at 24–26.
118. Id. at 32.
120. In May 2011, the Secret Service asserted a tweet from an agent was “unapproved and inappropriate . . . . Policies and practices which would have prevented this were not followed and will be reinforced for all account users.” CNN, Secret Service Apologizes for Twitter Gaffe, CNN POL. (May 18, 2011, 5:24 PM), http://politicalticker.blogs.cnn.com/2011/05/18/secret-service-apologizes-for-twitter-gaffe [hereinafter Secret Service] (quoting Secret Service statement regarding the offensive tweet).
strategic release of information. For example, the latest Apple technology offering was big news when it was supposedly found after being inadvertently left behind by an employee in advance of the public release.\textsuperscript{122} This type of news story was picked up and tweeted and posted throughout social networks between Apple fans eager to get a glimpse of the next great thing.\textsuperscript{123} If Apple had found bugs or manufacturing issues with that technology, the delay to market after such a story could have had a negative effect on the product launch. Impressions count; a bad news leak about an upcoming launch of a product or service can be devastating to the success of the product or service.\textsuperscript{124} In the social network realm, these leaks can be spread so quickly that trying to rewrite or remove the leak is nearly impossible.

An employee’s post to private friends in a social network can still spread virally to the public,\textsuperscript{125} so employee comments on upcoming products or services could potentially have a big effect on the intended launch advertising campaign.

B. Legal Risks

While certain businesses or industries are subject to federal or state laws and regulations as to content or disclosure of information,\textsuperscript{126} all companies with an Internet presence need to be aware of the less obvious legal risks.

1. Compliance Consideration with Company Policies

Just as contract law started as a common law right (versus a statutory right),\textsuperscript{127} companies are now held liable for compliance with their own posted policies (e.g., terms and conditions for its


\textsuperscript{126} See \textit{1 ANDRESEN}, \textit{supra} note 6, §§ 6:1–6:23 (discussing federal software regulations).

\textsuperscript{127} See \textit{1 HOWARD O. HUNTER}, \textit{MODERN LAW OF CONTRACTS} § 1:1 (2011) (discussing the roots and development of contract law in the United States).
Even if a company does not have a privacy obligation with regards to certain types of user data, if they have included a privacy obligation in the company privacy policy, a court will uphold that type of assumed obligation on a contract law basis. Even if a company’s terms and privacy policy include a company’s discretion to update, amend, or change them at any time, a company may be held liable if it is deemed a user would not have reasonably known of such change.

In addition, if a company attempts to limit or eliminate an obligation otherwise owed by law or regulation, such a clause would likely be held invalid and the entire term agreement or privacy policy could potentially be deemed invalid. Some of the easiest ways for a company to breach its own privacy policy can occur when the data use is not known or anticipated at the drafting stage of the policy. For example, one company created a privacy policy that it would not share or allow access to its users’ information with any third party. When that company ultimately attempted to sell its assets under a bankruptcy proceeding to a new company, the FTC Director of the Bureau of Consumer Protection wrote to the trustee that the user information could not be transferred to a buying entity without the express consent of each user based on the privacy policy in place.

Another possible risk is an overly broad social media policy. For example, in response to a nonprofit discharging employees because of posts on social media sites, the National Labor Relations Board (NLRB) challenged the organization’s social media policy as being overly broad and having a chilling effect on an employee’s


130. See Douglas v. U.S. Dist. Court for Cent. Dist. of Cal., 495 F.3d 1062, 1066 (9th Cir. 2007).

131. See, e.g., Circuit City Stores, Inc. v. Mantor, 335 F.3d 1101, 1109 (9th Cir. 2003) (“Under California law, a court has discretion whether to sever particular unconscionable terms or invalidate a contract entirely.”).


133. Id.
right to discuss working conditions.\textsuperscript{134}

2. \textit{Loss of Intellectual Property}

While a company typically is very careful to protect its intellectual property in contracts with vendors, clients, or other parties, it often fails to recognize the similar risks in simple disclosures through social networks, blogs, or even the company’s own website. For example, one of the deciding factors for the patentability of a new invention is based on the filing of the application taking place within one year of publication of the invention.\textsuperscript{135} A press release issued through a company’s social network page, or even its own website, would likely constitute publication if the invention was identifiable in the release.\textsuperscript{136}

Some companies have their entire business value tied to a specific trade secret (e.g., the recipe for Coca-Cola or Kentucky Fried Chicken). An informal chat within a social network context could result in the loss of a company’s trade secret if any of the trade secret is even inadvertently disclosed in the social network context (because such a disclosure is likely a publication extinguishing trade secret protections).\textsuperscript{137} While copyright is not lost when “published,” the ability to formally register with the U. S. Copyright Office may be lost if not timely filed within a certain time from publication.\textsuperscript{138} This loss of registration may result in an inability to recover actual or statutory damages because damages are only permitted for registered works, and non-statutory damages may otherwise be unknowable or incapable of proof.\textsuperscript{139}


\textsuperscript{135} See 1 ANDRESEN, supra note 6, § 3:18.

\textsuperscript{136} See id.

\textsuperscript{137} See id., § 4:7 (discussing the circumstances under which a disclosure could extinguish trade secret protection and considering a variety of factors, including who made the disclosure and whether the owner of the trade secret took meaningful, reasonable steps to protect the information).

\textsuperscript{138} 17 U.S.C. § 412(2) (2006); 1 ANDRESEN, supra note 6, § 2:21.

\textsuperscript{139} 17 U.S.C. § 504(c) (2006); see also 17 U.S.C. § 408(f)(4) (2006) (describing the effect of untimely application); 1 ANDRESEN, supra note 6, § 2:21.
Trademarks not used within company guidelines in a social media context may also result in the loss of intellectual property if the brand or quality associated with the mark is diluted, the brand develops negative associations, or if the use renders the trademark generic.¹⁴⁰

3. Liability Issues

A number of liability concerns arise when companies fail to implement coherent social media policies. For example, a business-to-business deal could include an obligation to keep the terms of the agreement confidential, potentially even obligating one or both parties not to disclose negotiations with the other party. An employee’s reference on a social networking web site to work associated either with the other party or on any terms of the contract would likely violate this contractual obligation, potentially resulting in a breach of contract claim or the loss of the business deal. For example, in the context of most high-level merger and acquisition deals, there is a very strict non-disclosure policy as even a hint of a deal could have securities law implications.¹⁴¹ A blog about their “busy day” sent between employees of the two companies could have the same impact or lead to the disclosure of the impending deal.¹⁴²

A company could also potentially be liable for a tort claim of invasion of privacy for disclosure of non-public information through social networks or otherwise. The claims may vary from state to state, but they typically require a non-public fact disclosed to the public. Companies should also recognize that at least one state appellate court has held a social network post as meeting the “publication” requirement to establish a privacy tort.¹⁴³ The publication element may be met both “by proving a single communication to the public, and . . . by proving communication to individuals in such a large number that the information is

¹⁴⁰. ¹ Andrésen, supra note 6, § 5:7.
deemed to have been communicated to the public.” While there is an exception for information “of interest” to the public, such as news reports, this exception does not extend to information that would be deemed “morbid and sensational eavesdropping or gossip.”

V. PRIVACY IMPLICATIONS FOR BUSINESSES DUE TO SOCIAL NETWORKS

Besides the marketing risk noted above, companies need to be mindful of how public disclosures may create legal liabilities. There are local, state, federal, and even international laws, rules, and regulations governing the protection of privacy rights for both consumers and employees. There are also privacy obligations assumed by a company through contract terms or even self-imposed by a company’s privacy policy posted on the company’s website. The risk level for a company, with regards to liability for privacy violations through public disclosures, is potentially compounded through an active social media presence.

A. Businesses Generally: Privacy Policies and Social Media

Privacy rights for consumers have been fairly rigorously protected in the European Union countries due to the Directive on Data Protection. In the United States, companies conducting business online within European Union member states, or directly in such European Union member states, have had to create a “safe harbor” policy to comply with this directive. In the United States, however, for the most part, lawmakers left the protection of privacy

144.  Id. at 42.
145.  Catsouras v. Dep’t. of Cal. Highway Patrol, 104 Cal. Rptr. 3d 352, 366 (Ct. App. 2010) (allowing claim for invasion of privacy to stand for public disclosure of photographs of decedent because “morbid and sensational eavesdropping or gossip ‘serves no legitimate public interest and is not deserving of protection’” (citation omitted)).  
146.  Apart from a company’s website terms, a company should consider in its standard vendor or client contracts whether or not social media use, access, or distribution should be addressed. The need for a social media clause will depend on the type of goods or services, the distribution methodology, and the intended marketing channel.
148.  See generally 1 ANDRESEN, supra note 6, § 13:6.
rights to market forces, and business is generally self-regulated. The presumption under the self-regulation framework is that businesses would address at least four key elements in the protection of a consumer’s privacy rights in a fair information practices approach:

(1) businesses should provide notice of what information they collect from consumers and how they use it; (2) consumers should be given choice about how information collected from them may be used; (3) consumers should have access to data collected about them; and (4) businesses should take reasonable steps to ensure the security of the information they collect from consumers.

In addition, a business may still be legally liable for violating an individual’s expectation of privacy, which is established either under common law, by statute, or by contract law through the company’s own website terms and conditions or privacy policy. This era of self-regulation may now be ending. Besides the privacy bills currently pending in Congress, the FTC has undertaken a fairly aggressive prosecution of privacy violations through section 5 of the FTC Act, which prohibits “unfair or deceptive acts or practices” claims. In support of this new approach, in 2010, the FTC issued a preliminary staff report entitled, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.

The FTC’s framework proposes the following:

- **Scope:** The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.
- **Privacy by Design:** Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

149. There are federal regulations for healthcare providers and financial institutions for personal information deemed critical and therefore protected by statutes under the GLB Act and HIPAA.


151. *Id.* at 7–8. At the time of this writing, several bills were pending in the 112th Congress. See, e.g., BEST PRACTICES Act, H.R. 611, 112th Cong. (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); H.R. 1528, Consumer Privacy Protection Act of 2011, 112th Cong. (2011).


153. See *Protecting Consumer Privacy*, *supra* note 150, at 39–78.
Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.

Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

- **Simplified Choice**: Companies should simplify consumer choice.
- Companies do not need to provide choice before collecting and using consumers’ data for commonly accepted practices, such as product fulfillment.
- For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.
- **Greater Transparency**: Companies should increase the transparency of their data practices.
- Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.
- Companies should provide consumers with reasonable access to data about themselves; the extent of access should depend on the sensitivity of the data and the nature of its use.
- Companies must provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected.
- **All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.**

In addition, at least one recent case makes clear that certain business practices would not fall under the ambit of an increased expectation of privacy. For example, this expectation of privacy does not extend to Google’s data collection practices for its map service, even in the access of private property. A social media policy should be distinct from an information technology (IT) policy. An IT policy typically clarifies the corporate position on equipment, software, and technology use (e.g., data retention,

---

154. *Id.* at 41–42 (citation omitted).
155. Boring v. Google Inc., 362 F. App’x 273, 280 (3d Cir. 2010) (holding there was no invasion of publicity for Google’s recording of property for Google’s map “Street Views” function).
email usage, etc.).

Within that type of policy is a subset of concerns that are specific to social media use. In particular, employees should be clear that, due to the public nature of social media, information that the company needs to protect as confidential cannot be referenced, even indirectly, in social media. While a company could encourage social media standards and appropriate use of privacy settings, since the employee’s use of social media is typically personal and not work-related, this standard may not be enforceable or capable of being monitored and may even be deemed illegal.

What a social media policy needs to clarify is that the corporate intent in dealing with confidentiality includes an employee’s personal use of social media. There are some general reasonable considerations that could be included in a social media policy, including: (1) that an employee’s opinion does not represent the opinion of the employer; (2) that workplace gossip is not tolerated and could have reprimand or termination consequences; and (3) that inappropriate language (e.g., racially or sexually offensive messages, harassment, indecent comments or pictures, or even anything that would reasonably be understood as defamatory or disparaging) may also lead to a reprimand or termination. If there are other company policies as to confidentiality (e.g., anti-harassment or other employment-related or security-related policies), which could be impacted by social media disclosures, these should be acknowledged and addressed in the social media policy.

These considerations are not limited to private corporations. Even federal agencies should have privacy policies that are

---

156. See, e.g., SORCHA DIVER, SANS INST., INFORMATION SECURITY POLICY—A DEVELOPMENT GUIDE FOR LARGE AND SMALL COMPANIES 12, app. 2 (July 12, 2006), available at http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331 (providing a sample of a technical policy and, more generally, discussing the importance of IT policies).

157. See, e.g., News Release, Nat’l Labor Relations Board, Settlement Reached in Case Involving Discharge for Facebook Comments (Feb. 8, 2011), available at http://www.nlrb.gov/news/settlement-reached-case-involving-discharge-facebook-comments (announcing a settlement of a case in which a company fired an employee for making negative comments about a supervisor on Facebook, and under the terms of the settlement the company agreed to revise its employee handbook to ensure that the company does not “improperly restrict employees from discussing their wages, hours and working conditions with co-workers and others while not at work, and that they would not discipline or discharge employees for engaging in such discussions”).
enforced. However, in 2010, the National Association of State Chief Information Officers (NASCIO), a social media and state government working group, conducted a survey of state governments and found that only one-third of the forty-three states participating in the survey had policies in place to address social media use. The Center for Technology in Government published a survey, *Designing Social Media Policy for Government: Eight Essential Elements*, in May 2010. The survey cited key elements that should be incorporated into a social media policy, including:

- Employee access
- Account management
- Acceptable use
- Employee conduct
- Content
- Security
- Legal issues
- Citizen conduct

The NASCIO survey also noted that many states chose to include social media into existing policies, but the Center for Technology in Government survey concluded that such policies may be insufficient to address “blurring boundaries around personal, professional, and official agency use.” In the NASCIO survey, the top five risks associated with social media use included security, terms or legal policies, privacy policies (and obligations), records management, and employee use/abuse. There are increased security risks with social media use, and any IT policy or security policy should be reviewed to ensure it meets the increased risks, such as employee posts that link to corporate sites and failure to meet confidentiality or security obligations related to corporate or client information that may be disclosed either inadvertently or purposefully in personal social media posts, tweets, or blogs. If a security policy requires data retention of all electronic

---

158. On May 18, 2011, the Secret Service announced that “an agent posted an unapproved and inappropriate post . . . . Policies and practices which would have prevented this were not followed and will be reinforced for all account users.” *Secret Service*, supra note 120.

159. *FRIENDS, FOLLOWERS, AND FEEDS*, supra note 47, at 5.


162. HRDINOVÁ, supra note 160, at 7.

communication, this may be deemed to include social media communication. A company should expressly consider if it could, should, or will monitor, retain, or control such social media communication.

If a company elects to have an official (i.e., corporate) account in a social network, there should be clear controls of administrative access rights, use constraints, and management or other organizational oversight to ensure compliance with business, legal, and other considerations. In particular, if a company is also subject to federal regulations on privacy (e.g., the GLB Act or HIPAA\(^\text{164}\)), then any privacy requirements specific to those obligations should also be expressly included in the social media policy, and express guidance should be given to the account manager regarding the company’s social network accounts.

B. Regulated Entities

Besides the privacy risks for companies, generally, in a social media environment, any entity subject to a regulation governing privacy will likely have even greater risk both in oversight by the regulatory authority and obligation under the privacy regulation. For example, both financial institutions and healthcare providers are subject to federal regulations for “personally identifiable information” or “protected health information,” respectively, as it relates to an individual customer.\(^{165}\) As a regulated entity, these types of companies should have increased awareness and concern as to what may be publicly disclosed through social media.

1. Regulatory Compliance

While most consumers understand that their financial and healthcare information is protected as private, not all consumers, or even business associates of regulated entities, necessarily understand the protections or the limits on those protections. Under the Gramm-Leach-Bliley Act (GLB Act), financial


institutions have to treat an individual’s financial account information as private and protected. This does not, however, preclude a financial institution from using a third-party vendor as its agent or contractor for the provision of certain services requiring access to that individual’s financial account information. For example, a bank is governed by both the GLB Act as well as related credit card processor rules regarding the protected nature of a consumer’s credit card transaction involving the debiting of funds from the individual’s bank account. The bank may use a third-party processor to collect and electronically submit the data either upstream to the credit card company or downstream into the bank’s account processing. One of these rules mandates that no copy of the credit card information is to be copied or stored for any longer than it takes to process the transaction and receive a verification code of successful transmission. One third party company that processed such credit card transactions on behalf of large retailers (such as TJ-Maxx) actually copied and retained the information indefinitely—which led to a huge data breach when its servers were hacked.

Healthcare providers are obligated to protect a patient’s health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). There have been numerous

---

168. 15 U.S.C. § 6802(b) (2) (2006) (allowing a financial institution to provide private information to perform services on its behalf, including use of the information for marketing purposes).
169. 15 U.S.C. § 6802(b) (2) (2006) (stating that the third party who gathers such information then is required to maintain the confidentiality of that information).
reported breaches due to a variety of factors, including poor/insufficient security, \textsuperscript{172} third-party vendor lack of controls,\textsuperscript{173} and inadvertent loss or employee carelessness.\textsuperscript{174} Not all use is precluded; a patient may expressly grant permission to use certain protected health information. For example, in a recent social media campaign on health promotion, Blue Cross Blue Shield of Minnesota received permission to monitor and post the health results of a man “living in a box” for thirty days at the Mall of America.\textsuperscript{175}

2. Breach Considerations

For regulated entities, the cost considerations for breaches of privacy are potentially astronomical. Some examples based on claims under HIPAA include a $4.3 million fine by the U.S. Department of Health and Human Services (HHS) for a healthcare provider’s flagrant violation of HIPAA and its refusal to investigate a request from the HHS Secretary,\textsuperscript{176} a $1 million fine for the negligent handling of data when an employee left information on the subway,\textsuperscript{177} and a breach involving 1,023,209 individuals that has cost the healthcare provider $7 million so far.\textsuperscript{178} According to the

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{175} See Press Release, PR Newswire, Shrinking Outside the Box: Blue Cross and Blue Shield of Minnesota’s “The Human Do.ing” Project Inspires Community to Live Healthier (Apr. 16, 2011), available at http://www.reuters.com/article/2011/04/16/idUS41453+16-Apr-2011+PRN20110416 (explaining that, as part of Blue Cross Blue Shield of Minnesota’s do. Campaign, a man lost weight, lowered his cholesterol, and improved his blood pressure by exercising and eating healthier while living inside a glass apartment at the Mall of America).
\item \textsuperscript{178} See Howard Anderson, 7 Million Good Reasons to Prevent a Breach,
Ponemon Institute’s 2010 annual study, the average cost of a data breach was $214 per compromised record (having risen from $138 in 2005), and the 2010 average organizational cost of a data breach was $7.2 million, with sixty-three percent of that cost coming in the form of lost business.\footnote{179}

Especially in the regulated environment, companies should be more proactive and effectively use management oversight to help avoid breach considerations.\footnote{180} The need to protect data, however, sometimes conflicts with the practical need to use real data in the development or testing of IT systems. For example, electing to use only test data for a new system deployment may ensure that no protected health information is disclosed during testing, but it may also mean that the test environment does not adequately test the true volume or complexity of actual data.\footnote{181}

C. Individuals

For certain professions, a breach of a privacy obligation may lead to the loss of accreditation or licensure. For one doctor, Dr. Alexandra Thran, posting news about her day with a trauma patient led to a reprimand by her state’s medical board and a loss of privileges to work in the hospital’s emergency room.\footnote{182} Although no patient name was included, the details of the post allowed others in the community to discern the patient’s identity. This was


\footnote{180. See 45 C.F.R. pts. 160, 162, 164 (2010) (containing regulations interpreting the HIPAA statute issued by the Department of Health and Human Services).}

\footnote{181. Test data is normally not complex enough to properly test a new system. Because of this, companies prefer to use real data when testing a new system. HIPAA allows real data to be used, provided security measures are in place, but a large risk of liability is involved whenever real data is used. A possible solution is to use high quality “fake” data. Fake data is real data that has been altered by a computer program. The alterations usually include dates, dollar amounts, and other private information. See Mathew Schwartz, Test Data: Security Loophole? ENTERPRISE SYS. (Sept. 1, 2002), http://esj.com/articles/2002/09/01/test-data-security-loophole.aspx (discussing data security testing programs and the threat of unintentional internal breaches with several examples).}

a case of first impression for the Rhode Island Board of Medical Licensure and Discipline but it is not likely to be the last case. It may even be possible that simply being “friends” in a social network could be deemed a violation of privacy rules depending on the doctor’s practice (e.g., psychology) if there is any reference to the doctor-patient relationship. Two other doctors have written about the challenges for doctors to maintain their professionalism by maintaining a healthy distance between their work and online identities.

Hospital employees in Wisconsin, Florida, California, and Michigan have been fired, suspended, or demoted for online postings deemed a violation of a patient’s privacy right. Two nurses were involved in taking a picture of a patient’s x-ray and posting the same on Facebook; the hospital may have been held liable for breach of HIPAA’s privacy rule. One nurse vented on Facebook.


185. See Nurses Fired Over Cell Phone Photos of Patient, WISN.COM (Feb. 26, 2009, 1:46 PM), http://www.wisn.com/news/18796315/detail.html [hereinafter Nurses Fired] (reporting that upon notice of a possible HIPAA violation, the nurse removed her Facebook page—including the photograph—and without any evidence that anyone had seen the photograph, the hospital concluded no state law had been violated and referred the matter to the FBI).

186. See John Commins, Shark Attack Victim Photos Put Hospital Employees in Hot Water, HEALTHLEADERS MEDIA (Feb. 26, 2010), http://www.healthleadersmedia.com/page-1/LED-247186/Shark-Attack-Victim-Photos-Put-Hospital-Employees-In-Hot-Water##%23 (discussing the reprimands hospital management administered to employees who published photos on social media sites of a patient suffering from shark attack injuries).

187. See Jennifer Fink, Five Nurses Fired for Facebook Postings, SCRUBS (June 24, 2010), http://scrubsmag.com/five-nurses-fired-for-facebook-postings (discussing the trend of nurses getting into trouble for posting sensitive medical data about patients and a particular incident of three nurses being terminated for such misconduct).


189. See Nurses Fired, supra note 185.
about having to treat a patient who happened to be the alleged “cop-killer” in a local shooting incident.\footnote{Katarsky, supra note 188.} Although no names were posted, based on the publicity of the event and the local news coverage including names, the information was deemed a violation of the patient’s right to privacy, and the nurse was fired.\footnote{Id.}

Even if a posting to a social media site does not lead to the firing, an employee who accesses the records of a patient without a need to know (i.e., just for curiosity’s sake) may still be fired.\footnote{See, e.g., Andrew Blankstein, Eyes on Celebrity Records Multiply: The Internet and a Rising Appetite for Entertainment News Fuel More Invasions of Medical Privacy, L.A. TIMES, May 20, 2008, http://articles.latimes.com/2008/may/20/local/me-tabs20 (noting the sensitivity many hospitals have for protecting their patients’ privacy).} In the recent headline news of Congresswoman Gifford’s shooting, staff at the Tucson hospital searched the electronic patient records of the associated victims of the shooting, and all three staffers were fired for the search.\footnote{Dylan Smith, UMC Workers Fired for Violating Patient Privacy After Sat. Shooting, TUCSONSENTINEL.COM (Jan. 12, 2011), http://www.tucsonsentinel.com/local/report/011112_umc_fired/umc-workers-fired-violating-patient-privacy-after-sat-shooting.} In fact, under the HITECH Act amendments to HIPAA, an egregious breach of privacy obligations may now lead to a criminal conviction.\footnote{Press Release, United States Attorney’s Office, Central District of Cal., Ex-UCLA Healthcare Employee Sentenced to Federal Prison for Illegally Peeking at Patient Records (Apr. 27, 2010) available at http://www.justice.gov/usao/cac/Pressroom/pr2010/079.html. The first individual, Huping Zhou, sentenced under this statute purposefully accessed medical records without a “legitimate reason, medical or otherwise” 323 times after dismissal for unrelated job performance reasons. \textit{Id.}; Chris Dimick, Californian Sentenced to Prison for HIPAA Violation, J. AHIMA (Apr. 29, 2010, 10:57 AM), http://journal.ahima.org/2010/04/29/californian-sentenced-to-prison-for-hipaa-violation.} In the case of Huping Zhou, his criminal conviction under HIPAA was based on electronic medical record access conducted post-dismissal; his ability to commit the crime, however, is due, at least in part, to the failure of the hospital which had employed him to remove his account access immediately upon dismissal.\footnote{Dimick, supra note 194.} The individuals affected by the privacy breach would likely have had a claim against the hospital for either failing to have a policy in place about terminating account access or failing to enforce it.\footnote{See also Security Rule of the Health Information Portability and Accountability Act, 45 C.F.R. pts. 160, 162, 164 (2010) (detailing security measures and management obligations to secure protected health information).} Individuals may have added issues even before employment
based on their social network profiles. At least one law school has
drafted a guideline on “Social Networking Professionalism” to draw
attention to the issues with online identity and the professional
image intended for practicing law. In addition, the ability to
preclude a motion to compel disclosure of the private portions of a
social network site—provided that such information is alleged to be
relevant—is difficult, as courts have held there is no expectation of
privacy on social networking sites. The party compelling
disclosure, however, will still need to be able to authenticate the
social network pages.

VI. CONCLUSION

For many companies, when the Internet took off commercially
in the 1990s, the key commercial factors included company
websites, the ability to email and transmit documents, and the
ability to market the company’s goods and services through search
engines. As social networks have developed over the last ten years,
the ability to connect to a broader market on a more frequent basis
through social networks has become a critical factor for businesses
in deciding whether or not to participate in social networks. It is
now clear that social networks are an inherent part of conducting
business.

Instead of operating casually in the social network sphere,

197. Career Development Office, General Information: Social Networking
/Careers/currentstudents/Documents/Informational%20Handouts/2010%20Up
dated%20Handouts/Social%20Networking%20Professionalism.pdf (last visited

2010) (upholding denial of motion to compel disclosure of Facebook pages
because “[a]lthough defendant specified the type of evidence sought, it failed to
establish a factual predicate with respect to the relevancy of the evidence” (citing
Ct. 2010) (holding that the public pages of Facebook and MySpace are sufficient
evidence that private pages may contain relevant information to grant a motion to
compel; because “neither Facebook nor MySpace guarantee complete privacy,
Plaintiff has no legitimate reasonable expectation of privacy”).

not authenticated and noting “[t]he potential for fabricating or tampering with
electronically stored information on a social networking site, thus poses significant
challenges from the standpoint of authentication of printouts of the site” and that
“the ‘complexity’ or ‘novelty’ of electronically stored information, with its
potential for manipulation, requires greater scrutiny of ‘the foundational
requirements’ than letters or other paper records, to bolster reliability” (quoting
businesses need to develop policies and practices to reduce both business and legal risks. The business risks include loss of trade secrets, brand dilution, and loss of market focus. The legal risks include breach of privacy obligations, both statutory and contract, as well as risks to intellectual property protections. Regulated entities have additional legal risks that must be addressed in the formulation of their policies and practices. All policies developed need to be managed and followed because a breach of even a self-imposed privacy obligation would likely be upheld under a contract law analysis. Even if a business elects not to self-impose certain privacy obligations, it may still be subject to an assumed privacy obligation under an FTC action for fair practices under a section 5 proceeding.

Companies should not only learn how social media can be utilized to maximize the benefits of viral marketing but should also consider the possibility of an expansion of services. Not only do the top social networks provide access to the majority of Internet users, but there are numerous industry-specific social networks and even software to allow a company to develop its own custom social network. The potential benefits of utilizing social networks to expand both marketing and business opportunities have not yet been fully realized. It is incumbent upon businesses to re-think how they conduct business in the new, viral sphere of social networks.