Potential Liability of Social Media in Higher Education Marketing

Nicholas Barnes
Nichols College

There is no longer any question that technology provides effective ways to reach current and potential students. Lost amongst this widespread adoption, however, is a clear sense of liability. Institutions have adopted a multitude of technology tools and services without pausing to set guidelines or create a social media policy. As a result, few organizations have closely analyzed the ramifications of moving an increasing amount of student interaction online. This paper aims to provide some insight into the liability of technology in marketing higher education.

INTRODUCTION

In the last several years, social media and networking technology has proliferated as high-speed Internet became readily available. There is no longer any question that technology provides effective ways to reach current and potential students. Lost amongst this widespread adoption, however, is a clear sense of liability. Institutions have adopted a multitude of technology tools and services without pausing to set guidelines or contingency plans. As a result, few organizations have closely analyzed the ramifications of moving an increasing amount of student interaction online. This paper aims to provide some insight into the liability of technology in marketing higher education.

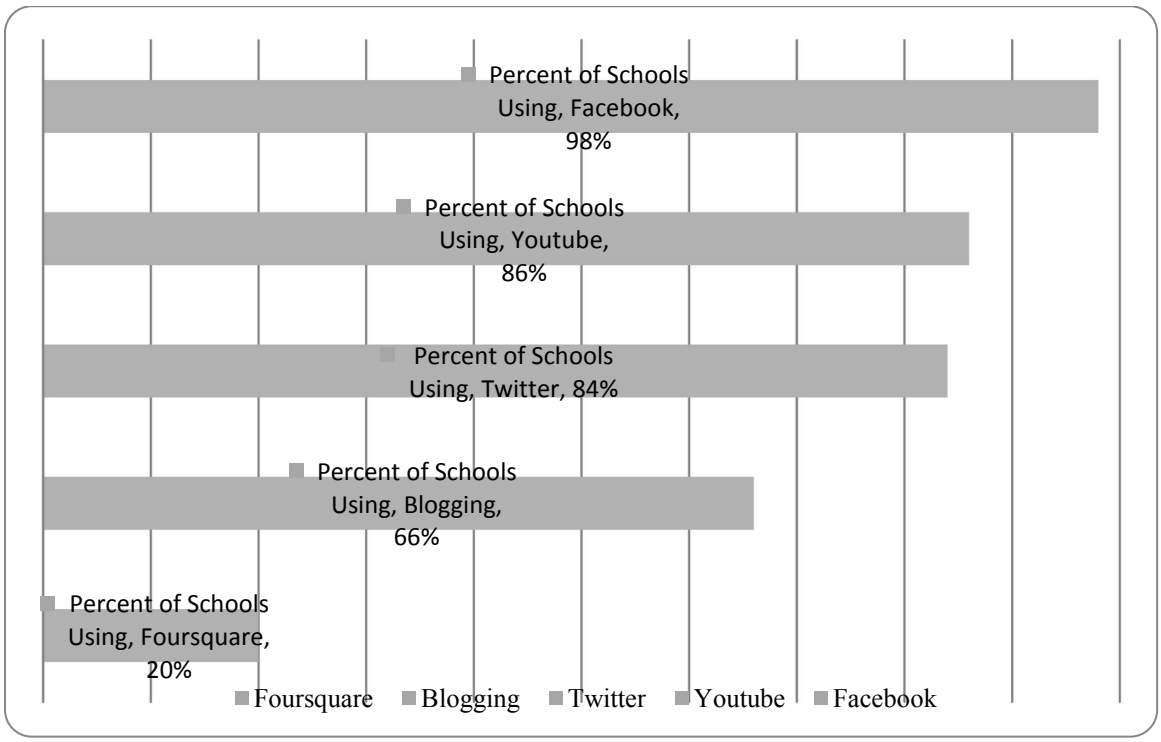
BACKGROUND

In 2007-2008, University of Massachusetts Dartmouth Center for Marketing Research conducted the first statistically significant study on the usage of social media by US colleges and universities. They discovered that 61% of the surveyed respondents were using some form of social media. In a follow-up survey one year later, that number rose to 85%. The next year's study, from 2009-2010, revealed 95% of schools had adopted social media. Finally, in this year's most recent survey, UMass revealed that 100% of the institutions surveyed were now using a least one social media tool. In a mere 4 years, adoption skyrocketed from 61% of colleges and universities to 100%. (Barnes & Lescault, 2011). Such dramatic change often has unforeseen consequences and unanswered questions. Are these new communications held to the same standards as other student interactions? What happens when students or staff post inflammatory speech to one of these social media technologies? Are there privacy concerns to account for? What about safety issues when using location-based interaction tools?

To better analyze the potential dangers, we must understand the technology at hand. By far the most popular social media among schools is Facebook, with 98% having at least one Facebook page (Barnes & Lescault, 2011). Some institutions, praised for the social media presence, have a great many Facebook pages and accounts; the University of Texas at Austin, for example, has over 200 accounts (Tsouvalas,

2011). It is not only popular with institutions, but Facebook is king among college students as well. In a forthcoming study, a survey of public and private undergraduate institutions revealed 96-97 percent of students use Facebook (N.J. Barnes, 2011). It is not surprising that a social network originally conceived for a college audience is so popular among that very group, as well as the institutions they attend. The second most widely used service per the UMass study is YouTube. Eighty-six percent of schools utilize the free video site. In addition to Facebook and YouTube, Blogging remains quite popular, with two-thirds of all institutions currently using the format. Twitter, considered a "micro-blog," was assessed separately, and 84% of colleges and universities report using the short-message tool. Additionally, we should also be aware of Foursquare. The location-based social media service is currently in use at 20% of the surveyed schools (Barnes & Lescault, 2011)

FIGURE 1
SOCIAL MEDIA ADOPTION IN HIGHER ED



The technologies above are the most prevalent in the higher education world, and represent a good cross-section of tools and services. Some, like Facebook, Twitter, and Blogging, allow organizations to communicate and interact directly with their target audience. Others, like Foursquare, provide entertainment for users while simultaneously promoting the institution. YouTube is largely an information delivery tool; some schools broadcast lectures or class samples on the video site, while others prefer to utilize it for campus tours and messaging. The key that links all of these technology products is that there is always an exchange of information. Typically the information flow is largely one-way, from the college or university to the consumer, yet all of these tools allow users to contribute via comments or replies. Some of these tools exchange even more than communication, raising privacy concerns. Navigating this exchange will be the crux of this paper's discussion.

DISCUSSION

When the Conversation Goes Bad: Censorship and Defamation

Against this backdrop of technology, certain legal issues loom larger than others. As mentioned earlier, all of these new technologies afford users the ability to discuss, comment, vote, or otherwise communicate with other users of the platform. As such, defamation and censorship are challenges that arrive hand in hand with communication. Defamation, or the harmful communication of false claims, is a concern for any public facing entity. There is a delicate balancing act between freedom of speech, protected by the United States Constitution, and defamation, which predates the country itself (Zenger, 1736). Further, censorship has always been a thorny issue, particularly in the world of education. There are two perspectives to analyze here, depending on whether the actor is an agent of the college or university, or a third party.

The third party speaker is a frequent cause of worry for anyone active in social media. The very design of "Web 2.0" is about user contributions and conversation, yet sometimes users say things that are troubling, if not downright offensive. Some commentators theorize that the anonymity of the Internet, combined with an audience, brings out the worst in people. New York University professor Clay Shirky, who studies social and economic effects of Internet technologies, explains: "There's a large crowd and you can act out in front of it without paying any personal price to your reputation," which "creates conditions most likely to draw out the typical Internet user's worst impulses" (Doig, 2008). What is an organization to do when confronted with such vitriol?

The first question a college or university should consider is whether or not the disconcerting comments can be redirected in a positive way. What starts as an angry rant might be an opportunity to engage the community, or demonstrate that these are the words of a bitter few. This is likely contrary to our instincts; when faced with things we don't want to hear, it is often easier to ignore or silence those things than deal with their meaning. Some of the technologies discussed here give organizations the ability to delete comments as they see fit. This opens up notions, however spurious, of censorship. While private institutions rarely encounter this problem, it is slightly more challenging for public institutions, as state actors are held to higher standards when it comes to freedom of speech.

Generally speaking, there are three justifications for deleting someone's comments or speech online. The first thing to bear in mind is that hate speech and threats are never protected, and one can remove such language without a problem. Next, if the site is run by another company (Facebook or YouTube, for example), all the content must be permitted by the site's terms of service, and violations can be flagged or reported. Finally, the organization must consider if the material in question is on one's own private site.

An institutional blog is one such example. As the host, the school may decide what content should be permitted on their site. This is true even for public institutions. The trend in the US thus far has been to err on the side of removing content. For example, recently the government requested YouTube censor the "Occupy Wallstreet" videos, and Yahoo to filter email relating to the protest (IBTimes, 2011).

Again, the best defense to avoid censorship liability is to try and deal with the comments, rather than rely on removal. This benefits an organization should they handle it successfully, and reinforces the commitment to discussion and interaction with its users. On a cautionary note, even if censorship meets one of the three circumstances above, it may have non-legal ramifications. There is a tendency on the Internet to thwart attempts to hide or remove information, thereby making it even more public. This is colloquially known as "the Streisand Effect," after the famed singer sued a coastal erosion photographer for including her beachfront property in his project. Rather than censor the image, it was quickly shared across the Internet (Greenberg, 2007).

No matter what users contribute to the site, the organization will not be held accountable for the content of third parties, particularly when it comes to defamatory statements (Communications and Decency Act, 1996). Colleges and Universities are not nearly as protected when the statements come from their own staff, however. In the race to provide content and communication channels to current and incoming students, many schools have engaged a wide variety of stakeholders to post, blog, and tweet. No longer limited to the marketing department, many schools, departments, and programs have student

bloggers.

Just because these technologies are new does not excuse an institution from being responsible for what is said on its behalf. Few organizations would let an amateur represent them on live television, but would instead rely on a public relations professional. The Internet reaches far more people, is more permanent than broadcast TV, and yet many digital representatives have no formal training in speaking to the public. As a result, using these new technologies exposes schools to more defamation liability. Should a representative make any false statement to hurt another's reputation or standing in the community, the school would ultimately be responsible.

Check-In Here: Geolocation and Privacy

Social media is not the only technology that is changing the face of interaction; the proliferation of "smart phones" has had a profound effect on the Millenial generation. Last year, survey data from two campuses in the Northeast showed between 48-50% of students have smart phones, or phones with advanced Internet and computing capabilities (N.J. Barnes, 2011). By contrast, over one quarter of all phone sales this year are projected to be smart phones (Biggs, 2011). Today's youth is clearly in the lead regarding smart phone adoption. Of the many features these phones offer, "Geolocation" is the most troubling for privacy proponents. Essentially, one's phone can act like a very precise GPS transmitter. This means the user can not only get directions, like a traditional GPS device, but it also means that various activities broadcast the user's location.

Facebook, for example, allows users to post updates and have the origin of the update "tagged" by the phone's location service. Foursquare, the youngest technology discussed here, is specifically built around the geolocation feature. Users "check in" to different businesses, groups, or events based on their current location. Other users can see who is currently attending an activity, who has been there, and when they checked in. To compete, Facebook now offers "Facebook Places," which provides similar features as Foursquare. Many schools are utilizing one of these geolocation services for marketing. In Student Advisor's assessment of the top 100 Social Media Colleges, Harvard placed second overall largely on the strength of their 70+ Foursquare check-in locations (Tsouvalas, 2011). The University of Kentucky embraced Facebook Places across their campus. Kelley Bozeman, the school's marketing director, told Ad Age, "we're encouraging students to check in, so when they do, it'll show up in their news feed and maybe their friends still in high school will see it over and over again" (Patel, 2010).

The legal problems here are twofold. One is an issue of privacy – should a school be soliciting where students are, and when? When it comes to privacy in general, there are fewer areas of the law more murky and unsettled. Privacy itself is not granted by law, but assumed from a number of other rights, like the Third and Fourth Amendments, for example (Griswold v. Connecticut, 1965). As such, privacy can be challenging to pin down and define.

The fear among students and privacy rights advocates is that services like geolocation is sharing information with people who we don't want aware of our movements. Providing where someone is located and when he or she arrives may unintentionally aid a cyberstalker. Facebook check-ins and status updates have already led to numerous robberies, as enterprising thieves knew precisely when someone was not home (See Chan 2010; Collins 2011; Roberts 2010). Can a school be held accountable for these status updates?

Probably not. The Supreme Court has ruled that privacy, especially from the government, extends to all places where we have a reasonable expectation to be private (Katz v. United States). It stands to reason that if a student chooses to "check in" to a location via their smart phone, they are not expecting that information to be private. This is the line of reasoning that University of Kentucky offers. "We do think about privacy," says Ms. Bozeman, "but this is about check-ins during the day, when you're on campus, in the classrooms and going to athletic events. Adults use good judgment" (Patel, 2010). The issue remains challenging when dealing with freshmen and incoming students, who may not be eighteen yet. Not only may their judgment be less reliable, but the school is also exposed to our second concern.

The other issue comes from FERPA, the Family Educational Rights and Privacy Act. FERPA generally prohibits the disclosure of student's personally identifiable information without written consent

from the student or, if a minor, the student's parent or guardian. Clearly, schools are not asking for written consent when they request students check-in to events or locations on campus. On the other hand, the data is not academic in nature, and FERPA is centrally about handling academic information (FERPA, 1974).

Unfortunately, there is no clear consensus on how location check-in's should be handled under FERPA. Until there is, to avoid potential liability, many schools encourage students to try geolocation without making it mandatory, or tied to any school incentives. Facebook and Foursquare themselves might ease this argument. At current, there are several ways to determine someone's location, even if they did not want you know. These include Foursquare displaying pictures of its checked-in users (regardless of their privacy setting), the ability to check in friends to your Facebook Place, and sometimes on either system by simply attending the same event or location. Should the companies shore up these privacy issues, schools can worry less about personal information being exposed to unknown third parties.

CONCLUSION

As colleges and universities rapidly embrace new technology and tools, they should keep in mind the standards of communication that have served them well in past endeavors. Communication online is no different than any other external communication, and poses many of the same risks. An organization can reduce its liability by planning ahead. A simple social media policy can help dictate who should be posting where, and what messages people should emphasize. Further, a one-hour session on the risks and dangers of social media could save months of headache down the road.

Even if the services change, and technologies give way to the next big thing, the challenge remains the same. Online, what you say and do is visible to the whole world, and should be treated as such. A little bit of planning, strategy, and training can go an incredibly long way in avoiding legal conflicts down the road. That way when the next great social media technology emerges, we will know what to expect before we forge ahead.

REFERENCES

Barnes, Nicholas J. "College Student Social Media Use, Comparing Public and Private Institutions." (2011, Spring) Forthcoming.

Barnes, Nora G. and Ava M. Lescault. "Social Media Adoption Soars as Higher-Ed Experiments and Reevaluates Its Use of New Communications Tools." *UMass Dartmouth Center for Marketing Research*. (2011, July) Retrieved from: http://www.umassd.edu/cmr/studiesandresearch/socialmediaadoptionsoars/.

Biggs, John. (2011, July 27). "Smartphone sales will hit 420 million in 2011 to take 28 percent of the total market." *Techcrunch*. Retrieved from: http://techcrunch.com/2011/07/27/smartphone-sales-will-hit-420-million-in-2011-to-take-28-percent-of-the-total-phone-market/.

Chan, Casey. (2010, September 12). "Robbers Checked Facebook Status Updates To See When People Weren't Home." *Gizmodo*. Retrieved from: http://gizmodo.com/5636025/robbers-used-facebook-to-see-when-people-werent-home.

Collins, Pat. (2011, August 19). "Facebook Folly: Status Told Robber About Vacant Home." *NBC Washington*. Retrieved from: http://www.nbcwashington.com/news/local/Facebook-Folly-Status-Told-Robber-About-Vacant-Home-128098078.html.

Communications and Decency Act, 47 U.S.C. § 230(c)(1). Enacted in 1996.

Doig, Will (February 26, 2008). "Homophobosphere". *The Advocate* (1002).

The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99. Enacted in 1974.

Greenberg, Andy. (2007, May 11). "The Streisand Effect." *Forbes*. Retrieved from: http://www.forbes.com/2007/05/10/streisand-digg-web-tech-cx_ag_0511streisand.html

Griswold v. Connecticut. U.S. Supreme Court, 381 U.S. 479 (1965).

IBTimes Staff Reporter. (2011, September 11). "Occupy Wall Street Activists Accuse Yahoo of Censoring Email." *International Business Times.*

Katz v. United States, 389 U.S. 347 (1967)

Patel, Kunur. (2010, September 3). "U. of Kentucky Encourages Students to Check In via Facebook." *Ad Age.* Retrieved from: http://adage.com/article/adages/college-marketing-effort-facebook-places/145732/.

Roberts, Liz. (2010, December 23). "Police warn of burglary risk from social media sites." *BBC*. Retrieved from: http://www.bbc.co.uk/news/uk-12070679.

Tsouvalas, Dean. "Top 100 Social Media Colleges." *StudentAdvisor.com*. (2011, Fall) Retrieved from: http://www.studentadvisor.com/top-100-social-media-colleges

Zenger, John Peter. (1736). *A Brief Narrative of the Case and Trial of John Peter Zenger*. New York City, NY.

ABOUT THE AUTHOR

Nicholas Barnes, Esq. is the Information Technology Management Chair at Nichols College, where he teaches courses in information systems, social media, law, and security. He is also an attorney, specializing in Internet and technology issues. Mr. Barnes received his Juris Doctorate from UNH School of Law, and his Bachelor of Science from Worcester Polytechnic Institute.