Facebook, Twitter, and Linked-In – all phenomena unknown and unimagined 10 years ago – we now find at the center of modern communications. From students to public relations professionals, media giants to politicians, flash mobs to scientists – social media has become the coin of the realm for disseminating information, advocacy, and keeping in touch.

- Facebook – launched in February 2004 – had more than 750 million active participants in July 2011.
- Twitter – launched in July 2006 – now has 200 million users.
- Linked-In – created in May 2003 – now reports having over 120 million registered participants.

What better way, then, to communicate to and with our campus communities. It is seductive, engaging, and terrifying. How can we harness this extraordinary technology to its best advantage, effectively, without increasing risks of liability and reputational harm?

I. What can we learn from past cases?

II. What are the implications for privacy and First Amendment protections?

III. How can/should social media be used in student disciplinary cases?

IV. What can/should institutions do about cyber-bullying?

V. Should we be developing new social network policies?
I. Case Studies

A. **DUKE WINCES AS A PRIVATE JOKE SLIPS OUT OF CONTROL** (NY Times October 7, 2010): A Duke Student wrote a joke thesis – a 42-Page Power Point presentation – evaluating sexual liaisons with 13 student athletes during her years at Duke – with pictures and graphs. She forwarded this mock thesis to her friends, who forwarded it to their friends. Within days, the “thesis” was published online by two web-sites, exploding onto the blogosphere on email and Twitter.

B. **TO CATCH A THIEF ON FACEBOOK** (ABC News February 28, 2010): A freshman at Arizona State University was arrested in his dorm room by campus police for burglary. The crime was sneaking into a closed dining facility over Thanksgiving weekend and stealing cereal and soda. How was the crime uncovered? Facebook. Officials on campus visited the student profile pages on Facebook and compared them to the surveillance images. It was a regular practice of public safety to use Facebook in the course of its responsibilities.

C. **TO CATCH A THIEF (2)**: The police department at Penn State University reported at least 3 incidents where Facebook led to the arrests of students. In one case, after a football game, many drunk students rushed the field – there was a Facebook page dedicated to students who had participated in the trespass activity.

D. **FACEBOOK, A PLACENTA AND A LAWSUIT** (Inside Higher Ed January 3, 2011 and Chronicle January 6, 2011): Four nursing students at Johnson County Community College in Kansas, MO, were expelled for taking pictures of themselves with a placenta, which the students saw as part of a clinical placement, and then posting the pictures on Facebook. The basis for the expulsion involved issues of demeanor and lack of professional behavior. The students have sued the community college for the disciplinary action taken. A federal judge ordered reinstatement of the ground that the students believed they had obtained permission from their instructor to post the photos, and that the posting did not constitute unprofessional conduct.

E. **YODER V. UNIVERSITY OF LOUISVILLE, 2009 WL 2406235** (W.D. Ky. Aug. 3, 2009): A student nurse was dismissed from a public university School of Nursing because of a MySpace blog posting that the University contended violated the privacy rights of a patient. The blog colorfully described the live birth of a baby that she had witnessed as part of her clinical training. The birth mother’s identity was not disclosed. The court agreed the blog was vulgar, but held it did not violate the professionalism provision of the honor code. The blog was not “unprofessional” but “non-professional” – it was not created or used in a professional context.”

F. **PARTY AT XXX FRATERNITY HOUSE THIS WEEKEND**: On a number of campuses, fraternities and other groups publicize their parties on Facebook. The
University may have no knowledge of the party – since there are no flyers and the party is not registered. If there are alcohol-related injuries or other issues at the party, what is the college’s responsibility?

G. CYBER-BULLYING: RUTGERS:

- VICTIM OF SECRET DORM SEX TAPE POSTS FACEBOOK GOODBYE, JUMPS TO HIS DEATH (September 29, 2010 ABC News): A Rutgers University freshman posted a goodbye message on his Facebook page before jumping to his death after his roommate secretly filmed him during a “sexual encounter” in his dorm room and posted it live on the Internet. Clementi’s post on his Facebook page, dated Sept. 22 at 8:42 p.m. read “Jumping off the gw bridge sorry.” Two students were charged with two counts each of invasion of privacy after allegedly placing a camera in Clementi’s room and live-streaming the recording online on Sept. 19, according to a written statement by New Jersey’s Middlesex County Prosecutor Bruce Kaplan. A Twitter page that appears to have been operated one of the students, but has since been taken offline, shows messages in which the accused student takes credit for the alleged videotaping of Clementi. On Sept. 19, the student tweeted: “Roommate asked for the room till midnight. I went into molly’s room and turned on my webcam. I saw him making out with a dude. Yay.” Student faces two additional counts of invasion of privacy for allegedly attempting to use the camera to view and transmit another sexual encounter involving the same student just two days later, said Kaplan.

- WHERE PRANKS END AND ABUSE BEGINS: (Chronicle of Higher Education October 11, 2010): In the face of the tragedy of Tyler Clementi, cyber bullying has become an even more significant issue in state legislatures, Congress, and college campuses. Senator Lautenberg and Representative Holt have introduced the “Tyler Clementi Higher Education Anti-Harassment Act,” which would require colleges to implement policies that would prohibit cyber harassment defined as: “conduct, including acts of verbal, nonverbal, or physical aggression, intimidation, or hostility (including conduct that is undertaken in whole or in part, through the use of electronic messaging services, commercial mobile services, electronic communications, or other technology that -- “(I) is sufficiently severe, persistent, or pervasive so as to limit a student’s ability to participate in or benefit from a program or activity at an institution of higher education, or to create a hostile or abusive educational environment at an institution of higher education; and

“(II) is based on a student’s actual or perceived –
“(aa) race;
“(bb) color;
“(cc) national origin;
“(dd) sex;
“(ee) disability;
“(ff) sexual orientation;
“(gg) gender identity; or
“(hh) religion.”

• **TYLER CLEMENTI HIGHER EDUCATION ANTI-HARASSMENT ACT THREATENS FREE SPEECH ON CAMPUS** (www.thefire.org November 23, 2010): The Foundation for Individual Rights in Education (FIRE) has concluded that this statute threatens free speech on campus by allowing campus administrators to punish views or expression they don’t like.

**H. ALLEGED SHOOTER WAS SUSPENDED BY PIMA COMMUNITY COLLEGE** (Inside Higher Education January 10, 2011). Jared Loughner, who shot Representative Giffords and others at a political gathering in Tuscon, Arizona, had posted a video on YouTube that resulted in his expulsion from Pima Community College shortly before the shooting. In the video, Mr. Loughner walks around the campus and narrates why it’s a “genocide school.” He was particularly agitated about having received a “B” grade in sociology.

**II. Privacy and the First Amendment**

Our notions of privacy – and more importantly our students’ views of privacy – have been dramatically changed in this new social networking, information age. Students share information that we would consider – TMI. They also use social media in ways that can be inappropriate to outrageous. What is the proper balance between privacy and protections of free and open speech on our campuses and what are the implications for college administrators?

It has long been held that student speech is protected on public campuses by the First Amendment unless that speech can be shown to “materially and substantially interfere with the requirements of appropriate discipline in the operation of the school.” *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969). While this underlying principle is clear, the application of this rule to social media is still the subject of debate. For example, the Third Circuit U.S. Court of Appeals recently
heard en banc a pair of cases involving secondary school students posting negative comments about school personnel. See Shannon P. Duffy, 3rd Circuit Mulls Student Suspensions for MySpace Postings, Law.com, June 4, 2010. In these two cases the trial courts reached opposite conclusions as to whether social media communications were “off campus speech” protected by the First Amendment – or speech that directly impacted the campus community and therefore subject to the Tinker rule. In Layshock v. Hermitage School District, Judge Terrence F. McVerry of the Western District of Pennsylvania found that school officials went too far when they suspended Justin Layshock for creating a fake profile of Hickory High School's principal, Eric Trosch, that said he was a "big steroid freak," a "big hard ass" and a "big whore" who smoked a "big blunt."

In J.S. v. Blue Mountain, on the other hand, Judge James M. Munley of the Middle District of Pennsylvania upheld a 10-day suspension of a student who posted a profile on MySpace in March 2007 that showed a photo of principal James McGonigle and described him as a pedophile and a sex addict whose interests included "being a tight ass," "fucking in my office" and "hitting on students and their parents."

Colleges and universities, as educational communities, are the most important venues for free and open debate – they are the quintessential “marketplace of ideas.” Healy v. James, 408 U.S. 169, 180 (1972). As such, and as a general rule, our institutions restrict any speech, including social media communications, at our peril -- and should do so only when we find that such speech poses a “true threats” to our campus communities, that is “[A] statement which, in the entire context and under all the circumstances, a reasonable person would foresee would be interpreted by those to whom the statement is communicated as a serious expression of intent to inflict bodily harm upon that person.” Planned Parenthood v. American Coalition of Life Activists, 290 F.3d 1058, 1077 (9th Cir. 2002) (en banc), cert denied, 123 S. Ct. 2367 (2003).

III. Should college administrators monitor social media cites?

As a practical matter, it would be impossible for campus administrators to monitor all of their student’s social media accounts, and would raise serious liability risks should they try to do so. The question is, are there any circumstances where monitoring a student’s account is appropriate?

In particular cases, review of a student’s postings may be proper. In cases where administrators have reason to be concerned about a student’s emotional health, limited review may be appropriate. And student disciplinary officers may use social media to find facts about a charge of student misconduct. In order to use social media in this way, it would be helpful if your campus policies made clear when such review is permissible.

IV. Can colleges discipline students for social media postings?
As suggested by the cases discussed above, the answer to this question is not clear. The answer may depend on whether your institution is public or private. But in either case, the answer will most likely depend on the nature of the communication and whether it can be shown to pose a threat to your community.

In a recent case, the Minnesota Court of Appeals upheld the right of the University of Minnesota to discipline a student in a mortuary-science class over comments she posted on Facebook – comments referring to stabbing someone and the use of cadavers in a way that upset the families of anatomy bequest donors. The student argued that the school had no jurisdiction over this off campus activity. The Court rejected that argument, upholding the university’s right to enforce its professional standards. Chronicle of Higher Education, July 11, 2011.

V. How should colleges respond to threatening postings? To arguable defamatory postings? To cyber-bullying?

When administrators are made aware of postings that may be threatening, or harassing, or defamatory, the community will often expect an aggressive response. This presents a significant challenge. Colleges and universities are frequently limited as a matter of law from taking strong action to restrict speech – and such action may violate campus policies and principles that foster open and free discussion.

That said, cyber-bullying and threatening communications and defamatory postings are very much in the news and cannot be treated lightly or ignored.

- Cyber-bullying: Two letters from the Department of Education’s Office of Civil Rights (“OCR”) remind institutions about their multiple responsibilities when responding to student harassment. First, it is critical for institutions to be mindful about students’ free speech rights, as anti-harassment laws are not intended to undermine the First Amendment. See Department of Education “Dear Colleague” Letter re First Amendment Issues (July 28, 2003). Second, student misconduct that falls under an anti-bullying policy also may trigger responsibilities under one or more of the civil rights laws enforced by OCR. See Department of Education “Dear Colleague” Letter re Bullying (October 26, 2010). This will include peer harassment based on race, color, national origin, sex or disability that meets the standard articulated by OCR.

While institutions do not have a duty to respond to every objectionable or offensive statement, they are obligated to respond to student harassment that is “sufficiently severe, pervasive, or persistent as to interfere with or limit a student’s ability to participate in or benefit from the services, activities or opportunities offered by a school.” A higher education institution has a responsibility to respond to harassment that takes place in any medium over which the school has “substantial control,” such as a University-sponsored online discussion forum. The most recent OCR “Dear Colleague” letter suggests an institution may also have a duty to respond to online harassment.
over which it has no control or oversight, provided it knew or reasonably should have known about it.

• Threats. Threatening postings may also require some action by a college or university. As reported in the Chronicle November 18, 2010, police officers in Florida arrested a student at Lynn University for allegedly posting a threatening note on Facebook. The Facebook message was said to include a taunt that the student would cause a “Columbine High School incident,” referring to the infamous school shooting in 1999. The student, Daniel Shana, told investigators that he had no intention of hurting anyone, though the police say he had posted threats on Facebook directed at his ex-girlfriend as well. “Quickwire: Lynn U. Student Arrested for Allegedly Posting Threat on Facebook”, The Chronicle of Higher Education, November 18, 2010.

• Defamation: With respect to postings that are arguably defamatory, you may well hear complaints from students or parents asking you to “take down” the posting or discipline the offending student. Administrators don’t have the ability to “take down” a posting, and may be limited in what they can offer in response. The best option is often to provide education and counseling – and to make sure your policies on open expression are clear.

VI.

VII. Should Institutions Develop a Social Media Policy?

There has been considerably discussion of whether campuses should adopt a specific policy governing the use of social media. It is not clear that this is needed – or even possible given the changing technological landscape. A different approach is to review your open expression policies and make sure that they are in sync with social media realities, and that they are sufficiently broad to cover social media communications.

Penn is in the process of developing a social media guidance document. The Office of Audit, Compliance & Privacy has already put together a document called “Top 10 Facebook Privacy Settings”, which I’ve attached as Attachment “A”

Conclusion

Social media provides a wealth of opportunity and challenges in the educational environment. It is important to be mindful of both the risks and benefits, and to make sure that your campus policies are robust enough to provide guidance in dealing with the many new issues that are arising as a result of the new technologies and cultural norms.
REFERENCES:

NACUA NOTES March 16, 2011, Vol. 9 No 7. From Tinker to Twitter: Managing Student Speech on Social Media, Denielle M. Burl, Special Assistant to the Vice-President, University of Connecticut.

http://blog.nielsen.com/nielsenwire/social/

http://www.upenn.edu/privacy/Brochures/top10fb.pdf
Top 10 Facebook Privacy Settings

This document describes important settings on Facebook to help you protect your privacy. Bear in mind that Facebook is a powerful interactive tool with significant and often complicated sharing capabilities. Also, Facebook often changes its privacy policies and practices. So, you should not share sensitive, private information on Facebook. Still, there are steps you can take to help protect your privacy for the information you do share on Facebook.

1. **Where to Start.** To start, click on “Account” and then select “Privacy Settings.” Then, you must click on the “Edit Your Profile” link to bring up a wide range of important choices you have regarding privacy.

2. **Friends Lists.** Before making those choices though, start making Friends Lists, as those lists may be just what you wish to select when setting privacy preferences. To make a Friends List, click on “Account”, then “Edit Friends” and then choose “Create a List.” Start putting together lists like “professional”, “family”, “high school”, or any that you wish. You may also create categories like “All My Friends Can See” and “Only My Most Trusted.”

3. **Edit Your Profile – Sharing Choices for Your Data. Don’t Forget the “Custom” Option.** Returning to the “Edit Your Profile” link via the Privacy Settings page, work your way through all of the categories of data that you can input and share (clicking on categories from “Basic Information” to “Contact Information”). For each data field shown, click on the lock on the right to show a drop down menu of choices. Select the one that is right for you.

   To protect your privacy, try restricting access to “Friends Only” or an even smaller subset, such as a Friends List. You can do so by selecting “Custom” on the drop down menu, then “Select Specific People” and then type in a Friends List or specific people. You can also use “Hide this from” to exclude a Friends List or specific people. You can choose these same options as you post and for each post, again, using the lock button and the drop down menus. You can now also use the “View As” button on the top right to see how your profile appears to named people.

4. **More Choices: How You Connect.** Now return to Privacy Settings and click on “How Your Connect.” Here Facebook provides choices on who can look you up, who can send Friends requests, messages, and post on your wall, and who can see wall posts by others. Walk through these steps, remembering that the Custom button allows you to restrict to Friends Lists and specific people.

5. **Tags: Limited Control.** Back to Privacy Settings, under “How Tags Work,” you can preview and reject certain tags about you and others. Bear in mind that the only control you have is what appears on your profile – your page. Tags about you – made by Friends or other “non-Blocked” people -- still appear throughout Facebook on other pages.

6. **Pay Special Attention: Your Location Information.** Under the “Tags” control area in Privacy Settings, pay special attention to the option “Friends Can Check Your Into Places.” For safety and other privacy reasons, you may not want any “Friend” to be able to tell every Friend or possibly the public where you are. Make sure this feature is “Off” or “Disabled” if you are concerned at all. Also, think twice before checking yourself into places as you post.

7. **What Your Apps and Friends’ Apps Grab from Your Page.** Return to “Privacy Settings” and click on “Apps and Websites”. Then click on “Apps you Use” and “How People Bring Your Info Into Apps They Use” to see which apps are taking which types of information from you – and to stop it. While you’re there, also make sure “Public Searches” is not enabled – or you will have any search engine search of your name turn up your Facebook profile.

8. **Block Lists.** Block people and apps that are concerning to you. Through the “Block Lists” on “Privacy Settings,” you can stop certain individuals from interacting with you on Facebook. You can also block apps and invitations.

9. **Facebook Ads.** Another stop on the road to good privacy settings is at “Account,” then Account Settings”, then “Facebook Ads”. Set your available options to “No one” for the most privacy protective approach.

10. **Security.** Take advantage of some good security options. Click on “Account”, then “Account Settings”, “Security”, and select “Secure Browsing”. You should also consider using “Login notification” or “Login Approvals”.

   Facebook changes its terms of use and privacy practices often. Reading up on and talk about Facebook privacy to make sure that the choices you make are thorough and do what you want them to do!