Social Media Legal Issues—Virtual Friends/Real Problems

By Francisco J. Valenzuela

Odds are that most of you are part of the hundreds of millions of people who are connected to some form of social media. With the rise of ever new social media avenues with evolving capabilities, new legal issues arise. What are those issues and how are they dealt with by a legal system designed for the "brick and mortar" world? The aim of this brief paper is to raise some issues employers, employees, schools, parents, students, and courts must contend with in the 21st century.

I. Social Media Issues at Work

It is nothing new that employers concern themselves with the activities of their employees, particularly those activities that affect their work. In addition, employers face ever new laws and regulations as to how their employees are to be treated, working conditions, etc. What is new, is that in addition to those "traditional" areas of employer concern, now employers must be concerned with social media and their impact on the workplace. Employers could find themselves liable for an untold number of claims based on their employees' use of social media.

A. Sample Issues

1. Defamation

Imagine that an employee at work is using her employer's computer and goes onto Facebook. While on Facebook she makes defamatory comments about a person, while mentioning that this is her company's opinion about the person as well. If a lawsuit is filed, it is possible that the employer may be included as a defendant to the suit.

2. Discrimination

A recent article in a legal magazine discussed the ins and outs of searching social media sites for evidence when a lawsuit has been filed. Any statements made by employees, whether at work or not, could be discovered during litigation and used as evidence of discrimination. So, for example, ABC Company is being sued for racial discrimination. The plaintiff claims that his supervisor treats him differently because he is African American. The company denies it, and as part of discovery, produces its internal emails. None of the evidence produced by the company shows any hint of discrimination. However, the tech-savvy plaintiff's attorney subpoenas access to the supervisor's social media sites. On the supervisor's

Facebook page, it is discovered that the supervisor made a discriminatory statement concerning African Americans or has friended or become a fan of a known white-supremacist group or person. This could make the difference between summary judgment and settlement.

3. Retaliation

This should be, perhaps, one of the areas of greatest concern for employers in regards to employment law based suits. In *Burlington Northern & Santa Fe Ry. V. White*, 548 U.S. 53 (2006), the U.S. Supreme Court held that a material retaliatory adverse employment action can be *anything* that might dissuade a reasonable employee from filing a complaint against his employer for discriminatory conduct. The Court specifically stated that context matters; conduct *outside* of work could be considered retaliatory.

Assume that a female employee complains to her supervisor that a male employee is sexually harassing her. The supervisor keeps the matter private in the office and follows the employers' practices and procedures for handling the matter. That night, however, the supervisor goes home and discusses the harassment complaint in detail on Facebook, disclosing the who, what, why, and how of the complaint. Numerous of the complainants' co-workers see the post. The next day, the office is buzzing and the complainant is embarrassed, confirming her fears that she shouldn't have reported the harassment. A court could find that the supervisor's actions were retaliatory and the employer could face damages.

4. Disclosure of Information

Employers should also be concerned that their employees not divulge confidential client or company information. In the legal context, a young, gabby lawyer might be in a meeting with a client and tweet about how he thinks that client X (maybe identifying the client in some manner) has no case because he was drunk when he ran the stop sign. This could be a violation of the attorney-client privilege and could result both in adverse results to the client, the firm, and the lawyer.

Another scenario, which has happened, is that an employee working at ABC Company posts the Company's new logo or product on her Facebook page because she thinks it's cool. The problem is that neither the logo or product have become public. An employee with access to confidential information could leak that information or discuss the information, harming the Company and costing it hundreds of thousands of dollars, or worse.

B. Social Media in Employment Decisions

1. Hiring

Employers are using social media sites when deciding on new hires. In fact, the city of Bozeman, Montana made headlines when it required new hire candidates to provide their online credentials to their social media sites so that the city could review the sites. After public outcry, this policy was changed.

It is understandable that some employers might choose to do this in order to avoid embarrassment, or worse, if it turns out that their new hire, who may be in a sensitive position or in a position of trust, engaged in questionable conduct. While employers may see a benefit to doing this, it also opens employers

to liability. Private employers may face liability based on, for example, the employer's failure to hire a female after seeing pictures of her antics during a party, but hiring a male employee who had pictures of a similar nature. In other words, an employer cannot be tagged for liability for making decisions based on social media information if it did not access the pictures and made the very same hiring decision based on other criteria.

With access, comes additional knowledge for which liability can attach, or at least be the basis for a claim that will have to be defended. Additionally, government employers should be aware that First Amendment issues are also present. There is much conduct that can be claimed to be "expressive", but make other people uncomfortable.

Regardless of the pitfalls, employer use of social media information regarding new hires is a growing trend.

2. Employee Discipline

Just as some employers are using social media sites to make hiring decisions, many employers use comments made or pictures posted by employees on social media to discipline employees. For example, in *Snyder v. Millersville Univ.*, 2008 U.S. Dist. LEXIS 97943 (E.D. Pa. 2008), a school district removed a student teacher from her position for her postings on her MySpace site concerning another teacher and her pictures showing her as what was described as a "drunken pirate". The school had warned student teachers during their orientation not to make comments on social media sites about their students or other teachers. Snyder disregarded that advice and was terminated from her student teaching position at the high school, preventing her from being certified through Millersville University.

A comprehensive list of examples is impossible to collect because the practice of disciplining employees for social media content is rampant. However, employers should beware because significant legal issues specific to social media communications can arise, in addition to discrimination and retaliation claims. For public employers in particular, the First Amendment can be asserted by employees as a basis for challenging employer action based on social media posts. All employers must be wary of invasion of privacy claims and violations of the Stored Communications Act. Under the Social Communications Act, it is a violation to "(1) intentionally access without authorization a facility through which an electronic communications service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system." The case law interpreting the Act is complex and employers are encouraged to contact lawyers *before* accessing any electronic and social media employee communications that could be considered private.

In *Pietrylo v. Hillstone Restaurant Group*, 2009 U.S. Dist. LEXIS 88702 (D. N.J. 2009), a jury found that the defendant violated the Stored Communications Act by accessing a private MySpace page without authorization. In *Pietrylo*, a supervisor asked an employee for the access password for a MySpace group set up by employees and former employees to gripe about the employer. This was a private, by invitation only group. The employee who was asked for the information thought that something adverse would happen to her job if she did not provide the information to the supervisor, though no such threats were explicitly made. The court held that the jury could have reasonably found this "authorization" to be

coerced, making the employer's access of the MySpace page unauthorized. The court also held that the jury could reasonably find that the employer's numerous visits to the private MySpace page, that was clearly marked as such, were purposeful and not accidental. Moreover, the employer continued to access the page, even when it knew that the employee who had provided the password information was uneasy about having provided it. The defendant was subject to both compensatory and punitive damages.

C. Comprehensive Social Media Policies

Employers should establish policies addressing social media. There is no "one size fits all" policy, because no two employers are alike. An employer's policy should vary based on the particular characteristics of the employer. A sample policy from the Texas Workforce Commission is included as an attachment to this paper as a sample policy, though we are not endorsing the policy in whole or in part in any fashion. The following are issues that should be addressed in some manner in any social media policy:

1. Definitions

It is important that employers define social media. Such definitions can include specific examples of social media sites existing today (i.e. MySpace, Facebook, Twitter, etc.), but the definitions should also be flexible enough to include future social media that have not yet been created or come to prominence. Technology and social media are evolving at dizzying rates, and a policy with a broad definition of what "social media" includes will help employers stay ahead of the curve.

Employers should, however, try to stay abreast of developments in the social media area to be sure that the definitions in their policies cover emerging technology and sites. If existing definitions are found to be lacking, then employers should promptly take action to adjust their policies accordingly.

2. Expectation of Privacy

All employer policies should be crystal-clear as to whether employees should have expectations of privacy on their work computers and other work-sponsored electronic media.

In *City of Ontario, Calif. v. Quon*, 130 S. Ct. 2619 (2010), the U.S. Supreme Court held that an employer's search of an employee's text messages from an employer-issued pager was reasonable under the circumstances. The City provided its police officers with pagers which had a monthly limit. On several occasions, Officer Quon exceeded the monthly limit and personally paid the difference out of his own pocket. The Police Chief, wanting to know whether the City's monthly limit was sufficient, requested the City's service provider to provide copies of the transcripts of Officer Quon's text messages for a two month period. A review of Officer Quon's text messages showed that many of his on-duty text messages from his employer-issued pager did not relate to police business and, as a result, Officer Quon was disciplined. Officer Quon filed suit alleging his Fourth Amendment right was violated by the City's review of his text messages.

The Supreme Court did not resolve the parties' disagreement over Officer Quon's privacy expectation but disposed of the case on narrower grounds. The Court assumed that Officer Quon had a reasonable privacy expectation and found that the City's review of Officer Quon's pager transcript was

reasonable because it was motivated by a legitimate, work-related purpose and it was not excessive in scope. The Court found that the review was for non-investigatory work-related purposes to find out if the monthly limit was appropriate – i.e., was an employee paying for work-related text messages or was the City paying for an employee's personal use. The Court found that the City's review of the transcript was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messages or personal use and it was not excessively intrusive since it was limited to just two months. The Court found no Fourth Amendment violation, but under different facts, a different result is possible.

3. Trade Secret and Private Information

Employer policies should clearly state that trade secrets and confidential information are not to be shared in any manner on social media sites.

4. "Friending" Restrictions

For those who may not know, social media users can "friend" other persons. If two persons become "friends", they have access to the other's postings. Private employers may consider restricting whether employees can "friend" each other in order to reduce the possibilities of employee-on-employee conflicts arising. A milder restriction could be to prohibit supervising employees from "friending" supervisees or lower rung employees. As supervisors are often the ones accused of sexual harassment and retaliation, prohibiting this type of "friending" could help reduce claims.

Public employers should beware when crafting such restrictions, however, because they could open the employer to First Amendment challenges based on free speech and association grounds.

5. Use of Employer Machines for Social Media Purposes

Both private and public employers may consider whether to limit or completely restrict employee access to social media sites on employer-owned or sponsored equipment. Not only should this make employees more efficient, but it removes the possibility of inappropriate images contained on social media sites from being displayed at work. Additionally, this reduces the time that employees have to engage in inappropriate behavior against co-workers online. For example, co-worker employee Facebook feuds sometimes carried on at work can make co-workers who are not involved in the feud uncomfortable.

6. Disciplinary Consequences

Employee policies should clearly indicate what disciplinary consequences may occur for violation of the social media policy. The policy should be straightforward, practically enforceable, and should be enforced. Any appeals process should be clearly laid out and followed.

II. Social Media Issues and Schools

It is no secret that social media engines are used and abused by students. News stories about cyberbullying, sexting, defamation, capturing sexual encounters, and the often tragic consequences that

ensue are constant. What follows are various legal issues that arise and some considerations as to how they can be addressed.

A. Students' expectation of privacy – cell phone search and seizure

After hearing rumors about sexting for example, generally speaking, the only way that school officials can confirm whether sexting is occurring is by searching a phone. Unless a student and his parents' consent, preferably in writing, to the search of the phone, school officials need to consider whether their search violates the Fourth Amendment or the federal Stored Communications Act.

The standard for a valid search under the Fourth Amendment in the school context by administrators is that the search must be justified at its inception and reasonable in scope. *New Jersey v. T.L.O.*, 469 U.S. 341 (1985). There do not appear to be any reported cases containing a judicial decision regarding the merits of a Fourth Amendment challenge to the search of a student's cell phone. In *Klump v. Nazareth Area School District*, 425 F. Supp.2d 622 (E.D. Penn. 2006), the district court denied a motion to dismiss based on qualified immunity in a case wherein the plaintiff claimed violation of his Fourth Amendment rights when school administrators searched his confiscated cell phone and dialed numbers found on it. In *Klump*, the cell phone had been originally confiscated because it was a violation of school policy to display or use a cell phone while at school. School administrators called other students whose numbers appeared in the plaintiff's cell phone to see if they were also in violation of school policy.

The situation in *Klump* is different than a situation, for example, where a student shows an administrator a nude picture (or some other inappropriate communication) that he received on his phone. An administrator could reasonably confiscate the phone and determine where the text had originated. It would be advantageous to schools and their employees if there is a clear district policy prohibiting sexting and allowing administrators to search phones if there is a reasonable suspicion that school policies had been violated. Please note that if a police officer or school resource officer were to conduct the search a more stringent probable cause standard may apply.

In addition to the Fourth Amendment, school officials must also be careful not to violate the federal Stored Communications Act. As explained above, under the Act, it is a violation to "(1) intentionally access without authorization a facility through which an electronic communications service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system." This is a complex area of the law and lawyers should be consulted. Unless a student comes up to an administrator and voluntarily shows her a sexted image, for example, schools are encouraged to try to obtain written consent from the student and parents prior to searching a cell phone. If consent is denied, cell phone companies can be the subject of search warrants and subpoenas.

B. Protecting confidential student information

Schools must comply with the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g). Under FERPA, with few exceptions, schools are prohibited from disclosing student identifying information. FERPA's reach is very broad and encompasses all information that could reasonably identify a student. FERPA's prohibitions cover disclosure of identifying information on social media sites. For this

reason, schools should consider amending their policies to specifically prohibit disclosure of such information on social media sites.

C. Student discipline for social media communications – What can schools do?

The contours of a school's ability to discipline students for social media communications is an unsettled area of the law. As a general proposition, it appears that schools and their officials can discipline students for off-campus conduct. What that means, practically, is anything but certain. For example, the Third Circuit issued two opinions on the same day in two separate cases having to do with students who created fake social media pages about their principals. In one case, one panel of judges held for the school district and their punishment of the student. See *J.S. v.Blue Mountain School District*, 593 F.3d 286 (3rd Cir. 2010). In the other case, another panel reached the opposite conclusion. See *Layshock v. Hermitage School District*, 593 F.3d 249 (3rd Cir. 2010). Both opinions were later vacated and oral argument was heard by the full Third Circuit sitting *en banc*. The common thread that appears to run through these and other similar cases is the application of the Supreme Court standard issued in *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969): a school cannot suppress a student's speech unless the school officials reasonably conclude that it will "materially and substantially disrupt the work and discipline of the school." Courts will look to whether the speech was made on or off campus, as well as whether it caused would reasonably cause disruption. In *J.S.* and *Layshock*, however, it seems that the two panels considered on-campus occurrences of the same kinds, but reached different results as to whether they were disruptive under *Tinker*.

The fact that this is an entirely unsettled are of the law should not lead school officials to believe that they are automatically entitled to qualified immunity. In *Evans v. Bayer*, 684 F.Supp.2d 1365 (S.D. Fla. 2010), a district court denied qualified immunity to a school principal who was sued for disciplining a student who created a Facebook page criticizing a teacher. The *Evans* court analyzed its case using *Tinker* and was decided after both *J.S.* and *Layshock*.

Other types of student misconduct through social media communications is wide-ranging. For example, cyberbullying, the ugly 21st century face of 20th century bullying is common. There is no limit to what can be said, whether true or not, or how far the bullying is disseminated worldwide. Another example is sexting, the forwarding of sexually explicit pictures of oneself or one's peers via text message. Sexting is occurring at an alarming rate. In recent studies, it appears that 1 in 5 teens have sent or posted nude or semi-nude pictures of themselves online or sent them via text message, and 22% of teens reported to have received a nude or semi-nude picture. It appears that 85% of sexting appears to take place between boyfriends and girlfriends, but 15% of teens questioned admitted to forwarding pictures to persons they only know online. Many times, a female will send nude or semi-nude pictures of herself to her boyfriend. Four weeks later after the couple breaks-up, the ex-boyfriend forwards the pictures of the ex-girlfriend to others. As with cyberbullying, there is no limit to how far the pictures might go.

What should schools do if sexting is found? Be careful. The National School Boards Association's Council of School Attorneys have made numerous recommendations that should be considered. See "Inquiry & Analysis – Sexting at School: Lessons Learned the Hard Way." First, the school district should inform the parents of the students involved. Second, report the sexting to the police. Schools should be aware, however, that the possibility exists for some of the offenders to be prosecuted as sex offenders or for

possessing child pornography. Third, report the sexting promptly as possible child abuse (assuming that that there is a good faith belief that a child could be the subject of the sexting). This is important in Texas as all persons are required to report possible child abuse to law enforcement officials (or other appropriate entities) under Texas Family Code § 261.101. Fourth, school districts should minimize its exposure to child pornography charges. Minimization of possible charges can be accomplished by prompt reporting of the sexting to law enforcement authorities; keeping the offending images off of school technological equipment (i.e. showing police the offending images off of a student cell phone, when possible); and not showing the offending images to any school personnel who is not strictly required by the job position to view the images in order for an investigation to be conducted. Fifth, even-handed discipline of students involved in the sexting. Schools should consider whether or not to discipline students who received the messages, viewed them, but then quickly deleted them. Sixth, prevent the harassment and bullying of students involved in the sexting. Students who are the subject of unauthorized sexting can become distraught and some have committed suicide. Additionally, schools should consider enacting anti-sexting policies.

Time is necessary for courts and the law to catch up to the social media revolution. It is not clear how courts will resolve the significant issues involved in such cases concerning student rights under the First Amendment or other laws. An area in which there are no reported cases but which may be ripe for creative plaintiffs' attorneys is asserting Title IX claims against school districts. For example, it seems possible that claims may be asserted against a school district for on-campus effects of cyberbullying or other social media abuse. Alternatively, Title IX may be asserted if the offending student accesses social media sites while on-campus and uses those sites to harass another student.

D. Student-teacher communications

All too often, reports surface of inappropriate relationships between teachers and students. These reports not only detail the actions that took place, but usually include details as to the social media communications between the teacher and the student. School districts should consider establishing policies limiting electronic communications between teachers and students. For example, a school district could limit such communications to certain times of day (i.e. 7 AM to 9 PM). A school district could try to limit the subjects of communications to areas like homework and tests. Schools districts may also consider prohibiting its personnel from "friending" students on personal social networking sites.

III. Social Media Issues in Litigation and Courtroom

1. Fact investigations and discovery

Investigation of social media sites and communications can, and should, play an important role in certain types of litigation. In employment litigation, an employee may claim that the employer's retaliation has caused her to be unable to find another job or that supervisor X discriminated against her, but be commenting on social media that she loves her new job or that supervisor X is great and has always treated her nicely.

For reasons like these, one of the first things that some lawyers do when receiving a new case is research the plaintiff on social media sites and print any relevant information found thereon. If there is no

public information available, discovery requests can be propounded and subpoenas issued to the social media sites to obtain relevant information.

2. Jurors' access to online information

Just like in the areas of work and school, jurors' access to online information and social media sites is having an ever-increasing impact on the judicial system. Numerous courts both at the state and federal levels have declared mistrials when jurors did their own online research. There are also numerous other instances of jurors discussing their cases on social media sites. The impact of these inappropriate uses of technology is enormous when considering the fairness of a trial and the waste of time and money represented by the need to re-try a case simply because jurors violated the rules by using technology.

In response to this problem, state and federal courts have begun to issue jury instructions specifically concerned with the use of technology by jurors. As some commentators have pointed out, it also important that the jury instructions include some explanation as to why independent research or communications about the case are improper and could damage the judicial process. Additionally, some have suggested that making it clear to jurors that they could be held in contempt for violations would also be effective, though some consider the penalty to be too harsh. Courts and lawyers should include questions during voir dire concerning internet and social media use, and the ability of the jurors to abide by the prohibition against research and communications.

IV. Conclusion

Social media's virtual reality is part of our new reality. Employers, schools, and courts face enormous challenges in effectively responding and managing the significant and novel issues presented. How these challenges are addressed will likely help to shape the law and our society during the 21st century.