NACUA

57th Annual Conference

Sheraton Grand Chicago · Chicago, IL
June 25 – 28, 2017

08G Data and Social Media Mistakes to Avoid - For Faculty, Administrators, and Counsel

NACUA

57th Annual Conference

Sheraton Grand Chicago · Chicago, IL · June 25 - 28, 2017

DATA AND SOCIAL MEDIA MISTAKES TO AVOID: FOR FACULTY, ADMINISTRATORS AND COUNSEL

June 25-28, 2017

Kevin E. Dolan
LaSalle University
Philadelphia, Pennsylvania

James A. Keller
Saul Ewing, LLP
Philadelphia, Pennsylvania

I. Mixing Work and Personal Life on Institutional Email – A Risk for All

Brief Summary of Section: This section provides an overview of the risks associated with using institutional emails, examples and repercussions of misuse, policies of universities that serve as a reminder that email is school property, a discussion on vicarious liability risks for the university, and suggested best practices to avoid any mishaps.

A. A REAL LIFE EXAMPLE

- A law professor at Drexel University sent an email with a link to a pornographic video to students. The professor was put on leave pending an investing into whether she violated the sexual harassment and misconduct policy. The question became whether she *intentionally* sent the video, knowing that it would be emotionally disturbing to students. Not only was the professor put on leave, but the University had to respond to backlash from the community and students. [1,2]

B. RELEVANT UNIVERSITY POLICIES

Most institutions that provide email accounts require an agreement with the user stating that the institution has a right to monitor and search through the email. Along with these agreements, most institutional websites include an "email policy" or "information technology policy".

At the University of Florida, for example, their email policy states, "All of these materials [emails], regardless of form, are open for public inspection unless the legislature has

---

1 Martinez, *UConn investigating professor email that included link to pornography*, http://fox61.com/2017/04/19/uconn-investigating-professor-email-that-included-link-to-pornography (April 19, 2017).

2 *See* Linkins, *Drexel Law Professor's Email Mishap Touches Off Idiotic Freakout With University Administration*, http://www.huffingtonpost.com/2015/04/08/law-professor-anal-bead-gate_n_7025812.html (April 8, 2015).

specifically exempted them from disclosure. One Florida court has held that 'information stored in a computer is as much a public record as a written page in a book or a tabulation in a file stored in a filing cabinet.'… E-mail created or received by University of Florida employees in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and open for inspection." [3] These risks are particularly acute at a public institution subject to a right know law. In another section, the University of Florida policy states that email is considered university equipment and all therefore must follow the "appropriate use" policy. [4]

As an example from the private university sector, the University of Chicago has a similar "acceptable use" policy stating that the university provides information technology to its faculty and students, and the university reserves the right to preserve, access, and disclose information gathered from the information technology as required.[5] Their policy indicates that although personal use of institutional email is not prohibited, it can be collected and used for a business purpose at any time. If personal email is among those that are business related, the university will not be able to filter out personal email from being viewed.

C. LIABILITY RISKS FOR THE INSTITUTION

Because the university claims ownership of the emails, it is important to understand whether the university could be vicariously liable for statements made by University employees or officials via email.

1. Defamation

One risk of using institutional email for private business is that a university employee might insult or even defame someone – the question, then, is whether the institution could be liable. In *Booker v. GTE.net LLC*[6], the court held that the employer was not vicariously liable for defamatory electronic communication sent by an employee because the employee was acting outside the scope of his employment. Factors for whether the employee's intentional tort was within the scope of employment are (a) whether the conduct was similar to what the employee was hired to perform, (b) the action occurred substantially within the spatial and temporal limits of the employment, (c) the action was in furtherance of the employer's business, and (d) the conduct was expectable in view of the employee's duties. The court found that the employee

---

3 https://ufcn.urel.ufl.edu/email/email.html

4 https://it.ufl.edu/policies/acceptable-use/acceptable-use-policy/

5 https://itservices.uchicago.edu/policies/university-chicago-policy-information-technology-use-and-access

6 *Booker v. GTE.net LLC*, 350 F.3d 515, 20 I.E.R. Cas. (BNA) 1273, 2003 FED App. 0427P (6th Cir. 2003) (applying Kentucky law)

sending an offensive email to a customer was outside the scope of employment, precluding the employer's vicarious liability. [7]

2. Harassment

In *Roof v. Howard University*, a professor sent harassing and racist emails to a student.[8] The court stated that the University would only be liable if it knew or had reason to know of the harassment, and failed to take remedial action. After the university was notified by the student, the they acted in a timely manner. The university was not held vicariously liable for the professor's harassing actions, conducted via institutional email.

3. Infringement

Most information found on the internet is copyright protected. Unless the information has been pulled from the public domain, copying and pasting information from the internet into an email without proper references can constitute copyright infringement.[9] Generally, however, only the sender – not the institution – would be liable.

4. Public Relations Risks

See, e.g., the Drexel example above.

D. BEST PRACTICES

An effective email policy is key for universities to communicate proper usage of the email system. It should include but is not limited to:

- A statement that the university's email system is the institution's property, and is to be used for the purposes of furthering university business,
- An explanation of the rules governing the use of the email system such as: the system should not be used to transmit or receive confidential information, discriminatory, harassing, sexually oriented, offensive, or other illegal and improper messages, etc.,
- The repercussions that could arise from the misuse of university property, and
- An explanation that the university can (not will, but can) monitor all email.[10]

---

7 3 A.L.R.6th 153 (Originally published in 2005).

8 *Roof v. Howard U.*, 501 F. Supp. 2d 108, 116 (D.D.C. 2007).

9 Laver and Luongo, *Employer liability for privacy breach?* http://professionalliabilitymatters.com/2015/01/26/employer-liability-for-privacy-breach/ (Jan. 26. 2015).

10 Smith, *Email In The Workplace: Avoiding Legal Landmines,* http://www.mediate.com/articles/smith.cfm

II. Data Security – A Risk for All

A. HIGHER EDUCATION DATABASES ARE "A PLAYGROUND FOR HACKERS"[11]: REAL LIFE EXAMPLES OF DATA BREACHES

Data breaches in higher education are on the rise, and the risks extend far beyond grades and leaks of demographic information. Personal information and key financial data are common targets, and the threat of higher education data breaches is only growing.[12] Due to the high volume of records kept by higher education institutions, the number of personal devices available, and the open, collaborative culture of a college campus, there are an abundance of examples involving data breaches from large universities to small liberal arts colleges.[13] The following are just a few recent examples of data breaches occurring on college campuses:

- Los Angeles Valley College: A virus locked the entire campus computer network, voicemail system, and email over the students' winter break. In order to restore the data, the college paid $28,000 in ransom to the cyber-attackers. The attackers sent a "key" to retrieve the data and the data was restored the following day.[14]

- Pennsylvania State University: Over the span of three years, the university was hacked twice. Outside forensic research confirmed that at least one of the attacks was the result of a "threat actor" based in China. The attackers sought the university's intellectual property and highly valued research, specifically information about Defense Department projects. As a result of the hack, all network users were required to change their passwords and an additional layer of authentication is now in place before access to the network may be granted. Approximately $2.85 million has been spent in response to the data breaches, including $450,000 to external experts to secure the network further and $2.4 million to replace infected hardware.[15]

---

11 Straumshein, *Inside Higher Ed: A Playground for Hackers*, https://www.insidehighered.com/news/2015/07/06/pennsylvania-state-u-cyberattackspossibly-part-larger-trend-experts-say (July 6, 2015).

12 Harris & Hammargren, *Higher Education's Vulnerability to Cyber Attacks*, https://www.universitybusiness.com/article/0816-wisp (Aug. 2016).

13 Coleman & Purcell, *Data Braches in Higher Education*, www.aabri.com/manuscripts/162377.pdf (Dec. 2015).

14 Bilus, *College Pays Bitcoin Ransom to Unlock Encrypted Data*, http://www.saul.com/publications/alerts/cyberattacker-offers-access-private-data-60-universities-and-agencies (Jan. 2017).

15 Coleman & Purcell, *Data Braches in Higher Education*, www.aabri.com/manuscripts/162377.pdf (Dec. 2015).

B. LEGAL RISKS AND ADDITIONAL CONSIDERATIONS REGARDING DATA BREACHES IN HIGHER EDUCATION

In addition to the practical risks of a data breach, there are legal risks to an institution. These include, but are not limited to, the following:

1. Civil Suits

Higher education data breaches have recently been the subject of civil actions under a variety of legal theories, including negligence and invasion of privacy. Class action suits brought against higher education institutions are followed by substantial expenditures in resources and time, exemplified by the following:

- University of Hawaii: Multiple campuses of the university had several data breaches between April 2009 and June 2011 compromising the information of 90,000 individuals (names, Social Security numbers, addresses, and credit card information). Affected individuals filed a class action suit which resulted in a settlement in 2012. The settlement required the university to provide credit monitoring and fraud restoration services to those affected, with total costs of about $550,000 and undisclosed attorneys' fees and costs.

- Stanford University Hospital and Clinics: A business associate's subcontractor at the university's hospital and clinic posted the health information of 20,000 patients treated by the hospital on the hospital's website. Specifically, the patient's names, medical records, emergency room dates, and medical codes were all revealed. The affected individuals brought a class action suit which resulted in a settlement for $4 million.[16]

2. Penalties for Violating State Security Breach Notification Laws

Higher education institutions are subject to state data breach notification laws. However, each state law is different and carries with it different notification requirements and penalties for violating the notification requirements. Many have broad provisions which hold anyone in possession of personal information liable for a data breach. Other state security laws are more narrow and only require notification by specific agencies or businesses in the event of a breach. Further, some states require entities to notify only consumers, while others require entities to disclose data breaches to credit reporting agencies or the government.[17] An institution must be familiar with the state regulatory and penalty landscape for breaches wherever it has campuses.

---

16 Harris & Hammargren, *Higher Education's Vulnerability to Cyber Attacks,* https://www.universitybusiness.com/article/0816-wisp (Aug. 2016).

17 Beadin, *Colleges and University Data Breaches,* http://www.nacua.org/securedocuments/nonsearched/jcul/41_jcul_657.pdf (2015).

3. Financial Loss and Harm to Reputation

The cost of a data breach can be quite substantial for a higher education institution. According to a study published by Ponemon Institute, which studies data protection, the average breach in higher education costs approximately $111 per record. Notifications to affected people without a known email address may also be costly. For example, Indiana University spent a total of $75,000 on an informational call center after a security lapse, and another $6,200 for mailing notifications for those without emails.

In addition to costs, higher education institutions with data breaches need to consider the reputational impact. Breaches, no matter whether they are realistically preventable or not, bring bad publicity to the institution and tarnish the brand name.[18]

C. APPLICABLE FEDERAL LAW CONSIDERATIONS

1. FERPA Considerations

The Family Educational Rights and Privacy Act ("FERPA"), which applies to all educational institutions receiving federal funding, does not require an institution to notify students or faculty in the case of a data breach. However, the FERPA Safeguarding Recommendations encourage educational institutions holding personally identifiable information to take mitigating steps to avoid data breaches and provides guidance with steps to implement in the case of a data breach.[19] Further, FERPA provides that when an institution outsources services, the outside party is under the direct control of the institution regarding the use and maintenance of the educational records disclosed to the third parties.[20] As such, higher education institutions should be cognizant of any data breaches resulting from third parties, as the outside party is to remain under the institutions direct control.

2. OCR/HIPAA Considerations

It is important to note that according to the Office for Civil Rights ("OCR"), the government agency that enforces the Health Insurance Portability and Accountability Act ("HIPAA"), the HIPAA Privacy Rule requiring security standards for health records generally does not apply to institutions of higher education unless a particular institution, or a portion thereof, is a covered entity as defined by HIPAA. However, if a higher education institution has an on-campus health clinic that services both students and non-students, the institution must

---

18 O'Neil, *Data Breaches Put a Dent in Colleges' Finances as Well as Reputations*, http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/ (March 14, 2014).

19 https://www.databreaches.net/ferpa-does-not-require-data-breach-disclosure/ (2017).

20 34 C.F.R. § 99.31(a)(1)(i)(B)(2)

comply with FERPA with respects to the records of the student and with the HIPAA Privacy Rule with respects to the non-student's heath records.[21]

3. FTC Safeguards Rule Considerations

In addition, the Federal Trade Commission ("FTC") issued the Safeguards Rule as part of the Gramm-Leach-Bliley Act.[22] Higher education institutions, as indicated by the FTC, are subject to the Safeguards Rule. This rule requires institutions providing financial services to establish a written information security program ("WISP") including technical, administrative, and physical safeguards to personal information.[23] The Safeguards Rule also requires colleges and universities to designate an employee(s) to coordinate an information security program, identify internal and external risks to security or confidentiality that could result in disclosure, and assess the sufficiency of the safeguards in place to control those risks. Further, the FTC requires higher education institutions to implement information safeguards to control the identified risks and regularly test and monitor the procedures and systems in place.[24]

D. IMPLEMENTING TOOLS TO BEAT THE HACKERS: BEST PRACTICES

Because higher education institutions have databases with sensitive information such as Social Security numbers, medical records, financial data, and intellectual property, it is increasingly important to have a data breach response plan in place. The U.S. Department of Education established the Privacy Technical Assistance Center ("PTAC") as a resource for educational institutions to secure data privacy and confidentiality. The PTAC developed a useful data breach response checklist, which includes the best practices listed below.[25]

1. Before the Breach[26]

---

21 http://www.thompsoncoburn.com/insights/blogs/regucation/post/2016-02-03/is-your-institution-of-higher-education-covered-by-hipaa- (2017).

22 Federal Trade Commission, *Safeguards Rule*, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule (2016).

23 Harris & Hammargren, *Higher Education's Vulnerability to Cyber Attacks*, https://www.universitybusiness.com/article/0816-wisp (Aug. 2016).

24 NACUBO Advisory Report 2003-01, *Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information*, http://www.nacubo.org/documents/news/2003-01.pdf. (Jan. 13, 2003).

25 Privacy Technical Assistance Center, *Data Breach Response Checklist*, http://ptac.ed.gov/document/checklist-data-breach-response-sept-2012 (Sept. 2012).

26 Id.

An effective and efficient data breach response plan begins before a breach incident occurs. The following will help mitigate breaches and assist in efficient and quick detection of potential breaches:

i. *Establish and implement a written data breach response policy including:*

    1. Applicable breach notification legal requirements;
    2. Data breach response strategy, goals, and requirements;
    3. Specific handling procedures regarding notification to law enforcement/outside parties;
    4. Identifying an incident response team and team manager; and
    5. Conducting regular reviews of the policy to include any necessary improvements.

ii. *Review your information system(s) and data and identify where personally identifiable information and other sensitive information resides.*

iii. *Continuously monitor for personally identifiable information and other sensitive data leakage and loss.*

iv. *Conduct frequent privacy and security awareness trainings as part of an on-going training and awareness program. This includes:*

    1. Providing mandatory privacy and information security training on a recurring basis to all employees, school officials, contractors, and other staff;
    2. Posting and communicating privacy policies to customers and users; and
    3. Clearly defining and making easily accessible processes for reporting privacy incidents and complaints.

B. Responding to the Breach[27]

The following will help make critical decisions during the breach response:

i. *Validate the data breach by examining the information and available logs to confirm a breach has in fact occurred.*
    1. If possible, identify the type of information disclosed and estimate the methods of disclosure (internal/external, malicious/accidental).

ii. *Once a breach has been validated, immediately assign an incident manager to be responsible for the investigation.*

iii. *Assemble an incident response team.*

iv. *Determine the scope and composition of the breach. This may include*:
    1. Identifying all affected data, machines, and devices;
    2. Conducting interviews with key personnel and document facts; and
    3. Preserving evidence for later forensic investigation.

v. *Notify the data owner as soon as possible and foster a cooperative relationship between the incident response team and the data owners.*

vi. *Consider notifying Family Policy compliance Office about the breach – while this is not required it is considered best practice by the U.S. Department of Education.*

---

[27] Id.

vii. *Determine whether to notify the authorities or law enforcement (situation dependent).*
viii. *Decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved.*
ix. *Determine whether notification of affected individuals is appropriate, and, if so, when and how to provide such notifications.*
    1. Notify affected individuals whose sensitive information, including personally identifiable information, has been compromised, as required by applicable laws; and
    2. If the breach represents a threat to affected individuals' identity security, consider providing credit monitoring or identity theft protection services to mitigate the risk of negative consequences for those affected.
x. *Collect and review any breach response documentation and analyses reports.*

III. "Friending" and Other Social Media Communications With Student: A Risk For All

A. TO FRIEND OR NOT TO FRIEND: REAL LIFE EXAMPLES

The increased use of social media blurs the boundaries between higher education faculty and students. The term "friending" is broadly defined as "a person associated with another as a contact on social media."[28] A few of the overarching concerns with social media contact are: the inability to convey tone and sarcasm, not knowing how communication will be perceived, the discrepancy between how different generations utilize social media, and potential legal and other practical concerns that may result.

The following are just a few "real life" examples where "friending" between and among faculty and students created issues:

> • A student bakes a batch of chocolate chip cookies and uploads their photographs on Facebook. His/her professor comments on the post, saying they look "scrumptious" and asks for the recipe.[29]
>
> • On the Facebook wall of a female professor, a male student posts wishing her 'Happy B'day, Ma'm' with a smiley and later questioning why he wasn't invited for her birthday bash with a sad smiley.[30]

---

28 Available at: www.dictionary.com/browse/friending.

29 This example was modified from an example in the following article: http://epaper.timesofindia.com/Repository/getFiles.asp?Style=OliveXLib:LowLevelEntityToPrint_CREST&Type=text/html&Locale=english-skin-custom&Path=TCRM/2011/05/28&ID=Ar01100 (May 28, 2011).

30 *Id*.

• A professor who is new to Facebook sees the "poke" feature, and not knowing what the feature does decides to "poke" a student who he friended. The student received the poke and found it inappropriate based on their own understanding of what this feature is used for (e.g. flirting). The professor and his middle-aged friends all poke one another, interpreting it as a friendly exchange, meanwhile the student and her friends do not interpret it this way.

• A faculty member friends a student on Instagram. The student posts photos partying at the beach or at a night club. The faculty member sends a private "direct message" to the student stating "Love the photo!"

• A student requests to be friends with a faculty member on Snapchat. The faculty member is under the faulty belief that only those who she "friends back" (not just accepting a friend request) can view her Snapchat story. Being new to Snapchat, the faculty member also accidently posts an indecent video to her Snapchat story, thus allowing the student to view the video.

B. RISKS: CROSSING THE LINE FROM SOCIAL MEDIA "FRIEND" TO ALLEGATIONS OF HARASSMENT OR STALKING

Two New York examples have provided some clarity on the risks of teachers friending students on social media.[31]

In the first, a teacher friended about six female students and commented on their photos stating "This is sexy."[32] Reports state that the teacher also had inappropriate language on his Facebook page including "I'm not a gynecologist, but I'll take a look inside." [33] While the female students did not file suit against the teacher or the school, the *New York Post* reported that the teacher was fired as a result of his comments.[34]

In the second, a substitute teacher "friended" female students and sent inappropriate messages on Facebook.[35] For example, one message to a female student stated that her boyfriend did not deserve a beautiful girl like her.[36] No apparent legal action was taken, but it is reported that the teacher was barred from substitute teaching.[37]

---

31 Available at: http://www.dailymail.co.uk/news/article-1322408/Facebook-flirts-Teachers-fired-inappropriate-relationships-students.html (October 2010).

32 *Id*.

33 *Id*.

34 Available at: http://nypost.com/2010/10/18/teachers-fired-for-flirting-on-facebook-with-students/.

35 *Id*.

36 *Id*.

37 *Id*.

C. POTENTIAL CIVIL/CRIMINAL LIABILITY FOR INAPPROPRIATE "FRIENDING"

A. Direct Liability for the "Friender"

1. *Civil liability*. As illustrated above, there is no clear distinction of when "friending" crosses the line, but claims under Title IX and in tort are feasible.[38]

2. *Criminal Liability*. There is also the potential for criminal liability under federal or state statutes for harassment and stalking. For example, under 18 U.S.C. 875(c) it is a federal crime to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another.[39] The statute is construed to apply only to communications of actual threats; thus drawing a distinction from a mere allegation and actual threats to injure another.[40]

3. *VAWA*: multiple social media contacts, within a year, that a reasonable person would perceive as harassing or inappropriate create a reporting obligation for the institution, and civil and possibly criminal liability risk for the employee/faculty member engaging in such conduct.

B. Violation of University Social Media Policy, Code of Conduct, or Ethics

It is also important to review university social media policy, code of conduct, and ethics policies. Friending or engaging in other social media communication with students may result in a violation, depending on the terms the university includes.[41]

C. Vicarious Liability

Universities, as the employer, also must be aware of theories of vicarious liability for discriminatory or harassing social media contacts by faculty or employees. Such claims require a case-by-case assessment to determine if the employee or faculty member acted within the scope of his or her employment. We have not located any case where a court considered whether

---

38 For the elements of intentional infliction of emotional distress, *see* McCollough v. Noblesville Sch., 63 N.E.3d 334, 342 (Ind. Ct. App. 2016); A negligence claim may result if a professor assumes a duty by friending a student on social media, commits a breach, and damages result. *See* 2011 Evaluating and Disciplining Student Speech in the Social Media Age: Compliance and Risk Mitigation PowerPoint slide provided via e-mail on May 30, 2017.

39 18 U.S.C. 875(c).

40 Available at: cyber.harvard.edu/vaw00/cyberstalking_laws.html.

41 For example, *see* The University of Delaware's Code of Conduct available at http://www1.udel.edu/stuguide/16-17/code.html#harass.

the act of "friending" itself would be within the scope of employment at a university; however, such a claim would depend on the facts of the case and is not infeasible.

D. OTHER CONSIDERATIONS: PRIVACY AND PUBLIC RELATIONS

Some other, non-legal considerations for higher education professionals include privacy and safety concerns and public relations issues.

1. *Privacy and safety concerns*. Today, a prevalent social media trend is to "check in" at a location, which notifies "friends" where a person is.[42] This could be problematic if, for example, a professor and a student both happen to be at a popular location (e.g. a local beach), and the student checked-in to that location earlier. Will the student fear that the professor was stalking him or her? This creates an issue that can easily be avoided. If the professor and student are not friends on social media, it negates the possibility that the professor showed up to a location based solely on a student's earlier check-in and provides a stronger case for a professor (or university) defending against harassment or stalking charges.

2. *Public relations issues*. In an increasingly connected world, misinformation gets issued and repeated more quickly than ever.[43] For example, when faculty members send a friend request to students, the students have the potential to screenshot the friend request on their smartphone, add their own personal commentary (e.g. "This is creepy" or "Stalker much?"), and send it to other students or post it on another social media site. Regardless of a faculty member's motive in friending a student, once the request is sent, there is no telling how it will be perceived and exposed to the world.[44] In sum, this gives students broad power to create negative publicity for the university.

E. WHAT IS THE AAUP'S POSITION?

The American Association of University Professors ("AAUP") is a nonprofit membership association of faculty and other academic professionals.[45] The mission of the AAUP is to

---

42 Available at: http://powerupsocial.com/checking-in-in-social-media/.

43 Available at: http://www.cnn.com/2012/03/06/tech/social-media/misinformation-social-media/ (March 6, 2012).

44 For an example of negative public relations resulting from faculty member social media use *see* https://www.insidehighered.com/news/2017/04/10/drexel-faculty-senate-looks-professors-controversial-tweets (discussing Drexel's response to a professor's controversial tweets that may be causing prospective students to withdraw their acceptance).

45 Available at: https://www.aaup.org/about-aaup.

"advance academic freedom and shared governance; to define fundamental professional values and standards for higher education; to promote the economic security of faculty, academic professionals, graduate students, post-doctoral fellows, and all those engaged in teaching and research in higher education; to help the higher education community organize to make our goals a reality; and to ensure higher education's contribution to the common good."[46]

The AAUP reported that faculty use of social media is increasing, with one survey indicating that seventy percent of those responding visited a social media site within the previous month for personal use.[47] Meanwhile, a separate and distinct study showed that social networking tools are used by ninety-five percent of students ages eighteen to twenty-four.[48]

The AAUP has long held that any type of intimidation and harassment is inconsistent with the maintenance of academic freedom on campus.[49] Although not explicitly stated, it has implied that this would extend to intimidation and harassment on social media.[50]

The AAUP recommends that each institution work with its own faculty to develop policies governing the use of social media.[51] However, it also has a firm belief that "the benefits from the free exchange of information and ideas are at the heart of the academic enterprise, whether conducted orally, in print, or electronically." [52] Furthermore, the AAUP has condemned a policy aimed at disciplining faculty members for "improper use of social media." [53]

F. BEST PRACTICES GOING FORWARD

---

46 Available at: https://www.aaup.org/about/mission-1.

47 Available at: https://www.aaup.org/report/academic-freedom-and-electronic-communications-2014 (November 2013).

48 Jamison Barr, Emmy Lugus, *Digital Threats on Campus: Examining the Duty of Colleges to Protect Their Social Networking Students*, 33 W. New Eng. L. Rev. 757, 761 (2011).

49 Available at: https://www.aaup.org/issues/sexual-harassment/policies-2002 (October 2002).

50 Based on the AAUP's mission and *Statement of Professional Ethics*, it rejects any of this type of conduct. For example, the Statement *of Professional Ethics* states: "Professors demonstrate respect for students as individuals and adhere to their proper roles as intellectual guides and counselors." *See* https://www.aaup.org/report/statement-professional-ethics.

51 Available at: https://www.aaup.org/report/academic-freedom-and-electronic-communications-2014 (November 2014).

52 *See* https://www.aaup.org/report/academic-freedom-and-electronic-communications-2014 (November 2014) (stating that the AAUP rejected Kansas Board of Regents attempt to adopt a rule allowing faculty members to be suspended or disciplined for improper use of social media).

53 *Id*.

It is important to note that the best practices for friending and engaging in other social media communications with students may vary, depending on the platform, purpose, duration, and options for privacy limitations. Some general guidelines include:

- Choose the right social media tool or platform that best fits the desired purpose;
- Consider crafting and implementing social media guidelines or an acceptable use policy;[54]
- Teach students, employees, and staff appropriate social media use;
- Be cognizant of the difficulty in conveying tone and sarcasm over social media;
- Look for social media tools built specifically for the classroom;
- Consider waiting until students have graduated or completed the course you teach before friending them on social media;[55]
- Set up a specific account, distinct from your personal social media account, that will be used for school activities only;[56]
- Stay up to date on privacy setting changes and updates;[57] and
- Advise teachers to only communicate with students through social media when a topic applies to school-related matters.[58]

Social media behaviors to avoid include:

- Do not use social media to comment on a student's physical appearance;
- Do not communicate on social media with students during late hours of the night or on weekends, unless otherwise required by a specific assignment;[59]
- Avoid using social media for activities that can be accomplished with comparable non-social media platforms;
- Faculty members should not pressure students to friend them;[60] and

---

54 Monica Fuglei, *Social Media In Education: Benefits, Drawbacks and Things to Avoid* (July 16, 2015), http://education.cu-portland.edu/blog/news/educational-social-media-use/.

55 Tina Barseghian, *30 Facebook Dos and Don'ts for College Professors* (June 22, 2011), https://ww2.kqed.org/mindshift/2011/06/22/30-facebook-rules-for-college-professors/.

56 Monica Fuglei, *Social Media In Education: Benefits, Drawbacks and Things to Avoid* (July 16, 2015), http://education.cu-portland.edu/blog/news/educational-social-media-use/.

57 Nancy Caroll, *Social Media for Teachers 101: Basic Do's and Don'ts*, http://nancycarroll.net/social-media-for-teachers-101-basic-dos-donts.

58 Ryan Lytle, *Student-Teacher Social Media Restrictions Get Mixed Reactions* (August 10, 2011) https://www.usnews.com/education/high-schools/articles/2011/08/10/student-teacher-social-media-restrictions-get-mixed-reactions.

59 Jeff Dunn, The *Dos and Don'ts for teachers on Social Media*, (May 28, 2015), http://dailygenius.com/the-dos-and-donts-for-teachers-on-social-media/.

60 Richard A. Paul, Beth Cate & Priya Harjani, *Faculty Ethics on Facebook*, http://www.facebook.com/group.php?gid=2229343363.

• Avoid informal communicative tools, such as acronyms (e.g. LOL or OMG) or emojis that misconstrue tone and sarcasm.

IV. A Social Media Issue Primarily for Counsel – Is Texting Legal Advice/Work Product Ok?

A. DON'T PRESS SEND!: INTRODUCTION AND REAL LIFE EXAMPLES

The use of text messaging in the legal world is increasingly popular and increasingly problematic. Although it is praised for its ease and swiftness, examples such as the ones below show the drastic effect that texting a client or counsel can have on any counsel's reputation and relationship:

- Johnny Manziel's attorney, Bob Hinton, drafted a text message in June 2016 to send to co-counsel, which contained confidential case facts (such as Manziel's $1,000 purchase of drug paraphernalia) and confidential legal advice regarding a proposed plea deal. Instead of sending the confidential text message to associated counsel, the attorney accidentally sent the text message to the Associated Press. Consequently, the attorney was removed from the case and fired. Importantly, the information in the text was no longer considered privileged or confidential.[61]

- The following text chain is another example:

  Client: I want to be listed as the only fiduciary on my son's estate.
  Lawyer: Ok. Meet me down at O'Shaughnessey's bar and bring friends of the female persuasion
  Client: Excuse me?
  Lawyer: O'Shaugnessey's bar. Bring women. You know what kind.
\ Client: What kind of lawyer are you?
  Lawyer: Oh, I'm so sorry. That text wasn't meant for you. After all, it is a Saturday.[62]

Evident from these examples, sending and responding to texts for legal advice creates heightened risks for counsel and counsel's client. There is simply an informality to text messaging that you do not usually see in letters or formal emails. Best practices and tips can assist counsel in protecting both themselves and their client from these risks.

B. HEIGHTENED RISKS: LITIGATION

---

61 Kevin Sali, *Johnny Manziel's Lawyer's Mistake is More Common than You May Think*, Huffington Post, http://www.huffingtonpost.com/kevin-sali/johnny-manziels-lawyers-m_b_10709498.html (updated June 28, 2016).

62 Susan Carter Liebel, *When Lawyer to Client Texts go Wrong!* SOLO PRACTICE UNIVERSITY, http://*solopracticeuniversity*.com/2016/01/19/when-lawyer-to-client-texts-go-wrong/ (Jan. 19, 2016).

Text messages that send or respond to a request for legal advice create a risk if any party to the text message is involved in, or becomes involved in, litigation. Text messages are a discoverable type of electronically stored information ("ESI") and are subject to the same discovery standard as documents, e-mails, and other social media platforms.[63] Absent a privilege, protection, or agreed limitation, counsel is obligated to produce all relevant text messages if requested.[64] Two significant risks involved are: 1) a potential waiver of privilege; and 2) a potential sanctions award for spoliation. Each will be discussed below.[65]

1. Text Messages Could Result in a Potential Waiver of Privilege and Protection

Text messages present heightened risks due to their electronic nature and the ease with which they can be accidentally transmitted to a third party, added to the wrong "text string", etc. The attorney client privilege can be waived in electronic communication by disclosure to a third party. Courts construe "disclosure to a third party" broadly, holding that this disclosure is achieved by forwarding electronic information to a third party, which in effect compromises the attorney client privilege and constitutes a waiver. [66] Because the same discovery standards are applied to e-mail and text message, text message communication that is forwarded will not be deemed privileged. "Forwarding" a text message on a modern electronic device is achieved easily, through either screenshotting the text message or clicking a forward arrow. This simple action can waive the attorney client privilege for the electronic communication, and can lead to irreversible errors if sent to the wrong recipient.

"Disclosure to a third party" also easily occurs if the text messages are sent or received on an employer issued phone, which can easily waive the attorney client privilege. If employees does not have a reasonable belief that they are having a confidential and private conversation in light of the employer use policies, then there is no confidential aspect to the communication.[67] Additionally, when a text message or email is sent from an employer-owned device, the employer may obtain access to the employee communications pursuant to internal policy.[68] Because of this, using an employer issued electronic device can compromise the confidentiality of access to the device, in turn compromising the attorney client privilege over the text

---

63 *Robinson v. Jones Lang LaSalle Ams., Inc* - No. 3:12-cv-00127-PK, 2012 WL 3763545, at *1 (D. Or. Aug. 29, 2012).

64 Job Seese, *Smart Discovery & Litigation Strategies for Text Messages: Part 3*, Linkedin (August 31, 2016), https://www.linkedin.com/pulse/smart-discovery-litigation-strategies-text-messages-part-job-seese-1.

65 Vera Nackovic, *OMG! My text messages could be discoverable?*, Inside Counsel (November 30, 2015), http://www.insidecounsel.com/2015/11/30/omg-my-text-messages-could-be-discoverable.

66 I In re West, 2012 WL 1344220 (E.D. Va. Bkr.) (holding that forwarding of an email containing legal advice destroyed the attorney client privilege, making the information available for discovery proceedings).

67 Paula Schaefer, Technology's Triple Threat to the Attorney-Client Privilege, 2013 PROF. LAW. 171, 186 (2013).

68 ABA Standing Comm. On Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011).

messages.[69] Analogous situations from the email context seem even more problematic when applied to text messages. For example:

- In *Terraphase Engineering Inc., et al. v. Arcadis*, counsel inadvertently sent an email containing privileged email advice to his client's former company e-mail address. The privileged materials were read by the former company, the privilege did not protect the information, and the court disqualified the law firm from the case.[70]

- In *Holmes v. Petrovich Development Co.*, emails a client sent to an attorney on a company computer were not protected by the attorney client privilege because the use of a company computer to send the emails constituted a waiver of the privilege.[71]

2. The Deletion of Text Messages Can Be Grounds for Sanctions

The use of text messages to send or respond to a request for legal advice also increases the risk for spoliation sanctions in litigation involving counsel or counsel's employer.[72] Generally, a party has an obligation to take reasonable and proportional steps to preserve discoverable information in the party's possession, custody, or control.[73] This duty extends to relevant information originating in any form, including electronically stored information.[74] A party is sanctioned for spoliation of evidence when a party "destroys, significantly alters, or fails to preserve evidence in pending or reasonably foreseeable litigation."[75] As stated above, this evidence does include text messages – which individuals simply do not usually take the same steps to protect or save.

It is becoming increasingly common for courts to issue spoliation sanctions, including dismissal, for failure to prevent the deletion of evidence that is contained in text message form. For example:

---

69 Id.

70 Case information from: *The Attorney Client Privilege in the Electronic Digital Age*, ABA, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/14_combined_session_documents.authcheckdam.pdf

71 Holmes v. Petrovich Development Company, LLC, 191 Cal.App.4th 1047, 1066 (2011).

72 Default Standard for Discovery, Including Discovery of Electronically Stored Information (ESI), available at http://www.ded.uscourts.gov/sites/default/files/Chambers/SLR/Misc/EDiscov.pdf.

73 Id.

74 Id.

75 United States v Kitsap Physicians Serv. 314 F.3d 995, 1001 (9th Cir. 2002).

- In *Taylor v. Shippers Transport Express*, the court stated that defending a spoliation motion on grounds that text messaging is a new technology is "dubious" and "purported ignorance." The court in *Taylor* emphasized that destroyed and deleted text messages warrant spoliation sanctions, regardless of the ability to recover the text messages.[76]

- In *First Financial Security, Inc. v. Freedom Equity Group, LLC*, the California court issued spoliation sanctions against the defendant for deleting relevant text messages.[77]

- In *Flagg v. Staples the Office Superstore East, Inc.* the Northern District of Ohio issued sanctions for a defendants destruction of relevant text messages, and for the defendants failure to preserve the text messages.[78]

- In *Hosch v. BAE Systems Information Solutions, Inc.* the Eastern District of Virginia sanctioned the plaintiff for deleting relevant text messages, and dismissed the case with prejudice, awarding attorney's fees and costs incurred from the motion.[79]

C. HEIGHTENED RISKS: ETHICAL OBLIGATIONS

Text messages that send or respond to a request for legal advice create heightened risks for violation of ethical obligations by counsel. Lawyers owe a duty of confidentiality, communication, and competence to clients. As the use of text messaging increases, the intersection of these duties is recognized by bar associations and ethics boards as increasingly problematic.

Model Rule of Professional Conduct (MRPC) 1.1 imposes a duty of competent representation.[80] The American Bar Association (ABA) recognized the heightened ethical issues present with electronic communication and this duty, and added comment 8 to rule 1.1. This amended comment states "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[81] This amended rule echoes the reasoning of *Perez*, emphasizing that lack

---

76 Taylor v. Shippers Transport Express, No. CV 13-02092, 2014 WL 12560879 at *9 (C.D. Ca 2014).

77 First Financial Security, Inc v. Freedom Equity Group, No. 15-cv-01893-HRL, 2016 WL 5870218 at *7 (N.D. Ca 2016).

78 Flagg v. Staples the Office Superstore East, No. 1:14CV0004, 2015 WL 5730704 at *2 (N.D. Oh 2015).

79 Hosch v. BAE Systems Information Solutions, Inc., No. 1:13-CV-00825, 2014 WL 168194 at *2 (E.D. Va).

80 Model Rules of Prof'l Conduct 1.1 (Am. Bar Ass'n,).

81 Model Rules of Prof'l Conduct 1.1, cmt. 8 (Am. Bar Ass'n,).

of knowledge about the risks attendant to text messages (sloppiness, "misdialing", etc.) is no longer an excuse.

D. BEST PRACTICES/TIPS

The following best practices/tips are suggested to avoid the heightened risks involved with texting legal advice/work product:[82]

- If texting is necessary to communicate legal advice:
  - Ensure there is a policy on the use of texts that protects any third party interference;
  - Ensure that there is not an "auto delete" function on the electronic device that deletes text messages after a period of hours or days; and
  - Ensure that the recipient is the correct one.

- Keep strictly separate personal and work phones, or if your employer has a "Bring Your Own Device" policy, ensure that the policy protects text messaging.

- Do not forward any e-mails or texts containing legal advice, and ensure communication regarding legal advice remains between you and your client.

- Encourage verbal communication and do not text legal advice or work product.

[82] Vera Nackovic, *OMG! My text messages could be discoverable?*, Inside Counsel (November 30, 2015), http://www.insidecounsel.com/2015/11/30/omg-my-text-messages-could-be-discoverable

DATA AND SOCIAL MEDIA MISTAKES TO AVOID: FOR FACULTY, ADMINISTRATORS AND COUNSEL

Kevin E. Dolan, General Counsel, La Salle University

James A. Keller, Chair, Higher Ed. Practice, Saul Ewing LLP


EMAIL
MISTAKES

Which of the Following Is Made Up?

A. Email goes to entire student body: “we might have to spend the better part of the coming school year closing down the college.”

B. Email from faculty member to class with new assignment: “I’d recommend starting on these exercises sooner rather than later”, with a link to “youporn.com”.

C. Email from President, intended for General Counsel, goes to all faculty: “I think we need to figure out a way to get rid of 30% of our tenured faculty this year.”

Other Email Risks

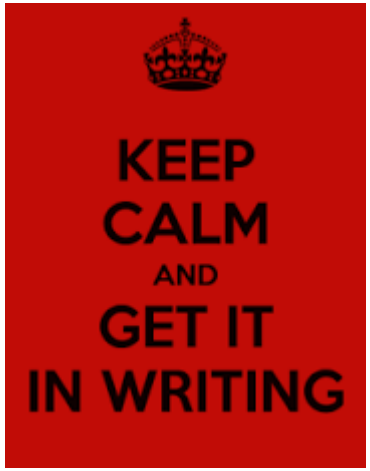
- Defamation.
- Harassment via email – vicarious liability for same?
- P.R. and "Public Shaming."
  - Drexel Professor example.

Mitigating Email Mistakes

- Separate out work and personal business as best as your can.
- Avoid reply all on anything sensitive – better to forward to select recipients.
- Recall that absent very unique circumstances, whatever is sent on institutional server has little to no expectation of privacy – emphasize this fact in training faculty/staff/administration.
- Training on/emphasize “Acceptable Use Policy”

Dolan Says…

Keller ... But ...




FRIENDS / 12" Single
WHODINI
BOT REWORK


Add Your Teacher as a friend?
Your Teacher
Add to List
Add a personal message...
Send Request
Cancel

Which Of The Following is Made Up?

A. Male professor “pokes” female student on Facebook; she views this as sexually harassing and pursues Title IX Complaint.

B. President sets up Facebook account and fails to set privacy settings; family photos and exchanges are viewed by entire campus and beyond.

C. Teacher FB-messages a student to say that “your boyfriend does not deserve a beautiful girl like you.”

Related Poll …

Do You "Friend" Students on Facebook or Instagram?

A. Yes.

B. No.

C. Is That On the World Wide Interweb?

D. Yes, and they never accept ☹

The Risks of (Cyber) Friendship

- Title IX/VAWA
- Violation of institutional social media policy
- What to like? What does it mean to like? Not like? Thumbs up to photo at the beach – what does that mean.
- The appearance of impropriety.

What Does the AAUP Say?

- Report on Academic Freedom and Electronic Communications (2014)
- Friending ok, all subsequent contacts might be appropriate.
- Policies aimed at restricting this: problematic to AAUP.
- U of Kansas Example.

Best Practices

- Make sure “appropriate use” broad enough to capture and define “appropriate” friending vs. inappropriate friending.
- Training: things that get lost in translation over social media:
  - Tone
  - Sarcasm
  - Intent – friendly “like” vs. prurient “like”.
- Use a separate FB/Instagram account to communicate with students/staff, assume public; keep personal one private.
- Stay away from social media late nights/weekends (at least re: student communication).
- Can I just talk to them on Monday? Do that.

Data Security and Cyber breaches

- Way, way too much for short time we have.
- See, generally:
  - Presidents
  - Adulterers
  - Colleges and Universities

Academia: "Soft Target" for Data Breaches and Cyberattacks

- Lots of personal data
- Lots of financial data
- If hospital system: lots of medical and protected health information.
- Open and collaborative environments
- Personal data often in hands of those not trained on careful use (e.g., faculty with protected student data)
- Examples: Los Angeles Valley College, PSU.

Liability / Risks

- Class Action Suits
  - U Hawaii
  - Stanford U Hospital and Clinics
- State Data Breach Notification Laws
- FERPA issues (and interplay with Gramm-Leach-Bliley Safeguards Rule).
- HIPAA issues.
- Reputational Risk.

Best Practices – To Mitigate a Breach

- Have written data breach/cyberattack policy in place.
- Audit IT systems and data – where are the risks?
- Training.
- Training.
- Training.

Best Practices – In Event of A Breach

- Follow Breach Policy.
- Assemble response team.
- Notify insurance.
- Involve counsel – at least internal – seek to maintain privilege/work product (??)
- Determine types of data implicated and resulting obligations
- If FERPA information involved – notify the FPCO(?)
- Notify those impacted (if required or appropriate).
- Notify law enforcement, when appropriate.
- Credit monitoring/identify theft protection – affirmatively offer it, when relevant – don't wait for the class action.

Texting

Do You Text Legal Advice / Work Product?

A. Yes, but only to my outside counsel/other lawyers on my team.

B. Yes, but only to President and high-level administrators.

C. Yes, but only during meetings when I am multi-tasking and really distracted.

D. Aren't you going to ask me to text my response right now? Don't you see the irony in that?


Messages
Mom
Edit
I got an A in Chem!
WTF, well done!
Mom, what do you think WTF means?
Well That's Fantastic

Risks of Texting

- Jonny Manziel Example
- Any riskier than email?
- Do people focus as much?
- As careful with spelling and wording?
- As careful about *retention*?
  - Spoliation examples.
- The inadvertent:
  - Responding to wrong text string
  - Disclosure to wrong third party … seems easier via text than email (??)
- If recipient has cellular service off …

Best Texting Practices

- Make sure not banned/frowned upon by your institution or local bar ethical rules.
- If legal work, and may be relevant to litigation, make sure not auto-deleted.
- If you have a separate work phone for work – use that one.
- What is the purpose? If it is to commit something to writing, might and email, or even an old-fashioned letter, be best? If it is just to chat, maybe a call?

Questions?

Do You Have Questions?

A. Yes, and I will text them to you.

B. Yes, I would email them but now I am worried about a data breach, thanks a lot.

C. Yes, but happy hour starts in 15, my friends.

D. If I say yes, then I am committed to follow through and come talk with you guys. So no. No I don't.