FDCC Winter Meeting
Hyatt Grand Champions Resort
Indian Wells, California
February 26 – March 5, 2011

AVOIDING SOCIAL MEDIA PITFALLS – TIPS FOR THE EMPLOYER

Presented by

Marc H. Harwell
LEITNER, WILLIAMS, DOOLEY & NAPOLITAN
801 Broad Street, 3rd Floor
Chattanooga, Tennessee 37402

©Copyright by Federation of Defense & Corporate Counsel,
11812 N. 56th Street, Tampa, FL 33617.
Reproduction of the contents hereof for noncommercial purposes is permitted.
AVOIDING SOCIAL MEDIA PITFALLS – TIPS FOR THE EMPLOYER

BY MARC H. HARWELL
(marc.harwell@leitnerfirm.com)

I. THE APPLICANT – POLICY CONSIDERATIONS FOR SCREENING

A. Discrimination Concerns

1. Avoid using social networks as the sole means for advertising/recruiting available positions. “According to the media analytics from QuantCast, only 5% of linked-in members are African-American and only 2% are Hispanic.” (See "Media Recruiting: Compliance Issues" by Robert Schepens, April 29, 2010.)

According to the EEOC Compliance Manual (the E-Race Initiative), “recruiting from racially segregated sources, such as certain neighborhoods, schools, religious institutions, and social networks, leads to hiring that simply replicates the societal patterns of racial segregation.” (Emphasis added.)

2. Obtaining knowledge of protected status/behavior is risky.

   a. Consider having a separate entity conduct the search to shield decision-maker from information regarding applicant that reveals protected status such as pregnancy, religion, sexuality issues, disability/etc. – Do you instruct against “friending”?

   b. Consider whether there is any distinction between “tell me about yourself versus a search of social media by name.” (In both instances so long as you have only accessed public information, aren’t you only getting information that the applicant chooses to make known to the public?) But what if you ask to “friend”?
c. Consider searching only on the final round of consideration; i.e., after interviewing and checking references – perhaps a means of reducing reporting workloads and responsibilities and perhaps reduce exposure to charges of discrimination.

(1) Document search.

(2) Document searcher.

(3) Document findings.

(4) Document decision points that are based on reasonable factors associated with legitimate business reasons or necessities.

(5) Beware of patterns to screening process to avoid disparate treatment and disparate impact.

B. Records Retention And Reporting Concerns

1. Follow OFCCP Guidelines on documenting, records retention, and reporting.

The Office of Federal Contract Compliance Program addresses recordkeeping for federal contractors and subcontractors and concerns the hiring process and the solicitation of applicants. The concerns in terms of the hiring process pertain to issues of race, gender, and ethnicity.

To comply with their recordkeeping requirements, (1) if an individual is considered for a particular position, maintain all expressions of interest; (2) maintain records identifying job seekers of a particular position; (3) for internal data bases, maintain records of each resume added (including the date added), the position for which each search of a resume was made, the criteria used to search resumes within the internal
data base, and when such criteria was used to search the resumes; (4) for *external data bases*, maintain a record of the position for which each search of the data base was made, the search criteria used, the date of the search, and each resume returned via such search. Only the resumes of jobseekers who meet the position’s basic qualifications must be saved. (See OFCCP Compliance: Understanding the OFCCP’s new ruling on internet applicants at http:\\ www.icims.com\docs\icims.ofccp.whitepaper.pdf.)

C. **Applicant Considerations**

1. Consider avoiding the creation of policies that are written for the lowest common denominator. Create lists of values, characteristics, and qualifications that are integral to your business. Educate and discipline based upon such values and characteristics. (Consider the example of NetFlix at SHRM HR Magazine, p. 34 (April, 2010).)

2. Screen to avoid the bad apple, and educate the applicant about your values.
   a. “In a recent study in the on-line *Journal of Managerial Psychology* (Vol. 24, Issue 6), Donald Klueemer of the Louisiana State University and Peter Rosen of the University of Evansville in Indiana say personal pages on Facebook and similar social networking sites can be used to predict the personality of a job-type candidate, much like a personality test.” (SHRM HR News at p. 22, February, 2010). Consider extraversion, agreeableness, conscientiousness, maturity, judgment, creativity, experience, etc.

D. **Interview Considerations (Pick the Right Time in the Process and Be Tactful)**

1. As you interview to cull the bad apples and to find employees with trustworthy qualities, consider the fact
that “49% of employees said a company edict would not influence their behaviors on-line, and about 53% said social networking pages are none of an employer’s business.” (SHRM HR News at p. 15, February, 2010.)

2. Consider asking about all publications including Twitter and Blogs (open to public). Perhaps explain that you are interested in their public expressions because what one says and does reflects upon both the individual and the employer.

3. Consider asking about nicknames.

4. Consider engaging in a discussion of social media use. Don't you want to know about the ability of applicant to promote him/herself; level of sophistication; qualities of discretion; adverse experiences with it; time spent with it, etc.? 

5. Consider explaining your social media policy to the applicant and asking whether the applicant has any concerns, questions, or problems with the policy. You want to determine whether the applicant will likely adhere to the policy.

6. Consider asking the applicant about his/her understanding of the pitfalls and problems that social media and electronic devices that interface with a network server present to you as an employer/client representative.

7. Consider explaining to the applicant your concern about the reputation of all employees and of your business. Explain the importance of safeguarding reputation from communications and activities that reflect poorly upon your business and its employees. Consider engaging the applicant in a discussion of such concerns including any perceived right to free expression and concerns of privacy. (First and Fourteenth Amendments apply to public entities.)
8. Consider explaining to the applicant that you reserve the right to monitor and do monitor employee social networking activities and other on-line activities and that any activities that conflict with your policies will likely result in disciplinary action. Engage the applicant in a discussion about his/her perceptions in regard to such a policy.

9. Disclose and enforce your right to manage every mobile device having connectivity to the network and your right to “wipe clean” the data of any such device.

10. Be mindful of employee confidentiality issues and concerns.

   a. Consider explaining the confidentiality rules of your business and the reasons for the rules. Engage the applicant in discussion of the importance of confidentiality versus the applicant’s perception about privacy rights and social networking.

   b. Strike a balance between the legitimate need to run the business in the best way possible and respect for employee’s privacy. True, you have a right to prevent workers from accessing “bad” websites and from importing harmful viruses that may compromise personal data; to guard employees from harassment; to protect trade secrets; to protect client confidences, etc., but can you monitor only to the extent necessary to achieve your legitimate needs?

   c. In considering your employee’s privacy rights, the courts will consider whether the employee’s interest in keeping the information private outweighs the employer’s interest in obtaining the information. (Restatement of Privacy § 7.03, Privacy Interest in Content Information.)
II. THE EMPLOYEE – SUPERVISION

A. Educate The Decision Makers – Consider the Laws That Apply

1. OFCCP; Title VII, State Human Rights Act; whistleblower laws; ADAAA; FMLA; ADEA; pregnancy discrimination; GINA; and HIPPA require your consideration in the context of social media and supervision of employees either because of confidentiality responsibilities (ADAAA, FMLA, GINA, and HIPPA), reporting and recordkeeping responsibilities (OFCCP), or protected status (Title VII, ADEA, Pregnancy Discrimination Act, ADAAA, FMLA, whistleblower, etc.) concerns that should at least be given some consideration in terms of your monitoring of employee communications.

2. The Stored Communications Act (SCA) covers access to stored wire and electronic communications and transactional records. The SCA prohibits third parties from accessing electronically stored communications without proper authorization. (18 U.S.C. § 2701.) You cannot intentionally access electronically stored information without authorization, and you cannot intentionally exceed an authorization to access electronically stored communications.

3. The Electronic Communications Protection Act (ECPA) (18 U.S.C. §§ 2510(17) and 2711(1)) protects against the interception of electronic communications without proper authorization.

4. Explain the concept of authorization versus intimidation in the context of an officer of Hawaiian Airlines. In Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), Mr. Konop, an airline pilot for Hawaiian Airlines, sued the airline alleging that it violated the Stored Communications Act when the Vice-President of the airline, who was concerned about whether the pilot was making untruthful allegations about the airline on a website, asked an
employee of the airline who had access to Mr. Konop’s website to give him access to the information. The Court held that, by logging onto the website, the Vice-President did not violate the “interception” provision of the Electronic Communications Protection Act. However, the Vice-President may have violated the Stored Communications Act by not having true “authorization” to access the website.

As an aside in light of the scope of this topic, the Ninth Circuit Court of Appeals remanded to the District Court the issues of whether Mr. Konop’s development and maintenance of his website constituted protected activity under the Railway Labor Act (RLA) and whether the airline interfered with Mr. Konop’s organizing activity in violation of the RLA. However, the Ninth Circuit held that the pilot’s critical comments of the airline were protected under the RLA. The rule seems to be that, unless the statements are made with actual malice such as knowledge of the falsity of the statement or with reckless disregard for the truth of the statement, the posting would be protected – even if false or defamatory.

5. Another case of poor judgment of an officer is Pietrylo v. Hillstone Restaurant Group d/b/a Houston’s, (2009 WL 3128420 (D.N.J. 2009)), where the Court upheld a jury verdict with punitive damages finding that the management of Houston’s violated the servers’/employees’ rights under the Stored Communications Act by accessing a CHAT group on an employee’s/server’s MySpace account without having received authorization from the employee to join the group. However, the jury found in favor of the employer on the plaintiffs’ invasion of privacy claims because the jury concluded that the plaintiffs had no reasonable expectation of privacy in MySpace.

6. Consider privileged communications in terms of privacy. Marina Stengart, who was the Director of
Nursing at Loving Care Agency until she resigned in 2008, used a company laptop and a business e-mail account. The New Jersey Supreme Court ruled on March 30, 2010 that Loving Care had violated Ms. Stengart’s rights to privacy when, after she left the employment of Loving Care, it viewed Ms. Stengart’s email exchanges with her attorney concerning a possible discrimination case against Loving Care. The New Jersey Supreme Court said that Loving Care’s written policy with respect to the right of the company to view personal e-mails was not entirely clear but also stated that even a clearly written company manual would not have justified Loving Care’s intrusion into her communications with her attorney. (Stengart v. Loving Care Agency, 990 A.2d 650 (N.J. 2010).)

7. To underline the importance of a written policy (that needs to be consistently enforced), consider the City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (the “sexting” case). Even if the employer is a public entity (consequently subject to the Fourteenth Amendment), the employee has little privacy rights in e-mail communications, text messages, or websites that they visit while at work if the employer has a policy in place that notifies employees of the fact that they do not have privacy rights in information posted via company property. If you fail to educate and explain your policy, employees’ expectations of privacy may be reasonable, and you may damage morale and productivity and create problems with respect to recruitment and retention. The Court concluded that the employer’s search of the messages was reasonable under the circumstances. However, the Court did not directly address Quon’s argument regarding privacy expectation. (If your client is a public entity, it may be confronted with a request for the release of records to the public even if the content of such records includes personal e-mails that are unrelated to the employee’s public employment; so be prepared to instruct. (See Larson v. Wisconsin Rapids
School District (Appeal No.: 2008AP967-AC, Wisconsin Court of Appeals (April 30, 2009).)

8. The Telephone Records and Privacy Protection Act of 2006 prohibits any individual from gaining access to an individual's telephone records through false representation without the consent of the individual whose telephone records are being sought. Consider this Act's application to the acquisition of text messaging information too.


10. Consider your restrictive covenants and non-solicitation agreement and non-disclosure agreement in terms of social networking websites such as Linked-In. In Tek Systems v. Hammernick, No. 0:10-CV-00819-PJS-SRN (Complaint filed March 16, 2010), (pending in the United States District Court for the District of Minnesota and is scheduled for trial on August 1, 2011), Tek Systems, Inc. is an IP staffing firm. Its employees included Brelyn Hammernick, who, as a condition to employment, signed an agreement that stated in pertinent part as follows:

For a period of 18 months following termination of her employment, she was prohibited from directly or indirectly approaching, contacting, soliciting, or inducing any person who had been a "contract employee" during the 2-year period prior to the date of her termination and about whom she knew by reason of her employment with Tek Systems: to cease working for Tek Systems at clients or customers of Tek Systems; to refrain from beginning work for clients or customers of Tek Systems; and to not provide services to any individual, corporation, or entity whose business is competitive with Tek Systems.
Tek Systems sued Ms. Hammernick and two other employees for violation of the agreement. Tek Systems alleged that Ms. Hammernick unlawfully communicated on behalf of her new IT employer with other contract employees via the social networking website LinkedIn.

11. Consider exposure associated with the well-intentioned employee who publicly supports a client’s product or you. Pursuant to Federal Trade Communications Act (FTC) at 16 C.F.R. § 225, Guides Concerning the Use of Endorsements & Testimonials in Advertising, “comments about an employer can be considered endorsements, advertising, and testimonials.” Does a connection exist between the endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement? If the connection is not reasonably expected by the audience, such connection must be fully disclosed.

… Although the Commission has brought law enforcement actions against companies whose failure to establish or maintain appropriate internal procedures resulted in consumer injury, it is not aware of any instance in which an enforcement action was brought against the company for the actions of a single “rogue” employee who violated established company policy that adequately covered the conduct in question.

B. Educate Your Workforce

1. Explain the perils of the use of social media – you cannot control your friends. Just because you make a setting private does not mean that your friend will not make such information public; consider the cookies that are installed as you navigate; the world is watching; you can never retract what you publish on the web – you can only apologize; etc.
2. Consider the company called [X+1]. From a single click on a website, [X+1] quickly identified Carrie Isaac as a young Colorado Springs parent who lives on about $50,000 a year, shops at Wal-Mart, and rents kids’ videos. [X+1] deduced that Paul Boulifard, a Nashville architect, is childless, likes to travel, and buys used cars. (See WSJ at p. 1, Wednesday, August 4, 2010.)

3. According to a Cisco 2010 Mid-Year Security Report, “[w]hen workers want access to social networking technologies, they’ll get it – even if it means circumventing corporate policies.” Cisco relied upon a report from Accenture which “found that millennials make heavy use of social networking sites while on the job whether their employers allow them to or not.” According to the [Accenture] report quoted in the Cisco 2010 Mid-Year Security Report, 45% of employed millennials [people who are 30 years old and younger] use social networking sites when they’re at work, but only 32% say that this use of social network is supported by their departments.” So perhaps 13% disregard their employer’s policies.

According to the Cisco 2010 Mid-Year Security Report, “only 1 in 7 of the companies participating in [their] study have established formal processes for adopting social networking tools for business purposes.

Only 1 in 5 businesses said they had policies in place for the use of social networking tools.

Only 1 in 10 survey respondents said that their IT Department had direct involvement with social media initiatives.”

4. Rather than alienating the millennials, consider enlisting the assistance of the millennials to educate those less knowledgeable and try to get them to buy into the security of your system. But note that millennials have been documented as having a “much
looser notion of on-line privacy than … older workers.”

30% of millennials [say] that they write openly about themselves on-line. (Cisco 2010 Mid-Year Security Report.) This underlines the importance of who you are hiring and whether you are getting “buy in” to your policies and of your need to monitor.

5. Recognizing that over 500 million people are using Facebook alone and are spending over 700 billion minutes per month on Facebook (www.facebook.com/press/info.php?statistics) (and of those users more than 150 million are accessing Facebook via mobile devices and use Facebook more than 2x non-mobile users) and recognizing the overwhelming use of other social media sites, consider whether an outright ban of your employees from any use of social media during business hours is practical and whether such a ban limits the effectiveness of your firm to use social media for the benefit of your firm. As an alternative, consider crafting a rule and an educational program that develops a proper use of social media and install productivity standards that must be met whether the employee uses social media or not.

6. Be consistent in your treatment of employees.

7. Set up and notify employees of chain of command for notification of problems and concerns.

8. Investigate reports of unacceptable conduct/communications.

9. Consider instructions to supervisors regarding limitations on the use of social media during the investigation of employees. Consider whether “friending” an employee is appropriate. (See concerns noted under “The Applicant”.)

10. Monitor unprofessional conduct/comments and violations of other policies.
11. “About 74% of employees said they believe it is easy to damage a brand’s reputation via sites such as YouTube, Twitter (this social media website allows users to “Twit” or to “Follow” other users by subscribing to a user’s Twitters, which do not require approval – so long as the twitter is not using the “private accounts option” – most do not), and Facebook. Even so 15% said that if their company did something that displeased them, they would comment about it on-line.” (SHRM HR News at p. 15, February, 2010.)


14. Be proactive; mentor; and re-educate regarding what is important/what should concern you.

15. Create a policy that outlines the devices that are acceptable to your business, and explain why certain devices are not permitted.

16. Plan to regularly revise your policies to provide for future technological advances.

17. Track who is accessing what information and with what device and for what reason.

18. In 2009 in the United States alone, the total loss linked to on-line fraud was $559.7 million – up from $265 million in 2008 (See Cisco 2010 Mid-Year Security Report.) An innovation gap exists between criminals and businesses. Businesses must answer to shareholders and clients and employees; comply with laws and regulations; and establish systems, policies, and protective controls. Criminals find no reason to spend hours in research and development making sure that their results are proof-positive. If something works, they use it. If it doesn’t, they turn to another idea.
19. In the first three months of 2009, Microsoft announced 58 vulnerabilities and in the first three months of 2010, Microsoft announced 77 vulnerabilities. In the same period in 2009, Adobe announced 9 vulnerabilities; in the first three months of 2010, Adobe announced 26 vulnerabilities, and these companies delivered patches and updates. If your employees are not downloading the patches or responding to the requests for updates, they become the weak link to your system.

20. Your lawyers may be the biggest risk of security breaches to your firm. Consider that your lawyers may be your firm’s most difficult employee to control. Your lawyers are perhaps the ones pushing the hardest to have the most trendy new device/cell phone and perhaps rarely ask IT for permission to use the device. Your lawyers are probably the most mobile of your employees. They spend more time on the road and have more opportunities for laptops and mobile devices to be stolen or lost or penetrated. Also, cyber criminals have become very adept at using information on Facebook, Linked-In, and other social media sites to piece together seemingly innocent bits of data to crack passwords and hack into email accounts. (Cisco 2010 Mid-Year Security Report at page 23.)

21. In 2009, a Times researcher from the Carnegie Mellon University demonstrated that by using publicly available information from social networks the researcher could reliably predict the social security numbers of nearly 5 million Americans in fewer than 1,000 attempts. (Cisco 2010 Mid-Year Security Report.)

22. How strong are your access control protocols? What protections are built into your network to prevent breaches?

23. Explain to your employees the necessity of using strong passwords and explain to them the reason
they need to change their passwords on a regular basis.

24. Avoid surprises; conduct annual 360° reviews that provide direct and honest feedback; be fair; do not coddle; do not tolerate substandard performance.

25. To what extent can you redact personal information from an employee’s file – such as family health history information; social security numbers; information regarding health; and other sensitive data?

26. Consider the problems and the potentials associated with web-privacy software such as “VaporStream” which has a self-destructing e-mail feature that allows the users to send e-mails and instant messages that cannot be forwarded, saved, or printed, and which leave no electronic record after they are read; or “Connect In Private Corp.,” which routes a user’s web traffic through computer servers in Canada to mask their IP addresses, or “Anonymizer, Inc.” which secures web connections that mask a user’s IP address and provides e-mail aliases for on-line form. (WSJ, at p. B-6, September 8, 2010.)

27. Thirty-five years ago under the IPV4 protocol, IP addresses were established, but by 2012 IPV4 addresses are expected to be depleted. Consequently, an IPV6 initiative has been deployed which should provide trillions of new addresses but which is susceptible to rogue network devices that masquerade as IPV6 routers and other potential security problems. Is your firm ready for the change?

28. Consider whether you may use the Communications Decency Act to secure an agreement from an employee and/or client to obtain an agreement that transfers to you a copyright of any on-line content about you or your firm. Dr. Jeffrey Seagal, who is a neurosurgeon and founder of “Medical Justice,” has created such mutual privacy agreements that prohibit patients from rating their doctors. If the patient
violates the agreement, the doctor uses the agreement to have the ratings website remove a particular post by the patient. (See ABA Journal, June, 2009 at p. 14.)

29. Instruct and obtain written acknowledgement of receipt and understanding regarding:

a. Policies against discrimination and harassment at work/away from work;

b. The obligation to report any knowledge of any act/statement of discrimination or harassment (at work/away from work);

c. The understanding of his/her "at will" status subject to the exceptions – may not fire you because of your age, race, religion, nationality, because you file a workers’ compensation claim, because you report illegal activity, etc.;

d. The duty to maintain confidences and not publicize private information;

e. The acknowledgement and understanding that communications via social media are not private;

f. The prohibition or limitation of personal communications during business hours. (Do you allow the lowest common denominator to define the policy?);

g. The policy that all employee communications via company property or connection to company server may be monitored by company;

h. The prohibition against disparaging the company and employees of company (stress the team concept; reliance upon reputation; and zero tolerance for tearing apart or
adversely affecting team or reputation through unprofessional conduct);

i. The obligation to comport oneself in a manner that reflects favorably upon the professional organization – dress, conduct, speech, writings, postings, etc.;

j. The prohibition against taking business/client documents home; the prohibition against recording or copying business/client documents on any personal device; and the prohibition against transmitting any business/client information without the approval of your decision makers;

k. The appropriate use and access of company/client information via devices that connect to server; and

l. The prohibition against employee public promotion of the Firm or a client without appropriate disclosure under FTC guidelines.

m. The obligation of the employee to notify your IT Director of all personal devices used to connect to your network; to always update with the patches that are recommended; to change passwords; etc.

III. THE EMPLOYEE – DISCIPLINE

If an employee does something that is wrong or violates your values and the expected characteristics of your professional organization, explain the violation, seek the response of the employee to the charge, seek a statement of understanding from the employee regarding the discipline, and seek the employee’s understanding of the responsibility of the business to use all resources and laws to protect reputation, confidences, and private information.
Consider the severity of the discipline; consider an amicable departure; allow the employee to keep any shred of dignity that he or she may deserve; get a release in exchange for severance, etc.

IV. A FACTUAL SCENARIO

Jane Sass is a mother of twin baby girls. She is Assistant General Counsel of Grab-N-Go which is a chain of 530 restaurants located throughout the Sun Belt.

While Jane was attending a mediation in Houston, her husband was attending to the libido of their next door neighbor.

After struggling through a difficult divorce and in order to address a crushing loneliness, she turned to Facebook and E-Harmony to network a team of dates that she called her bullpen.

A photo of her in a bikini that she posted on Facebook and on E-Harmony generated much of the interest that formed her bullpen.

Within a day of transmitting the photo, she was told that she could accept a severance agreement and quit or she would be terminated for violating the company’s policy against the use of the company’s property (the company furnished laptop and an e-mail address) for personal use. She accepted the severance agreement and quit.

Within just a few days, she submitted a resume to The Firm with a cover letter and a letter of reference from an officer/good friend of Grab-N-Go. Her resume was impressive – Order of Coif from University of Georgia, a top 50 law school; Law Review; 4 years as an associate at Leitner, Williams, Dooley & Napolitan’s office in Nashville; and 3 years as Assistant General Counsel at Grab-N-Go. The Firm considered her application (attached hereto). The Firm interviewed her. The Firm was hopeful that she might be helpful in getting the Grab-N-Go business. A letter of reference from an executive at Grab-N-Go fueled the hope. Her explanation that she quit to return to private practice where she could make more money; be more stimulated; and use her experience and connections with Grab-N-Go to further the interests of The Firm seemed reasonable – albeit a bit rash. The Firm needed an experienced associate to replace an associate who left to work for an Atlanta firm that assured her that she could set her own hours and would not have to meet any minimum hours threshold so long as she gave them good work product.
The Firm searched Jane Sass, and it found nothing scandalous or inappropriate. The Firm did not try to friend her, so her privacy setting blocked her Facebook information. The Firm did note that she had 852 friends in Facebook. The Firm did not ask about friends and references (it relied on letter from the executive officer; good resume; good interview; and the confidence of a litigator (Hiring Committee Chair) to read people.)

In its search of public records, The Firm discovered that she was recently divorced and had custody of twin girls. The Hiring Committee worried about whether she could bill the requisite 2,000 minimum hours and be a mother to two babies and work to develop the business. Also they were upset that she had not been forthcoming when she said that she did not have any concerns about meeting their demands. Some committee members thought that they could not refuse to hire her based upon such a concern. After much discussion, the immediate demands of the day and the allure of a connection to Grab-N-Go won, and she was offered a job as an associate.

Jane worked hard. She put out good work product. The Hiring Committee gloated over their choice … until the managing member sent a photograph of a bikini-clad Jane with a note from General Counsel of Trinity Savings & Loan (an important client of The Firm) asking, “Isn’t this your new associate, Jane Sass? Who are you hiring over there?”

The managing member, Reid Cox, confronted Jane Sass with the photograph. He reprimanded her; ridiculed her judgment; and demanded that she do nothing further to jeopardize The Firm’s relationship with Trinity in particular and the professional reputation of The Firm in general.

Eager to keep her job, Jane agreed, but she was upset with his treatment of her. After all, it was just a photo of her in a bikini from Neiman Marcus. She thought that she looked great.

While still upset that evening from her home, she posted on Facebook and E-Harmony from her I-Pad: My boss, OZOB, threatened to fire me over the photo of me in my bikini, on my float, in my pool – PLEASE delete that photo. I don’t need any more trouble from him. The posting elicited similar responses from many of her 852 friends – (1) He sucks; (2) That sucks; (3) He can’t get away with treating you like that; (4) You look hot, no can do; (5) Whatever happened to freedom of expression?; (6) Reid Cox is a communist Nazi; (8) A friend of mine knows that guy and knows a guy who waited on Cox at dinner last week – he’s a drunk; … .
Determined to not get another call from Trinity about Ms. Sass and because she had been showing up to work closer to 9:00 a.m. rather than 8:30 a.m., Mr. Cox instructed the head of The Firm’s IT Department to step up the monitoring of Ms. Sass. Within days, the increased scrutiny pays off. A player in Ms. Sass’ bullpen (nickname “Pinhead”) sends her a text message on her Firm’s cell phone that says, "If your boss is not making you work late, let’s tie one on tonight at your place after you put the kids down."

The IT Director searches “Pinhead” on Facebook and finds that he has a public setting – he wants everyone to see him; to know when he is eating, drinking, walking, moving, breathing. … He sees the rants against Mr. Cox and sees her reference to him as OZOB (his 12-year-old explains that OZOB is BOZO). He provides the information to the managing member who decides that he’s through with her. A Google search of his name brings up (and continues to this day to bring up) a couple of hits that reference him as being a communist, a Nazi; a drunk; and more. One rant even has a link to a photo of him in a Speedo.

He terminates Jane Sass for violation of The Firm’s Code of Professional Conduct; for violation of The Firm’s prohibition against the use of Firm property for personal use; and for insubordination.

Ms. Sass finds herself unemployed in a terrible economy; with two children; and a “for cause” termination that threatens any prospect that she has for hire with another firm. Feeling trapped and thinking that Mr. Cox has treated her unfairly, she files a lawsuit against The Firm and avers that the underlying reasons for her termination were gender based. After all, it is common knowledge that Mr. Cox swims at the Sports Barn in a Speedo.

She was no more late than most of the other associates. She only made one comment about Mr. Cox being an OZOB and that was to her friends as she tried to do what Mr. Cox wanted her to do; i.e., not have the bikini photo circulated any more. She contended that all reasons proffered by The Firm for the termination were pretextual.

She tells her 852 friends on Facebook that she has been fired and doesn’t know what to do. She has two baby girls to feed; no money to open her own practice; and no prospects for employment.
A firestorm erupts on Facebook. Twitters and blogs are posted. The common theme (aside from Mr. Cox and the Firm “sucking”) are that Mr. Cox and The Firm discriminate against women; subjected Ms. Sass to a moral/professional standard that others in The Firm failed to meet; that a right wing Christian group that made up the Board of Trinity Savings and Loan worked to get the mother of two fired; ….

A. Questions Raised By The Factual Scenario

- Before hiring Ms. Sass, would you have logged onto Facebook and asked to be “friended” by Ms. Sass?

- If you refused to hire Ms. Sass after performing your on-line search and discovering that she is the mother of twin girls, did you increase your exposure in a gender-based lawsuit?

- In considering Ms. Sass as an applicant or in monitoring Ms. Sass as an employee, does The Firm’s request of Ms. Sass to “friend” The Firm as either a condition of getting an offer or as a condition of remaining an employee violate the authorization requirements of the Stored Communications Act? What are the considerations?

- If The Firm required a “true friend” of Ms. Sass who was also an employee of The Firm to copy Ms. Sass’ “private” Friend pages for The Firm’s review, did The Firm “access” the information in a manner that violates the Stored Communications Act?

- If a representative of The Firm had created an E-Harmony account and a profile that was designed to and did gain the representative access to Ms. Sass’ E-Harmony profile, would The Firm have violated the “access” provisions of the Stored Communications Act, or would it have violated the privacy interests of Ms. Sass?

- If The Firm discovered Ms. Sass’ status as a single mother of twin baby girls by “friending” Ms. Sass on Facebook or through an E-Harmony profile and if following the acquisition of such information The Firm either refused to hire or terminated her, to what extent is The Firm’s exposure to a claim of gender-based discrimination affected?
How would such employer practices affect employee morale in general and the morale of Ms. Sass in particular?

Is there a significant difference between asking the question in an interview, “Tell us about yourself,” versus gaining access to private information through a public portal?

In tough times and responding to the demands of a powerful client, The Firm instructed Ms. Sass to “do nothing further to jeopardize The Firm’s relationship with Trinity and the professional reputation of The Firm.” In what ways could The Firm have handled the client in a better fashion? In what ways could The Firm have dealt with Ms. Sass in a better fashion?

What, if anything, would you have recommended The Firm do to avoid the public backlash against Mr. Cox and The Firm?

What, if anything, could The Firm and/or Mr. Cox have done to avoid the critical comments posted by Ms. Sass?

What “non-private” clues in Ms. Sass’ resume and limited, publicly displayed information on Facebook may have warranted scrutiny or concern?

Marc H. Harwell
Leitner, Williams, Dooley & Napolitan
801 Broad Street, 3rd Floor
Chattanooga, Tennessee 37402
Tel: (423) 424-3908
Fax: (423) 308-0908
Web: www.leitnerfirm.com
MARC HARWELL

In 1986, Marc H. Harwell obtained his Bachelor of Arts degree from the University of Tennessee at Knoxville, where he graduated *cum laude*. In 1989, he graduated from the University of Tennessee at Knoxville College of Law. He was a member of the *Tennessee Law Review* and has been published by that *Review*.

Since 1995, he has been a member of the law firm of Leitner, Williams, Dooley & Napolitan. Since approximately 2004, he has served as the Chairman of the Hiring Committee for the six offices of that firm.

Since 2009, he has served as a Disciplinary Hearing Committee member for the Tennessee Supreme Court’s Board of Professional Responsibility. From approximately 2004 through 2010, he served as co-editor of the ALFA International *Transportation Update* – a quarterly publication. He has published (including FDCC’s Quarterly – Spring, 2008) and lectured extensively on transportation, employment, and insurance related issues.

In Chattanooga, Tennessee, he has served as member and as chairman of numerous organizations such as the American Heart Association-Hamilton County, Siskin Foundation’s 365 Club (for disabled children), the Arts and Education Council, and the American Cancer Society’s PINK-Hamilton County.