

Good example of cyberharassment essay

[Business](#), [Employee](#)



This memo is in response to the conversation that we had in regards to the use of social media and your possible exposure to lawsuits. Some of your concerns included lawsuits for defaming language which you may post on Facebook, Twitter, Instagram, blogs, forums, websites or various other places on the Internet as well as other common social and other types of media communications. You also expressed concerns pertaining potential legal liability regarding requests for access to employment candidates' social media sites who are being interviewed for a position at your company.

In this memo, I intend to discuss specific federal, state, and local laws and regulations that govern the use of social media. The topics that I intend to focus on in this memo include the following: Cyberharassment, Cyberstalking, and existing laws governing workplace interviews and social media password requests.

Cyberharassment is characterized by the use of threatening or harassing email, instant messages, blog entries or websites with the sole purpose of tormenting a person. It should be noted that the term “ Cyberbullying” is at times used interchangeably with “ Cyberharassment.” However, Cyberbullying is used to refer to the harassment or bullying of minors within an electronic context, such as the Internet. Therefore, for purposes of business law, it would be best to focus on the topic of Cyberharrassment. According to the statutes stipulated by Alabama laws in Section 13A-11-8: “ Communicates with a person, anonymously or otherwise, by telephone, telegraph, mail, or any other form of written or electronic communication” in a manner which is intended to alarm or harass then that person is guilty of committing the crime of harassing communications (2014, Alabama

Legislative Information System Online [ALISON], pars. 7, 8). Please note that harassing communication can be interpreted as communication which annoy and molest. Therefore, if your company plans to post information on social media sites such Facebook, Twitter, Instagram, and SnapChat, then this should be done in a non-invasive manner, and these posts should not be made frequently as to cause annoyance and molestation of the individual. The penal code section of 422-422. 4 of the state of California stipulates that any individual who “ willfully” threatens to commit a crime which will result in “ death and greatly bodily injury to another person” with the “ specific intent” with the statement being made “ verbally, in writing, or by means of an electronic communication device” is to be taken to be a threat(2014, California Legislature, par. 1). This is irrespective of the fact that there was an intent to carry it out (2014, California Legislature). This crime shall be punished by “ imprisonment in the county jail not to exceed one year, or by imprisonment in the state prison” (2014, California Legislature).

It should be noted that if an employee of your company uses threatening, harassing and defaming language on the internet, you could be liable for this employee’s actions if disciplinary measures are not implemented by your company. For instance, the Espinoza v. County of Orange case, which was filed in February 9, 2012, the Court ruled that the employer of Mr. Ralph Espinoza should pay \$1. 6 million to him for their failure to take action against an employee for harassing Mr. Espinoza through his blog entries or posts (2012, O’Learly & Ikola). O’Learly and Ikola wrote that the jury “ returned a verdict” against the defendant, finding it “ liable against for harassment based on plaintiff’s disability and failure to prevent the

harassment” (2012, O’ Learly & Ikola, Section 6, para. 2). The jury found the defendant on the “ retaliation and wrongful discharge” were “ causes of action” and in favor of “ the individual defendants [Mr. Espinoza’s co-workers] on all claims” (2012, O’Learly & Ikola, Section 6, para. 2).

Cyberstalking

Although it is difficult to incriminate someone who is accused of Cyberstalking, Cyberstalking is still an issue that both you and your company should be concerned about. Katherine Quarmby’s article, “ How the Law is Standing Up to Cyberstalking” in her article outlined how Leandra Ramm, who was harassed and threatened by Cyberstalking living in Singapore, was able to be the first person to successful in an international Cyberstalking case (2014). Ms. Ramm hired a cybercrime expert, A. J. Fardella, who had connections with the US Secret Service, who could “ navigate the American and Singaporean legal system” (Quarmby, 2014, para. 4). The article explains that Cyberstalking cases (especially cases which transnational) are often difficult to prosecute because “ countries have different laws on stalking” (Quarmby, 2014, para. 6).

Nevertheless, it should be noted that the there are various stipulations governing the Cyberstalking in numerous states. For example, the laws in the state of Florida defines the term “ Cyberstalk” as the act of engaging in a “ course of conduct to communicate, or to cause to be communicated” words, pictures or other images, or language by or through the use of electronic mail or other electronic communication “ directed at a specific person” causing “ substantial emotional distress” to that individual (2014, The Florida Legislature, para. 5). The Florida Legislature revealed that

whoever Cyberstalks another individual commits the crime of “ stalking, a misdemeanor of the first degree” (2014, The Florida Legislature, para. 6). The most recent Cyberstalking case which took place on the shores of the United States involved Jason White, the owner of an art gallery in Temecula Art Gallery and art dealers based in California (2014, US Attorney’s Office). The Federal Bureau of Investigation (F. B. I.) reported on its website that White “ allegedly” sent threatening text messages his former employer, his son, and his former supervisor (2014, US Attorney’s Office, para. 6). The FBI report indicated that art professionals whom White had business relationships with were harassed with “ threatening emails to demand hundreds of thousands of dollars” in exchange for taking down websites with derogatory information about them which he had published on the Internet (2014, US Attorney’s Office, para. 4). White was later sentenced to death on September 29, 2014 to 60 months in federal prison.

Therefore, based on an analysis of the international Cyberstalking cases involving Ms. Ramm and the art dealers, it is easy to conclude that the FBI has the resources to thoroughly investigate Cyberstalking cases despite the fact they are difficult to prosecute. As a result, as your legal counsel, I will advise that you ensure that none of your employees at your company engage in such acts as this will ensure that your company to be exposed to the scrutiny of the FBI and it is a possibility that your company can be liable if your employees engage in such activities you, as their employer, refuse to enforce the requisite disciplinary measures, as illustrated in the Cyberharassment case of Espinoza v. Orange County.

Laws Governing Workplace Interviews and Social Media Password Requests

Laws governing workplace interviews and social media password requests have been recently introduced in states such as California. There was an Assembly Bill was recently amended in this state on August 21, 2014. The Senate in California is expected to give a third reading of this proposed bill, as indicated by the Official California Legislative Information's website (2014, California Legislature). This Amended Bill stipulates that an employer shall not request or require an employee or an "applicant for employment" to disclose a "username or password for the purpose of accessing personal social media," access "personal social media" in the presence of the employer, or divulge "personal social media" except in special circumstances (2014, California Legislature, p. 3, ll. 23-27). The employer can request access to an employee's or potential employee's social media account if this information is "reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and violations" (2014, California Legislature, p. 3, ll. 29-35). The Amended Bill stipulates further that the employer is permitted to request a password and a username or "other purpose of accessing" an "employer-issued" electronic device (2014, California Legislature, p. 3, 36-39).

Louisiana has made itself step ahead of California by enacting the Personal Online Account Privacy Protection Act on May 22, 2014 (2014, Louisiana State Legislature, para. 3). This act allows an employer to comply with a "duty to screen employees or applicants" before hiring or "to monitor or retain employee communications" that are established pursuant to state or federal law, rules or regulations, case law, or "rules of self-regulatory

organizations” (2014, Louisiana State Legislature, p. 4, ll. 9-12). However, an employee cannot request or require an employee or “ applicant for employment” to provide any “ username, password, or authentication information” which permits access to the employee’s or applicant’s personal online account (2014, Louisiana State Legislature, p. 2, ll. 28-30). The employer is also prohibited from discharging and disciplining an employee or applicant for employment for “ failure to disclose” any authentication information to access a personal online account.

I hope that you will find the information which I have provided to be informative and useful in creating the most appropriate policies for your organization so as to avoid lawsuits and not violate the privacy of employees and potential employees of your company.

References

Brenner, S. (2001). State cybercrime legislation in the United States of America: A survey. *Richmond Journal of Law and Technology*, 7(3). Retrieved November 25, 2014, from http://jolt.richmond.edu/v7i3/article2.html#N_10_

California Legislature (2014, August 21). Assembly BillNo. 25. Retrieved November 25, 2014, from http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0001-0050/ab_25_bill_20140821_amended_sen_v96.htm

California Legislature (2014, November 25). AB 25 Assembly Bill - Status. Retrieved November 25, 2014, from http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0001-0050/ab_25_bill_20141031_status.html

Florida Legislature (2014, November 25). The 2014 Florida Statutes.

<https://assignbuster.com/good-example-of-cyberharassment-essay/>

Retrieved November 25, 2014, from http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0700-0799/0784/Sections/0784.048.html

Louisiana State Legislature (2014, November 25). 2014 Regular Session.

Retrieved November 25, 2014, from <http://www.legis.la.gov/legis/BillInfo.aspx?s=14RS&b=HB340&sbi=y>

Louisiana State Legislature (2014, May 22). Regular Session, 2014 House Bill No. 340. Retrieved November 25, 2014, from <http://www.legis.la.gov/legis/ViewDocument.aspx?d=908152>

O'Learly, J., & Ikola, J. (2012, February 9). ESPINOZA v. COUNTY OF ORANGE | Leagle.com. Retrieved November 25, 2014, from <http://www.leagle.com/decision/InCACO20120209057>

Quarmby, K. (2014, August 13). How the law is standing up to Cyberstalking. Retrieved November 25, 2014, from <http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html>

US Attorney's Office (2014, September 29). Cyberstalking case involving violent threats against art dealers and their children leads to five-year federal prison term. Retrieved November 25, 2014, from <http://www.fbi.gov/losangeles/press-releases/2014/cyberstalking-case-involving-violent-threats-against-art-dealers-and-their-children-leads-to-five-year-federal-prison-term>