

Practical tips regarding social media and text messages

by Tricia Hoffman-Simanek
phs@shuttleworthlaw.com

In the context of litigation and investigations, social media websites, like Facebook and MySpace, and communications like voice and text messages can be sources of evidence an employer may wish to have to support their position in litigation or during investigations. However, the communication industry frequently cites the Stored Communications Act, claiming they cannot divulge materials and information absent one of the exceptions of the Act.

The Stored Communications Act (SCA) states:

A person or entity providing an *electronic communication service* to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service. A person or entity providing *remote computing service* to the public shall also not knowingly divulge contents of any communication carried or maintained by the service.

18 USC § 2702 (2008). There are a few exceptions to whom the communications can be disclosed. Such communication can be disclosed:

1. to an addressee or intended recipient of such communication

- or agent of such addressee or intended recipient;
2. as otherwise authorized (relating to investigations, criminal warrant, etc);
3. with the lawful consent of originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
4. person employed or authorized or whose facilities are used to forward such communication to its destination;
5. as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
6. to the National Center for Missing or Exploited Children;
7. to a law enforcement agency if contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime; or
8. to a governmental entity, if the provider believes in good faith that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

From a statutory perspective, in civil litigation, it seems as if there are only two real ways to obtain the information: (1) see if the addressee

or intended recipient will provide consent to allow for the release of the information or (2) obtain consent from the originator, addressee or intended recipient in the case of electronic communication services, or from the subscriber in the case of remote computing service. The case law reviewed seems to be clear that a subpoena alone (absent consent) will not overcome the SCA. The Courts have commented that there is little support that allows a court to compel a third-party to provide the information just because of a subpoena.

Thus, as it pertains to social media, and even text messages, it remains largely uncertain how each state will interpret and apply the statute.

(continue on next page)

ALSO IN THIS ISSUE

Retention policies of carriers Page 2

LinkedIn & Trade Secret / Non-compete issues Page 3

Employee's praise = Misleading advertising? Page 4

Guns & the workplace Page 4

Notable Dates & Speaking Engagements Page 5

(cont. from Page 1) . . . **Facebook and text messages**

Social Media / Facebook

Facebook specifically has a Q & A on its website regarding release of content. It notes that federal law and Facebook policies prohibit the disclosure of user information, citing the SCA. Facebook states that those statutes prohibit Facebook from disclosing the **contents** of a user's account to any non-governmental entity, even pursuant to a valid subpoena or court order. (Facebook's policy does note that if you are a represented party to a civil case and believe the basic subscriber information is "indispensable" and is not within the possession of a party, you must personally serve a valid California or federal subpoena on Facebook. Basic subscriber information only includes: name of subscriber; address; local and LD telephone toll billing records; telephone number or other account identifier; type of service provided; and length of service rendered).

Further, even though the SCA seems to suggest that a proper authorization (as noted above) will allow the release of information, attempts by our own office with Facebook have been met with resistance. Facebook's lawyers have stated it's position is that the Stored Communications Act provides that content *may* be provided with a valid authorization – not that it *must* be. Thus, in a recent attempt, Facebook refused to provide the information, despite an authorization.

The lesson: If you see content on Facebook about an employee that you think you may want to have later if litigation ensues, print it then and there and/or save it in some fashion. This is important because if the information on Facebook is later deleted by the owner of the account, Facebook states it not be able to provide content once a user deletes content from his/her account.



Text Messages

A similar problem may also be found with cell phone providers or other services. Additionally, the multitude of cell phone providers have varying policies on how long text messages are kept.

The lesson: Again, if you are in a situation where you have access to a voice mail message, text message or other that you believe may be important later, and can validly save the message (i.e., company phone), then methods to perpetuate that information should be made at the time as there is no guarantee you'll be able to access it later from the company itself.

When in doubt, contact your Shuttleworth attorney for more advice on how to properly obtain and preserve this type of potential evidence. ♦



Common carrier current retention policies

Below is a chart of some of the common carriers and what they have conveyed to us as their policies as of today for saving text messages, as well as maintaining call logs.

****Since carriers may change their retention policies, please contact them specifically for more details should you desire obtaining such information.****

US Cellular

- ♦ Content of text messages retained 3-5 days
- ♦ Text messages – number to/from – 1 year to date
- ♦ Incoming call logs – year to date
- ♦ Outgoing calls logs – indefinitely; would show on customer's monthly bill

I-Wireless

- ♦ Content of text messages retained up to 1 year
- ♦ Incoming calls – varies. Presently for prepaid customers, 18 months; for postpaid customers, 3 months

AT&T

- ♦ Content of text messages not retained
- ♦ Date of text messages – number to/from – 3 yrs
- ♦ Incoming calls logs– 3 yrs
- ♦ Outgoing calls – 3 yrs

T-Mobile

- ♦ No content of text messages retained



Employee use of LinkedIn and trade secret / non-compete issues

by Terri Davis tcd@shuttleworthlaw.com

Many employers not only allow, but encourage their employees to use social and professional networking sites, such as LinkedIn. In many fields where networking and contacts are all-important, LinkedIn can be an essential tool in creating and managing that network of potential clients, customers, or business partners. Many employees create contacts with all of their customers on LinkedIn, connecting with them on the site. The question then arises: if the employee leaves the company, does her continued use of her LinkedIn page, with all its information about the customers of the company, violate a non-compete obligation or reveal the former employer's trade secrets in the form of "customer lists?"

In a recent case in the U.S. District Court of New York, a former employer of a recruiter sued the employee when she left the company to start her own recruiting company. There was no non-compete or non-solicitation agreement in place between the parties. However, the employer claimed that the former recruiter was contacting the company's clients and "poaching" away all of its recruiters. The company also claimed that its database of customer information was a trade secret entitled to protection, and that the recruiter was using that customer information in her ongoing contacts with the company's customers. The employee won the case by showing the court that all of the information contained in the employer's customer list could be easily recreated by simple internet searches, particularly LinkedIn, as well as through use of phonebooks, trade publications and through a firm's own media advertising. Of particular importance was the ease with which she could locate the proper decision maker in a company through a LinkedIn search.

The New York case is helpful for employers, in that it provides a list of things NOT to do if you want to protect trade secrets, such as customer lists and related information. Things NOT to do include:

1. FAIL to require employees to sign confidentiality or non-solicitation agreements
2. FAIL to take reasonable steps such as password protection, to protect your database
3. FAIL to designate confidential information in your

database as confidential

4. SHARE your database with potential business partners without restriction
5. FAIL to install firewalls or security software

A related issue is whether an employee under a non-compete/non-solicitation agreement who resigns to join a competitor can immediately change his LinkedIn profile to reflect that new employment. This update is broadcast to all of the employee's contacts on LinkedIn, which likely includes many customers and clients of the former employer. From the employer's perspective, the employee is in violation because he has notified all of the employer's customers of his new employment through his updated profile. From the employee's perspective, he did not affirmatively initiate contacts with any former customers, he merely updated his profile. Each state



will view the non-compete / non-solicitation agreement differently, and there are likely to be a variety of different outcomes in cases

challenging contacts through LinkedIn updates. Employers can, however, take steps to sway this debate in their favor. These steps include:

1. draft non-solicitation agreements that specifically prohibit an employee from notifying clients of their change in employment, even through social networking websites
2. draft confidentiality agreements that clearly define confidential information to include client identities and contact information, and bars the employee from using this information, even through social media
3. include a social media paragraph that specifically addresses social media and other internet usage issues related to the employment.

It is not impossible to protect your customer lists and other trade secret information, but in this information age, it is becoming ever more difficult. An employer must take clear and deliberate steps to indicate to employees what is confidential, then to protect that confidential information from being widely disseminated, particularly through social media. It is best to have an employment law practitioner draft and/or assist you with your agreements to make sure they comprehensively address these issues. ♦

Employee's praise for Employer = Misleading advertising???

FTC updates guidelines on online endorsements

by Mark Hudson mph@shuttleworthlaw.com

Over the past year, the Federal Trade Commission (FTC) has updated and clarified its position on online endorsements. With the age of blogs, online polls, and customer reviews, the FTC has published guidance for companies on how to keep their endorsement and testimonial ads in line with the FTC Act. While this guidance is not new, the recent enforcement should cause pause amongst companies that encourage (actively or passively) employees to write about the great products or services the company provides.

What do the guidelines require?

The FTC enforcement guidelines require employees to disclose their relationships with their employers any time they post a positive review or comment about their employer's products or services. The guidelines apply not only to employees but also to any individual who receives compensation for the positive comments. Accordingly, if an employee posts on Facebook that this company sells the best coffee in Cedar Rapids, the employee has to disclose that he or she works for that company.

How serious is the FTC about enforcement?

Since the release of the updated guidelines, multiple employers have received enforcement letters. For

example, in August of 2010, Reverb Communications received such a letter. Reverb is a company that provides public relations, marketing and sales services to developers of video game applications. Over a nine month period, the company posted reviews about their client's games using account names that gave the reader the impression that the reviews were written by disinterested consumers. Importantly, these posters/bloggers did not disclose that they were hired to promote the games. The FTC will continue using enforcement letters to promote truth in advertising as it defines.

What are the employer lessons?

Every employer wants its employees to share the wonderful products or services of their employment. All businesses want employees to spread the word about greatness of its business or product. However, employers need to be aware of the FTC guidelines and make sure employees are also aware of what they can and cannot say. Employees are free to make great comments about their employer, but they need to disclose that that is their employer as well. In the end, the behavior of employees for the benefit or detriment will continue to be an issue that all workplaces will face. Hence, it is vital to get ahead of such activity before you open a letter from the FTC detailing what it calls deceptive advertising. ♦

Do guns and workplaces mix?

by Mark Hudson mph@shuttleworthlaw.com

With violence in the news, employers are now faced with the tough decision about how to (or whether to) restrict firearms in the workplace. On January 1, 2011, Iowa's new law (S.F. 2379) on concealed weapon permits went into effect. S.F. 2379 shifted Iowa from a "may issue" to a "shall issue" state. Meaning, law enforcement will have less discretion when issuing concealed weapons permits.

Does the new law address employers?

No. The topic of firearm restrictions on private property and in the workplace was not addressed in the new law. However, Iowa's Department of Public Safety stated publically that it believes that private property owners can establish conditions for the presence of guests. Moreover, in 2003, the Iowa Attorney General issued an opinion that cities had the right to enforce weapons bans in spite of the concealed weapons laws. While we are in different time

and under a new law, such an opinion is persuasive support that employer restrictions are permitted.

What should employers do?

Employers should consider whether restricting firearms and other weapons is an appropriate step for their business. If so, consider the scope of such restrictions. For example, can employees leave a weapon in a locked car or locker? As the employer, these decisions must be considered and addressed to insure clarity in the policy. Like all policies, there is no one size fits all weapons policies. Consider the culture of the workplace and make sure it makes sense for the business. In the end, while the law did not address employer's rights to restrict firearms, the passage of the law presents an opportunity for employers to review, consider, and reinforce such policies. ♦



Notable Dates



January 31

*2011 Tax Withholding
Tables Implementation
Deadline*



January 31

*IRS Deadline
for
Distributing W-2s*



February 1

*First Day of
OSHA 300A
Posting Period*



February 22

*Comment Deadline
for Proposed NLRA
Rights Poster*



Upcoming Speaking Engagements



February 22

A Whirlwind Tour of the Ever-Changing World of Workplace Law

19th Annual SHRM State Legal & Legislative Conference
Presented by Central Iowa SHRM and The Iowa State SHRM Council
Keynote by Mark P.A. Hudson



April 8

HIPAA, Electronic Records & Privacy

University of Iowa Heartland Center's 13th Annual
Occupational Health Symposium
Presented by Mark P.A. Hudson and Diane Kutzko



May 17

Employment Law Update

Presented by Benefit Solutions, Inc.
Speakers: Shuttleworth & Ingersoll Employment
Section Attorneys

**SHUTTLEWORTH
& INGERSOLL, P.L.C.**
ATTORNEYS AT LAW
ESTABLISHED 1854

EMPLOYMENT LAW OR RELATED SERVICES

Terri C. Davis
Practice Chair
Phone: 319-731-2362
Email:
tcd@shuttleworthlaw.com

Attorneys in this Area:

John M. Bickel
Cynthia M. Boyle
Terri C. Davis
Dean R. Einck
Richard C. Garberson
Tricia Hoffman-Simanek
Mark P.A. Hudson
Donald L. Johnson
Douglas R. Oelschlaeger
Gary J. Streit
Jason R. Sytsma
Mark L. Zaiger

Employment Law Update
is intended for
distribution to our clients
and to others who have
asked to be on our
distribution list. If you
wish to be removed from
the distribution list,
please notify:

tcd@shuttleworthlaw.com

*The contents of this update are
intended for general
informational purposes only
and should not be construed as
legal advice. Readers are urged
not to act upon the
information contained in this
publication without first
consulting an attorney.*