Social Networking, Website Accessibility, Cyber Liability, and Wage and Hour Issues

Thomas L. McCally, Esq.
Equity Member, Carr Maloney PC
2020 K Street, NW, Suite 850, Washington, DC 20006
(202) 310-5506  ▪  TLM@carrmaloney.com

Copyright © 2015 by Carr Maloney P.C. All rights reserved. No portion of this publication may be reproduced without prior written permission. This publication and program are intended to provide current and accurate information about the subject matter covered. This publication as well as orally conveyed information should not be construed as legal advice.
Today’s Agenda

• Social Networking – Refresher and Update
• Website Accessibility Requirements under ADA – It’s Coming. Get Ready.
• Cyber Liability – An Ever Changing World
• Wage and Hour – Be Careful with Bonuses
Social Networking

• “Social networking” means communicating with others over the Internet for social, professional, or other purposes on sites such as Facebook, Twitter, LinkedIn, Instagram and YouTube.

• It also includes participation on media or news sites which permit readers to post comments. Social networking also includes authoring or posting to blogs and almost all forms of electronic communication, even those not thought of yet!
Social Networking

- Employee use of Social Networking sites poses many issues and potential risks:
  - Harassment, discrimination, defamation, retaliation claims
  - Breach of confidentiality
  - Inadvertent creation of attorney client relationships
  - Waiver of Attorney/Client privilege
  - Trademark/Copyright infringement
  -Disclosure of Attorney-Client privileged information
Social Networking

• Retaliation Example:
  • Employees of the Coyote Ugly bar sued for alleged violations of the wage and hour provisions of the Fair Labor Standards Act, and the court held that the reactions by management on Facebook were sufficient to state claims for retaliation. *Stewart v. CUS Nashville* (M.D. Tenn. Feb. 6, 2013)
Social Networking Policies

• Employers can minimize risks by implementing Social Networking Policies that apply on and off the job
  • Clarify use at work – best practice is to limit use to work related while at work
  • Specify that use of social media on employer network, even if strictly personal, is governed by all employment policies
    • Discrimination and harassment prohibited
    • Protect Confidential and Proprietary Information
    • Protect Attorney/Client privilege
    • No right to privacy if accessed on Employer network – discoverable
Social Networking Policies – Best Practices

• Clarify that employees are not authorized to speak on behalf of the Employer on personal networking sites.

• If using employer network, require employees to obtain approval prior to publishing or commenting on a matter in their capacity as a firm employee, or to include disclaimers making it clear that the employee is expressing views that are personal and not those of the employer.

• Require Compliance with Trademark and Copyright Laws.
Social Networking Policies – Best Practices

• Clarify policy on ownership of client contact information. (Example, LinkedIn).

• Many networking sites ask users to import contact information *en masse* from their contact lists, and some sites attempt to do so surreptitiously. To protect client and company confidential information, do not allow employees to export or upload any client contact information, or to export or upload any contact information obtained from employer’s contacts database, address book, or other source maintained by the company.

• Require employees to report violations of the employer’s Social Networking policy.
Social Networking Policies – Best Practices

- Avoid blanket prohibitions about discussing confidential company information. (i.e. terms and conditions of employment)
  - NLRA - Employees cannot be prohibited from discussing working conditions/terms and conditions of employment. This is protected as “concerted activity” under NLRA.
Social Networking Policies – Best Practices

• Prior to disciplining an employee for making a statement on social media, make sure the statement could not be considered “protected concerted activity” – no matter how offensive. *Pier Sixty, LLC, 362 NLRB 59 (March 31, 2015)*

  • Employee posted on Facebook that his supervisor “is such a NASTY MOTHER F—ER don’t know how to talk to people!!!!!! F—k his mother and his entire f—ing family!!!! What a LOSER!!!! Vote YES for the UNION!!!!!!!”

  • NLRB held that the post was protected concerted activity, and that termination of the employee violated the NLRA.
Web Accessibility and the ADA

Get Ready, Its Coming!

• This act and its amendments guarantee equal opportunity for persons with disabilities in employment, state and local government services, public accommodations, commercial facilities, and transportation.

• Both public and private entities are affected by the ADA.
Overview of the ADA

• Disabilities covered under the ADA include:
  • Physical disabilities (for example, inability to ambulate, restrictions on lifting)
  • Sensory (for example, blindness, deafness)
  • Cognitive (for example, dyslexia, traumatic brain injury, attention deficit disorder)
• Later amendments make it clear that disability is to be broadly defined and include psychological, emotional, physiological and temporary conditions.
Overview of the ADA

• The Americans with Disabilities Act consists of five sections overseeing different aspects of life and an individual’s engagement with society:
  
  • **Title I:** Employment
  • **Title II:** Public Entities
  • **Title III:** Public Accommodations
  • **Title IV:** Telecommunications
  • **Title V:** Miscellaneous Provisions
Provisions of Title III

- General rule of Title III of the ADA is that “[n]o individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation.” 42 U.S.C. § 12182.

- Title III applies to all places of public accommodation, regardless of size. It applies to small start-up companies as well as to big retail chains.
Provisions of Title III

- 42 U.S.C. § 12181(7) lists a number of physical places, such as an inn, hotel, restaurant, bar, movie theater, grocery store, shopping center, museum, library, park, zoo, gymnasium, etc., that would be subject to the ADA.
Provisions of Title III

• The ADA was originally enacted in 1990, at a time that the internet was not widely used by businesses.
  • Accordingly, the ADA does not specifically identify a “website” as being a place of public accommodation subject to the ADA.
• Most of the public accommodations listed are “brick and mortar” businesses with an actual physical location that is open to the public.
Provisions of Title III

- The internet has drastically changed the way business is conducted, and questions regarding the ADA’s application to internet activity are becoming increasingly more common.
Provisions of Title III

• Organizations and associations that provide support to those with disabilities, such as the National Association for the Blind and the National Association for the Deaf, are increasing efforts to ensure that the disabled are provided equal access to goods and services provided over the internet and on “websites”.
Web Content Accessibility Guidelines (WCAG)
http://www.w3.org/WAI/intro/wcag

- Web Content Accessibility Guidelines (WCAG) are developed through the W3C process in cooperation with individuals and organizations around the world, with a goal to provide a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.

- The WCAG documents explain how to make web content more accessible to people with disabilities.

- Web “content” generally refers to the information in a web page or web application, including:
  - Natural information such as text, images, and sounds
  - Code or markup that defines structure, presentation, etc.
Does Title III Apply to Websites?  
The Department of Justice’s Perspective

• In September of 2010, the Department of Justice (DOJ) announced in an Advanced Notice of Proposed Rulemaking (ANPRM) that it would issue new regulations under Title III of the ADA to address the accessibility of businesses.

• The DOJ made a number of statements that reasonably led businesses to conclude that their websites did not necessarily have to be accessible as long as the business offered an equivalent alternative way to access the goods and services that were provided on the website.
Does Title III Apply to Websites?

The Department of Justice’s Perspective

• The DOJ’s statements also led businesses to believe that once DOJ issues a final regulation, they would have time to make their websites comply with the technical accessibility standards in the final DOJ Regulations.
Does Title III Apply to Websites?  
*The Department of Justice’s Perspective*

- Unfortunately, many Courts have disagreed – and in 2015 the DOJ reversed its position when it filed “Statements of Interest” in two lawsuits brought by the National Association for the Deaf (NAD) against two major private universities. In its briefs, the DOJ stated that the obligation to make websites accessible exists right now, even in the absence of any new regulations.
Does Title III Apply to Websites?

The Department of Justice’s Perspective

• The DOJ also stated: “[T]he scope and timing of any final rule on web accessibility is speculative and far from imminent; although the title III proposed rule. . . is currently scheduled for a Spring 2016 publication, there is no scheduled date for publication of a final rule.”

• Still no “Final Regulations” from DOJ
Does Title III Apply to Websites?
The Department of Justice’s Perspective

• Based upon the DOJ’s statement, it appears as if it could be years before we see any final regulations on website accessibility:
  • The DOJ continues to participate in efforts to force businesses to make their websites accessible to the disabled.
  • It does so by filing amicus briefs in litigation between private parties, and by threatening enforcement actions.

Does Title III Apply to Websites?

The Department of Justice’s Perspective

- DOJ Web Accessibility Related Litigation and Settlements
  - Harvard
  - MIT
  - CVS
  - Red Roof Inn
  - Toys “R” Us
  - Reebok
  - Bank of America
  - Carnival Cruise Line
  - NBA
Does Title III Apply to Websites?

The Department of Justice’s Perspective

- The question will most likely be subject to court interpretation for many years, leading to inconsistent results and making it difficult for businesses to know whether the ADA applies to their website, and if so, how to ensure compliance.
Does Title III Apply to Websites?

**The Court’s Perspective**

- Even though websites are not included in the definition of “public accommodation,” courts in different jurisdictions are split as to whether websites are covered by the ADA.

- Some courts have held that the ADA does not apply to websites, especially when there is not sufficient connection between the virtual discrimination alleged and a physical place (or have held that Title III only applies to physical brick-and-mortar places only).
Does Title III Apply to Websites?

The Court’s Perspective

• The majority of recent courts show a growing trend of finding that websites are places of public accommodation subject to the ADA, particularly when they are associated with a physical place of public accommodation. (e.g., Toys “R” Us and CVS)
• Law firms with offices in different states may be subject to conflicting case law on website accessibility.
What does this all mean?

• There is a growing trend towards finding that the ADA applies to website locations that are related to a physical place of public accommodation. Courts have almost consistently held that traditional brick-and-mortar stores must make their websites accessible.

• This same argument likely applies to law firms.
Remedies Available to Plaintiffs

- Injunctive relief
- Attorneys fees and costs of suit (possibly including expert fees)
- Damages
- Penalties that increase with the second violation
- No punitive damages
Defenses

• Undue burden - means significant difficulty or expense. 28 C.F.R. §36.303(a).

• According to 28 C.F.R. §36.104, in determining whether an action would result in an undue burden, factors to be considered include:
  • The nature and cost of the action;
  • The overall financial resources of the company involved in the action;
  • Other factors such as financial condition of parent corporations, if any.

• Difficult standard to meet for employers.
What does this all mean?

• To achieve website accessibility, old platforms may need to be fixed, or it may be more cost effective to implement new software.
Other Factors to Consider

- Using inclusive design practices for your website will make it less likely that you will be a target of ADA lawsuits.
- Using inclusive design practices will protect brand image, not only by avoiding litigation, but also by appearing cutting edge.
- Using inclusive design practices may lead to an increased customer base and growth of business.
- Avoidance of litigation and decreased exposure to cost of defense and possible liability.

DON’T BE THE POSTER CHILD FOR ENFORCEMENT!!
Examples of Corrective Action Required from DOJ Enforcement Actions and Current Case Law

• Include an audio description and transcript for blind users or ensure that the blind can convert text to audio.
• Use a media player that has keyboard-operable controls to accommodate people who cannot use a mouse.
• Provide captioning and/or transcripts for all videos.
• Use alt-tags (alternative attributes) and title tags to label all of your images and videos. Screen readers will interpret these for the visually impaired and learning disabled.
• Don’t use “click here”. Always have your links make contextual sense.
Examples of Corrective Action Required from DOJ Enforcement Actions and Current Case Law

• If your graphics contain any important information, make sure you also provide that information in text form.
• Don’t rely on rollovers to deliver important information.
• Avoid using cascading menus whenever possible. These are difficult and sometimes impossible for adaptive technology to interpret.
• Minimize the need for scrolling. For people with repetitive stress injuries or physical disabilities, excessive scrolling can be very difficult.
Examples of Corrective Action Required from DOJ Enforcement Actions and Current Case Law

• When creating forms, make sure that the text label for the field is very close to the actual field.
• If you have tables on your Web site, be sure to identify row and column headers.
• Use a strong color contrast between your text and background.
• Provide redundant information about color. If you’re selling a brown shirt, don’t rely on the picture. Label the image as brown. About 8 percent of men suffer from red-green colorblindness, so don’t use red alone to denote important information.
Cyber Liability
An Ever Changing World
Data Breach Statistics

- Data breach incidents have been increasing significantly in recent years.
- According to a recent data breach study conducted by Experian, half of all of the organizations surveyed experienced at least one data breach incident in the past 12 months.

Data Breach Statistics

• The number of U.S. data breaches tracked hit a record high of 783 in 2014.
• This represents a 27.5 percent increase over the number of breaches reported in 2013 and a significant increase of 18.3 percent over the previous high of 662 breaches tracked in 2010.
• 2015 U.S. data breaches tracked totaled 781.
  • Identity Theft Resource Center Breach Report, January 12, 2015 and January 25, 2016, Identify Theft Resource Center:

Common Causes of Data Breach Incidents

• Hacking
• Employee Mistake; e.g. loss of a laptop or handheld device that contains confidential information
• Disgruntled employee intentionally disclosing confidential information
Data Breach Incidents Impact Businesses of all Sizes

- While the high profile cases (i.e. Target, Sony) get a lot of media attention, data breach incidents can impact businesses of all sizes.
- The results of these types of incidents can be catastrophic, particularly for a small business.
- This is why the demand for cyber liability insurance has increased significantly in recent years.
Cyber Liability Insurance

• Check your policies to understand what is and what is not covered.

• The policies vary, but typically cyber liability insurance policies will provide coverage for both first and third party claims.
First Party Claims

• First party claims will typically include direct costs incurred by a business in the event that there is a data breach of their computer networks, including attorneys’ fees and costs of a computer forensic vendor.

• Example:
  • A large retailer learns that its server has been hacked and thousands of credit card numbers have been compromised.
  • The policy would cover the costs that the business has to incur bringing in a computer forensic vendor to stop the breach and to determine the extent of the breach.
First Party Claims

• Example:
  
  • The policy may also cover the costs of an attorney to advise the company of reporting obligations as a result of this incident.
  
  • The policy may also provide business interruption coverage, or coverage for the costs associated with restoring or replacing computer systems that have been compromised.
Attorney Involvement with Data Breaches

• It is often necessary to bring in an attorney prior to litigation to respond to a data breach incident.
  • It is typically fairly complicated to determine what obligations a business might have to report a data breach incident depending on the circumstances and states the firm is doing business in.
  • Protecting the attorney-client privilege with respect to communications concerning the data breach in the event.
Third Party Claims

• There are two main types of third party claims that cyber insurance policies typically cover:
  • Claims brought by third parties whose sensitive information was compromised as a result of a data breach;
  • Claims brought by third parties arising out of content contained on the website of a business (i.e. defamation, copyright/trademark infringement).
Third Party Claims

- There are a number of different claims that can be asserted against a business for failing to safeguard confidential data:
  - Statutory claims for violation of various privacy statutes
  - Negligence claims for failure to prevent breaches/failure to adequately safeguard sensitive information
  - Other common law claims (i.e. breach of contract; breach of covenant of good faith and fair dealing)
No Uniform Federal Laws

- There is currently no comprehensive federal law to govern the obligations of businesses to prevent and respond to data breaches.
- In light of some of the more recent high profile breaches, such as breaches at Target and Home Depot, there has been increasing talk in Congress of passing this type of legislation - but it has not been passed to date.
No Uniform Federal Laws

• What businesses are left with is a patchwork of state laws and industry specific requirements that can vary significantly.
• 47 States and the District of Columbia have adopted their own data breach notification laws.
District of Columbia Law

- In the District of Columbia, any business that experiences a data breach must notify affected D.C. residents as soon as possible in writing or, if authorized, by email.

- If the security breach affects more than 100,000 people, or the cost of notification exceeds $50,000.00, businesses can issue alerts via public service announcements.

- If an event affects more than 1,000 people, all consumer-reporting agencies must also be notified.

  - D.C. Code Ann. § 28-3851 (West)
District of Columbia Law

- **Definition of Protected Information**
  - Combination of:
    - Name or other identifying info, PLUS
    - One or more of these "data" elements:
      - SN;
      - Driver's license number;
      - Credit card number or debit card number;
      - Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password that allows access to or use of an individual's financial or credit account.
Who is Subject to Law?

• Any person or business conducting business in DC who licenses or owns computerized or other electronic data that includes personal information – required to provide notice to consumer of any breach of security.

• Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own – required to notify the owner or licensee of the information of any breach of the security.
**Remedies**

- **Regulatory Action**
  - Injunctive relief, fines up to $100/person, plus costs and attorney fees.

- **Private Cause of Action**
  - Actual damages, costs and attorney fees. Dignitary damages, including pain and suffering, are not recoverable.
    - D.C. Code Ann. § 28-3853 (West)
Litigation Trends

• To date, the majority of reported cases involving data breach incidents have been dismissed at an early stage because of the Plaintiffs’ inability to establish that Article III standing = Damages.
To bring a case in federal court, a plaintiff has to establish that they have actually suffered some type of injury caused by the defendant’s conduct.

Consumers who have had personal information exposed as a result of a data breach have difficulty meeting this threshold.
What it Means for Law Firms

• This is a Rapidly Changing Legal Environment.
• Law firms are generally seen as a soft target for data breach incidents.
• Banks and hospitals have been subject to regulations for years that put specific obligations on them to safeguard personal data.
• Law Firms representing banks and hospitals may have access to some of the same types of information, but don’t have the same safeguards in place.
• Check your insurance policies to understand the coverage.
Ethical Issues

• The loss or inadvertent disclosure of confidential data can result in ethical issues unique to attorneys.

• Example:
  • An attorney loses a laptop that contained confidential client information.
  • If the laptop was not password protected, it could implicate Rule 1.1 - Competence or Rule 1.6 - Confidentiality of Information.
Ethical Issues

• The ABA recently amended the comment section of the Model Rule of Professional Responsibility dealing with competence to specifically require attorneys to have knowledge of “the benefits and risks associated with relevant technology.”
Wage and Hour: Be Careful with Bonuses

• Effective December 1, 2016, the minimum wage requirement to qualify as an exempt employee under the FLSA will significantly increase.

• Standard salary level will increase from $455 to $913 per week ($47,476.00 annually for a full-year worker).

• Many employees who meet the current criteria and are currently exempt may not qualify after December 1, 2016 – and may become eligible for overtime pay.

• Accordingly, it is more important than ever to review compensation policies to ensure that employers accurately calculate an employee’s regular rate of pay for purposes of calculating overtime.
Wages and Overtime

• A recent Federal case in Wisconsin (*Gilbertson v. City of Sheboygan*) may dramatically impact the manner in which employers calculate an employee’s regular rate of pay for overtime purposes.
Discretionary and Non-Discretionary Bonuses

• Under the Fair Labor Standards Act, discretionary bonuses are not considered overtime-eligible, as defined in 29 CFR 778.208-215, and are therefore not required to be included in the employee’s regular wage rates when calculating overtime.

• Non-Discretionary bonuses are required to be included in an employee’s regular rate of pay for purposes of calculating overtime.
When is a Discretionary Bonus not Discretionary?

To be considered a discretionary bonus, all four of the following criteria must apply:

1. The employer retains discretion whether bonus will be paid.
2. The employer retains discretion on the amount of the bonus.
3. The employer retains discretion about whether a bonus will be provided very near the time frame it covers.
4. The bonus must not be paid pursuant to any prior contract, agreement, or promise.
When is a Discretionary Bonus not Discretionary?

• In *Gilbertson v. City of Sheboygan*, the City awarded employees bonuses that it described as “discretionary,” but which were awarded to employees who met certain objective criteria.

• The court ruled that under existing case law and the FLSA, bonuses that are based on objective criteria must be included in the regular wage rate.
When is a Discretionary Bonus not Discretionary?

- The City also offered employees a Health Reimbursement Arrangement (HRA) under which the City reimbursed employees for uninsured medical expenses. Under the unique facts present in that case, the Court ruled that the reimbursement payments to employees must also be included in the employee's regular wage rate for purposes of computing the employee's overtime wage rate.
- The decision may be appealed, and it is unclear whether other jurisdictions will follow the holding, particularly with respect to HRA reimbursements.
What to Take Away

• Make sure that any discretionary bonus is truly discretionary and not based on purely objective criteria.
• Do not promise any employee a “discretionary” bonus.
• If an employee would expect or be entitled to the bonus under specified circumstances, it may not be treated as discretionary.
• It is important to review all compensation plans and health care reimbursement plans to make sure they are structured in a manner that will allow payments to be excluded from employee’s regular rate of pay.