Employees, Smart Phones and Social Media: Best Practices for Mobile Computing and Social Media Policies

John J. Heitmann, CIPP, Partner, Kelley Drye & Warren LLP
Introduction and Session Roadmap

CATBERT: EVIL DIRECTOR OF HUMAN RESOURCES

100% OF YOUR EMAIL MESSAGES THIS MONTH INVOLVED LINKS TO FUNNY VIDEOS.

THE COMPANY IS VIOLATING MY RIGHT TO PRIVACY! THIS IS AN OUTRAGE!

ACTUALLY, I WAS JUST GUESSING.

IT STILL HURTS.
Introduction and Session Roadmap

• Mobile computing and social media in the workplace
  ➢ Trends and technology
  ➢ The (US) legal landscape
  ➢ Translating trends, technology and the legal landscape into Mobile Computing and Social Media Policy best practices
Mobile Computing and Social Media in the Workplace

Trends and Technology
Trends and Technology: Mobile Computing

• US businesses and consumers are embracing mobile technologies

• More mobile phone users (US)
  ➢ 83% of adults have mobile phones¹
    – 322.9 million wireless connections as of June 2011²
    – 29.7% of households have “cut-the-cord”³
Trends and Technology: Mobile Computing

• More “smart” mobile devices (US)
  ➢ As of June 2011 – U.S. consumers owned more than 275 million data-capable devices$^4$, including:
    – 95.8 million smart phones or wireless PDAs
    – 15.2 million wireless-enabled laptops, notebooks, tablets and wireless broadband modems
  ➢ As of October 2011 - 11% of adults own tablet computers (US)$^5$
    – 77% use the tablet daily
    – Users spend an average of 90 minutes
Trends and Technology: Mobile Computing

• More uses for mobile phones (US)
  ➢ Voice
    – Most popular use:
      1.15 trillion MOUs
      (January-June 2011)$^6$
  ➢ Texts
    – More than 2 trillion text messages
      over 6 billion per day sent (January-June 2011)$^7$
Trends and Technology: Mobile Computing

• More uses for mobile phones (US)
  
  ➢ Apps
    – 50% of U.S. adults have cell phones with apps
    – 68% use apps
    – 46% paid to download an app to their phone
  
  ➢ Location-Based Services ("LBS")
    – Nearly 6000 “location aware” apps for the iPhone, 900 for Android and 300 for Blackberry
    – Only 1 in 4 U.S. adults have used LBS
    – Less than 10% of U.S. adults use automatic location-tagging in their social media, i.e., Facebook, Twitter and LinkedIn
Trends and Technology: Social Media

• Facebook
  - More than 800 million active users
    - More than 50% of active users log onto Facebook each day
    - Users can interact with more than 900M objects (pages, groups, events and community pages)
    - More than 7M apps and websites are integrated with Facebook
    - More than 350M active users currently access Facebook on mobile devices
    - More than 50% of the Global 100 have a Facebook page
Trends and Technology: Social Media

• LinkedIn\textsuperscript{13}
  
  - More than 135 million members in over 200 countries
  
  - More than 2 million companies have LinkedIn pages
  
  - 75 of Fortune 100 companies use LinkedIn’s corporate hiring solutions
  
  - 100K+ job applications submitted using Apply With LinkedIn
Trends and Technology: Social Media

• **Twitter**
  - More than 100M active users
  - 250M tweets sent each day
  - Average of 460,000 new accounts created each day
  - 182% increase in mobile users over the past year
Trends and Technology: Social Media

- foursquare
  - Approximately 15M users
  - Over 1.5 Billion user “check-ins”
  - But LBS use is limited:
    - Only 5% of U.S. adults use LBS at least once per month
    - Typical use is for location-based directions, i.e., GPS
    - Majority (at least 55%) of users are concerned about loss of privacy
Trends and Technology: Social Media

• Business use of Social Media is growing\textsuperscript{19}
  ➢ Over 75% use for business purposes
  ➢ Almost 30% block employee access
  ➢ Almost 25% monitor the use at work
  ➢ 55% have social media policies; 44% cover use at work and outside of work

• A recent survey\textsuperscript{20} shows
  ➢ 90% of recruiters and hiring managers review potential candidates’ profiles
  ➢ almost 70% make hiring decisions based on social networking profiles
Trends and Technology: Mobile and Social Media in the News

Making news ... good and bad

➢ Mobile tracking
➢ Mobile device data breaches
➢ Wireless network security
➢ “Facebook Privacy”
  ➢ Too many headlines, too little time
➢ Too Linked-In?
  ➢ “Social ads” -> endorsements
➢ Be careful what you Tweet
What’s All This Fuss About?

• Privacy

➢ “Privacy Gaps” can exist between employer and employee privacy and control expectations when using mobile devices and social networks\(^{21}\)

  – Usage model variants
    ▪ Mobile
    ▪ Social
  – Employee expectations
  – Company expectations
What’s All This Fuss About?

• Security

- Increased use of personal mobile devices to access business systems or hold business information leads to increased risks of data breaches
  - 419 publicly-disclosed breaches in 2011
  - 18% of breaches caused by loss of mobile data devices
  - 17% of breaches involved hack attacks against businesses
  - Growing problem of malicious software and “tainted” apps that can result in stolen information from mobile devices
What Could Go Wrong?

• Damage to employer/employee relations
• Damage to business
• Damage to “brand”
• Breach disclosure requirements
• Investigations
• Enforcement
• Litigation
Mobile Computing and Social Media in the Workplace

The Legal Landscape
Legal Landscape: Employer Monitoring vs. Employee Privacy

• Monitoring employee communications
  - Federal law
  - State law
  - Case law

• Other considerations
  - Sector-specific privacy and security laws
  - Labor and employment law
  - International law (especially for multi-nationals)
  - Intellectual property law
Legal Landscape: US Electronic Communications Laws

• Federal electronic privacy law

• Electronic Communications Privacy Act (ECPA)
  ➢ Passed in 1986 to amend the Wiretap Act to cover all electronic communications, not simply wire transmissions
    ➢ Electronic communication in transit (Title I—provisions drawn from Wiretap Act)
    ➢ Communications in storage (Title II—Stored Communications Act)
    ➢ Pen register/trap and trace devices that record dialing, routing, addressing, and signaling information used in the process of transmitting wire or electronic communications without a search warrant (Title III)
  ➢ Protections and requirements for communications in transit and in storage differ
  ➢ Exceptions include single party consent, ordinary course of business, and provider authorization (using of equipment provided by the communications provider)
Legal Landscape: US Electronic Communications Laws

• State electronic privacy laws
  ➢ Most states have wiretap or electronic privacy laws that restrict the interception of wire and/or electronic communications
    – Restrictions similar to federal law
    – Many states require two-party consent to intercept an electronic communication
  ➢ States with two-party consent (or all party consent) requirements are not satisfied by simply obtaining the consent of the employee
    – Conflicting court decisions
Legal Landscape: Monitoring Phone Calls

• Case Law

➤ Monitoring of personal calls without the consent of the employee over employer phone lines violates ECPA\(^26\)

➤ Monitoring must cease when it becomes apparent that the call is personal – unless the employee consented\(^27\)
Legal Landscape: Monitoring Phone Calls

- Consent is implied when employees are informed that phone conversations will be monitored, but not when informed that their conversations might be monitored.

- Exemption applies if the equipment used to intercept the employee’s calls is provided by the phone company and not the employer.
Legal Landscape: Monitoring Phone Calls

• Best Practices for Monitoring Phone Calls

  Employers who monitor calls should:

  – Prohibit undisclosed monitoring or recording of calls with residents of states that require all parties to a conversation to consent

  – Ensure that the monitoring is for a legitimate business purpose

  – Immediately stop monitoring a call as soon as it is determined that the call is for personal use
Legal Landscape: Monitoring Email, Internet, Computer and Mobile Device Usage

- Employers generally can monitor employee emails and computer usage.
- Employees generally do not have reasonable expectation of privacy when using employer’s computer system\(^{30}\).
- Employers generally exempt under ECPA as providers of an electronic communications service\(^{31}\).
Legal Landscape: Monitoring Email, Internet, Computer and Mobile Device Usage

- Employers can adopt lawful computer usage policies to protect assets, reputation and productivity of business\(^\text{32}\)
  - Policies bolstered with employee notice and consent
- Monitoring can extend to employer-issued equipment such as home computers\(^\text{33}\)
- Employers can search former employee’s company e-mails on company-issued laptop when investigating employee sharing of proprietary information\(^\text{34}\)
Legal Landscape: Monitoring Email, Internet, Computer and Mobile Device Usage

- Passwords can provide additional protection for employee communication when stored on employer computers\textsuperscript{35}

- May trigger legal obligation to act if employer discovers illegal activity

  - Employer with actual or implied knowledge that employee was using company computer to access child pornography had duty to investigate and stop employee’s activities\textsuperscript{36}
Legal Landscape: Monitoring Email, Internet, Computer and Mobile Device Usage

• Confidentiality of employee attorney-client communications

  ➢ Varies based on company policies

  ➢ Where company policy explicitly prohibits use of company equipment for personal e-mails, employee’s attorney-client correspondence is not confidential\(^{37}\)

  ➢ Employee’s use of company equipment to send attorney-client e-mails using personal e-mail account was confidential because company policy did not address personal e-mail accounts\(^{38}\)
Legal Landscape: Email, Internet, Computer and Mobile Device Usage

• US Supreme Court guidance
  
  ➢ Employer ability to monitor employee texts varies based on company policies
    
    – “employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated”

39
US Supreme Court guidance

- Use of GPS to track an individual constitutes a search or seizure under the Fourth amendment

- Consequently, employer use of GPS devices to track employees could be an unlawful search and seizure
Legal Landscape: Email, Internet, Computer and Mobile Device Usage

- Best practices for monitoring email, Internet, computer and mobile device usage
  - Clearly disclose that monitoring *will* take place, and that any communications on the employer’s system are not private
  - Disclose that the employer will monitor the contents of all Internet communications, including personal email over the company’s computers, including mobile devices
  - Compose technology use policies that are broad enough to include a variety of different technologies – do not draft policies for a specific technology
  - DISCLAIM that policies may be altered by a supervisor’s oral statements
  - Limit monitoring to specific business purposes
  - Regularly provide notice and obtain written consent to such monitoring
Legal Landscape: Monitoring Social Media / Blogging

• Employer can monitor publicly visible employee conduct on social media websites for legitimate business purposes, *i.e.*, protecting confidential information, trademarks, intellectual property, etc.

• Two general guidelines
  - Should be done under lawful means and not under false pretenses
  - Employers should not require access to employees’ private information
Legal Landscape: Monitoring Social Media / Blogging

• ECPA and state laws apply

  ➢ Employer accessing social networking site by pretending to be someone else may violate ECPA and state laws⁴¹
Legal Landscape: Monitoring Social Media / Blogging

- Federal Computer Fraud and Abuse Act (CFAA) makes it a crime to gain “unauthorized access” to a computer
  - An employer that gains access to a social networking site by pretending to be someone else could violate the CFAA by violating the terms of the website
  - *Drew* case illustrates the potentially serious ramifications of misuse of, or misbehavior on, social media (cyberbullying/suicide)⁴²
Legal Landscape: Monitoring Social Media / Blogging

• National Labor Relations Act

- Employees have right to engage in discussions concerning wages, benefits and other terms and conditions of employment

- National Labor Relations Board (NLRB) often files charges against employers that restrict employee discussions or terminate employees based on use of social media for covered purposes
  - NLRB approved a settlement of a complaint against a company for unfair labor practices for firing an employee after she posted negative comments about her supervisor on Facebook[^43]
Legal Landscape: Monitoring Social Media / Blogging

• National Labor Relations Act

- Several recent NLRB advice memorandums upheld terminations based on employee social media comments because employees’ comments did not constitute protected activity\(^4^4\)
  - Employer must guard against giving impression of surveillance:
    - “the employee would reasonably assume from the [employer’s] statement that their [sic] union activities had been placed under surveillance” \(^4^5\)
    - Test met when employer “reveals specific information about protected activity that is not generally known and does not reveal its source.” \(^4^6\)
Legal Landscape: Monitoring Social Media / Blogging

• Best practices for monitoring employee use of social media / blogging

  ➢ Employer technology use policies may not prohibit legal/protected activities of their employees, such as blogging about union activities

  ➢ Employers may access social networking sites such as Facebook and MySpace to monitor employee conduct related to employment

  ➢ Employers may not monitor an employee’s social media activities by entering those websites under false pretenses, or by pretending to be someone else
Legal Landscape: Monitoring Social Media / Blogging

• Employee activity / employer liability: Communications Decency Act (CDA)

➢ Protects online service providers from liability for claims based on content provided by third parties
  – CDA immunity is not unlimited
  – Generally does not cover content posted by employees
  – No immunity where company “materially contributes” to the offensive content posted to the website⁴⁷
Legal Landscape: Monitoring Social Media / Blogging

- Employee activity / employer liability: Digital Millennium Copyright Act (DMCA)

  - Limits service provider liability for copyright infringement when material is posted by a third-party
    - Service provider must have DMCA-compliant notice and takedown procedures
    - Generally does not cover content posted by employees
Legal Landscape: Monitoring Social Media / Blogging

- Employee activity / employer liability: Fair Credit Reporting Act (FCRA)
  - FCRA could place some limitations on an employer’s use of social networking sites in screening and evaluating potential employees
  - Key definitions
    - “consumer report” and “consumer reporting agency”
      - Some Internet sites or services and mobile apps may meet the definitions; most social networking sites do not
  - An employer’s use of social networking sites to screen potential employees is likely not a FCRA violation
Legal Landscape: Monitoring Social Media / Blogging

• Employee activity / employer liability: Tort Actions

- Employer can be held vicariously liable for employee activities on the Internet based on theory of "respondeat superior"\textsuperscript{48}
  - Vicarious liability may extend to both willful and malicious actions, as well as negligence
  - Success of claims depends on whether employee was acting within scope of his employment at the time of the action
  - Note: "Scope" is interpreted broadly
Legal Landscape: Monitoring Social Media / Blogging

• Employee activity / employer liability: FTC Endorsement and Testimonial Guides

➤ Address endorsements and testimonials by consumers, experts, organizations and celebrities

  – Guides govern certain employee behavior on social media, email, mobile apps and other communication methods, creating liability risks for employers

➤ Require disclosure of “material connections” between endorser and company or product

  – An employee that is providing an endorsement or testimonial has a “material connection” to the employer
Legal Landscape: Monitoring Social Media / Blogging

• Employee activity / employer liability: New FTC guidance
  - Employment Background Checks and Credit Reports
    [link](http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre36.shtm)
  - The Fair Credit Reporting Act & Social Media: What Businesses Should Know
    [link](http://business.ftc.gov/blog/2011/06/fair-credit-reporting-act-social-media-what-businesses-should-know)
    - Social Intelligence Corporation letter
Mobile Computing and Social Media in the Workplace

Translating Trends, Technology and the Legal Landscape into Effective Social Media and Mobile Computing Policies
Why Employers Should Have Policies

• A comprehensive company communications policy is the most effective means of protecting an employer’s right to monitor

• Goals:
  ➢ Protect brand
  ➢ Manage risk
  ➢ Notice & consent / legal and regulatory compliance
  ➢ Happy employers and happy employees

• But, if you don’t intend to comply with your policies, you might be worse off for having them...
Mobile and Social Policy Best Practices

• The need for clear policies is driven by a lack of clarity regarding privacy protections applicable to new communications methods

➢ Unresolved: whether the Fourth Amendment protects a person’s right to privacy in emails, Internet searches, etc.

➢ Courts are cautious
  – *Quon* illustrates the US Supreme Court’s disinclination to establish broad precedents as to privacy rights vis-à-vis electronic devices and emerging technologies
Mobile Computing Policy Best Practices

• Assemble the right team
  ➢ IT, legal, HR and relevant business units

• Identify the use(s) of mobile computing in the company’s information technology infrastructure
  ➢ Remote access to company’s network
  ➢ Mobile devices
  ➢ Mobile drives
Mobile Computing Policy Best Practices

• Tailor the Scope of the Policy
  ➢ Address company specific needs
  ➢ Make good choices regarding remote access, mobile devices and mobile drives
  ➢ Consider the data sets available and adopt appropriate controls
Mobile Computing Policy Best Practices

• Approval of Devices and Software

➢ Hardware
  – Minimum requirements?
    ▪ Remote access variables
  – Security settings and solutions?

➢ Software
  – Minimum requirements?
    ▪ Operating system and program requirements
    ▪ Identify supported versions
    ▪ Plan to phase-out older versions
Mobile Computing Policy Best Practices

- **Build-in Security**
  - Remote wipe
    - Assess capability
    - Obtain consent
  - Utilize third-party mobile security services
    - Numerous established and upcoming mobile security vendors

- **Proprietary and Confidential Information**
  - Legal and regulatory requirements
  - Preserving legal protections
  - Preserving competitively sensitive information
  - Encryption and other solutions
Mobile Computing Policy Best Practices

• Technical Security
  ➢ Conform to policies or conform policies
  ➢ Maintain compliance

• Retention and Disposal
  ➢ Hard copy documents
  ➢ Locally-saved copies
Mobile Computing Policy Best Practices

• Review and Revise the Policy on an Ongoing Basis

➤ Assess changes in
  – Employer goals
  – Data types and data uses
  – Employee expectations
  – Technology
  – Risks
  – Laws and regulations
Social Media Policy Best Practices

• New media presents new risks

• Claims may involve

  ➢ Employment and intellectual property law
    – harassment
    – defamation
    – IP infringement (copyright, trademark, trade secret)

  ➢ Technology and media law
    – CAN-SPAM Act
    – TCPA
    – Section 5 of the FTC Act
    – State law

  ➢ General torts under *respondeat superior*
Social Media Policy Best Practices

• Identify the company’s corporate culture and the role of social media in the company’s communication strategy

➢ Options

  – Embrace and Incorporate Social Media
  – Permit Some Professional Use of Social Media
  – Permit Some Personal Use of Social Media
  – Restrict All Use of Social Media
Social Media Policy Best Practices

• Basic determinations to make regarding the company’s social media communications

  ➢ Purpose
    – Define and set appropriate boundaries

  ➢ Audience
    – Segmentation
    – Content guidelines

  ➢ Tone
    – Informal or not, it’s forever
    – Etiquette
Social Media Policy Best Practices

• Consider the risks and plan ahead
  ➢ Traditional laws apply to non-traditional media
    – Monitoring and compliance
  ➢ Consult industry guidelines
    – Instructive or binding?
Social Media Policy Best Practices

• Training
  - Plan a comprehensive program
  - Employee certifications
  - Update and refresh regularly

• Monitoring
  - Provide notice
  - Get written consent

• Build-in CDA and DMCA awareness and protections
  - CDA immunity
  - DMCA limit of liability
Social Media Policy Best Practices

- Not one-size fits all
- Key Provisions
  - Transparency (material connections)
  - Product / service claims
  - Content (original, third party and offensive)
  - Protect company information
  - Protect consumer information
  - Other company policies
  - Social media site rules
  - Responsibility
  - Mistakes
  - Etiquette (be nice; be polite)
  - Reporting suspicious behavior (if something doesn’t feel right)
Key Take-Aways

• Monitoring and mobile computing
  ➢ Assess new mobile computing technologies and uses and their impacts on expectations, obligations and risks
  ➢ Adjust by providing notice and getting consent
  ➢ Set expectations and limits in a written policy

• Monitoring and social media
  ➢ Assess new social media technologies and uses and their impacts on expectations, obligations and risks
  ➢ Adjust by providing notice and getting consent
  ➢ Set expectations and limits in a written policy

2, 3 Wireless Quick Facts, CTIA at http://www.ctia.org/media/industry_info/index.cfm/AID/10323

4  50 Wireless Quick Facts, CTIA at http://www.ctia.org/media/industry_info/index.cfm/AID/10378


6, 7 50 Wireless Quick Facts, CTIA at http://www.ctia.org/media/industry_info/index.cfm/AID/10379

8  Pew Research Center Internet & American Life Project, Half of adult cell phone owners have apps on their phones (Nov. 11, 2011) at http://pewresearch.org/pubs/2123/cellol-phone-apps-mobile-downloads

9, 10, 18 ACLU of Northern California, Location-Based Services: Time for a Privacy Check-In (Nov. 2010) at http://dotrights.org/sites/default/files/lbs-white-paper.pdf
Resources


13 LinkedIn, About Us at http://press.linkedin.com/about

14 Twitter Blog, # Numbers at http://blog.twitter.com/2011/03/numbers.html


15 foursquare, https://foursquare.com/about/

Resources


26 Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992)

27, 28 Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983)

29 Epps v. St. Mary’s Hosp. of Athens, Inc., 802 F.2d 412 (11th Cir. 1986)


31 Ideal Aerosmith, Inc. v. Acutronic USA, Inc., 2007 WL 4394447 (E.D. Pa. 2007)
Resources

32, 35, 38 *Stengart v. Loving Care Agency Inc.*, 990 A.2d 650 (N.J. 2010)


Resources


45 *Flexsteel Industries*, 311 NLRB 257 (1993)

46 *Stevens Creek Chrysler Jeep Dodge*, 353 NLRB 1294 (2009)

47 *Fair Housing Council v Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008)

Statutes

- Communications Decency Act (CDA) 47 U.S.C. § 230
- Digital Millennium Copyright Act (DMCA) 17 U.S.C. § 512
- Electronic Communications Privacy Act (ECPA) 18 U.S.C. §§ 2510 - 2522
- Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681
- Federal Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030
Questions?

John J. Heitmann
PARTNER, KELLEY DRYE & WARREN LLP
Privacy & Information Security
Telecommunications
(202) 342-8544
jheitmann@kelleydrye.com

Connect with Kelley Drye
Web: www.KelleyDrye.com
Twitter: @KelleyDrye

www.privacyassociation.org/summit