Employee Privacy – Or the Lack of It – In the Digital Age

Presented By:
Jackie Ford and Kim Cunningham
for
Association of Corporate Counsel
September 8, 2015
Overview

• Workplace Privacy 101
• Technology and Privacy
  — BYOD Programs
  — Social Media
  — Off-site Work
• Best Practices For Balancing Corporate Needs With Privacy Concerns
"On the Internet, nobody knows you're a dog."
Workplace Privacy: The Basics

• Common Law
  – Reasonable Expectation of Privacy
  – Breach/Violation
  – No Applicable Exemption / Affirmative Defense
    ➢ Example: Waiver
Privacy: Almost Always a Balancing Test

- Some courts weigh not only the expectation of privacy but the reason for the breach.
- Example: Was the breach for a work-related reason - or were you just snooping?
Statutory Privacy Protections in the Workplace

- HIPAA protections for medical info via your health plan
- ADA and FMLA confidentiality provisions regarding medical information
- Federal Wiretap Act – prohibits recording conversation unless at least one party consents
- Stored Communications Act (SCA) - protects information on password-protected accounts / prohibits hacking
When Do Work & Privacy Intersect?

• Traditional Privacy Concerns:
  — Desk/Locker Searches
  — Medical Inquiries
  — Personal relationships and activities

• Technology and Privacy Add Another Layer
  — Telephone monitoring
  — E-mail, Texts, and Web-Based Platforms
Blurred Lines Between Personal and Professional?
... or Just Word Crimes?
Does Off Work Mean Off Limits?

- **Microsoft**: Picture of Apple Macs arriving at MS warehouse posted on worker’s social media page.

- **Harvard University**: Disgruntled office worker made threats on her blog. “I am one shade lighter than homicidal today. I am two snotty e-mails from professors away from bombing the entire Harvard campus.”

- **Starbucks**: Manager’s blog criticized boss for not allowing him to go home sick. Manager had signed a non-disparagement agreement, violated by his blog.
What’s an Employer To Do?

• You learn that one of your employees has a blog in which he discusses his addiction to painkillers.

• A Facebook post from one of your employees accuses his manager of buying and using illegal drugs.

• An employee’s Twitter post hints that your company is developing new experimental technology.
Shifting Regulatory Landscape Meets Rapidly Changing Technology

• BYOD Programs
• Employee Use of Social Media
• Technology Use and Access Away from the Office
Bring Your Own Device (BYOD)

• AKA, BYOD meets OMG
BYOD

• **Employer data issues:** How are your employees handling, storing, and sharing your information stored on their devices?

• **Employee data issues:** To the extent employee data is mixed with Company data, how best to avoid learning what you would rather not know – without giving up rights to your own information?

• **Balancing Act:** How to accomplish both goals without being seen as “Big Brother.”
Privacy and BYOD: An Unhappy Marriage

• Employee uses his own Smartphone to access Company e-mail or software, or to perform other work for the Company.

• Company info ends up stored on phone.

• Employee’s phone is lost or stolen – or the employee resigns or is fired.

• What happens to the Company information?
Can Security Solve the Privacy Problems?

• More security products emerging

• Concept: “Split” a single device into personal and business use

• MDM (Mobile Device Management) and “containerization”
“Containerization” and “Sandboxing”

- Sandboxing is a form of software virtualization (via MDM software) that allows programs to run in an isolated virtual environment on a device.
- MDM software can then manage the sandboxed portion of the device only and encrypt and wipe data inside the sandbox as necessary.
Will What’s In the Sandbox Stay In The Sandbox?

• Two close cousins of BYOD – **BYOA** (Bring Your Own App) and **BYOC** (Bring Your Own Cloud) – make it difficult to employ sandboxing methods to safeguard data.

• **BYOA** includes all of the apps on your employees’ devices.

• **BYOC** means that many smartphones back up data to the cloud automatically, and many apps operate in their own proprietary clouds or interface with multiple clouds at once.

• Inevitably your data is at risk of being comingled in places you don’t control.

• Privilege implications?
“By using Siri or Dictation, you agree and consent to Apple’s and its subsidiaries’ and agents’ transmission, collection, maintenance, processing, and use of this information, including your voice input and User Data, to provide and improve Siri, Dictation, and dictation functionality in other Apple products and services.”
Can You Recover Data from Employee’s Phone?

- Stored Communications Act Issues
- Can Expectation of Privacy be Waived?
BYOD and Litigation Record Holds

• Can you / should you include employees’ personal devices in record holds?
• If you know that employees are using personal devices to discuss / conduct business, can you avoid including them in your record hold?
• Do you have “possession custody or control” of such devices for discovery purposes?
Searching Employee Devices

• Can you require Employees to give you access to their personal devices for purposes of investigation or discovery?

• State law variations?
SCA Overview

- Part of the ECPA, passed in 1986
- Still using 1986 law to determine parameters of technologies invented decades later
SCA Provisions Generally Mean...

• … that if you want disclosure from the service provider, you probably need a subpoena.

• Need consent from the user if you want access to a password-protected account
City of Ontario v. Quon: If It’s Yours Can You Look At It?

• Supreme Court reviewed case from City of Ontario, California.

• City issued pagers to officers to communicate with each other.

• Pagers routinely exceeded monthly allotment.

• City asked system provider (Arch Wireless) to give it transcripts to see content of messages.

• Officer Quon had been sending sexually explicit messages – to two different officers.
Quon (cont’d)

- Supreme Court: Dodged issue of whether Officer Quon had a “reasonable expectation of privacy” in the pager messages.

- Either way – privacy or no privacy – the Court found that the City’s review of the messages was “reasonable” because it was limited to legitimate business purposes.
Quon (cont’d)

• Supreme Court: Don’t read much into our decision.

• “Prudence counsels caution before the facts in this case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations of employees using employer-provided communication devices.”
Quon: - What About the Other Half of the Case?

• Supreme Court did NOT review portion of lower court’s finding that Arch Wireless, the service provider, violated SCA (Stored Communications Act) by providing City with transcripts to the messages.

• Right to those messages lies in USERS not OWNERS.

• Result: Get consent for future access as condition of issuing equipment/access to employees?
Policy Solutions

• As condition of access, Employee gives Company right to swipe and wipe the phone, with or without notice to the Employee.

• No expectation of privacy in ANY of the content of the phone.

• Uncomfortable? Get a second phone for business.
Facebook Firings, Twitter Terminations and Pinterest Pitfalls
Pietrylo v. Hillstone Restaurant Group, d/b/a Houston’s (D.N.J. 2009).

• Restaurant employees set up a gripe site on MySpace to complain about their jobs.
• Site was password protected.
• Hostess mentioned it to Manager.
• Hostess gave Manager the password.
• Manager read posts and fired several employees.
Pietrylo (cont’d)

• Jury: Hostess was “coerced” into giving the password to her Manager.
• Therefore, Manager was not “authorized” to access the site.
• Manager’s access therefore violated Stored Communications Act (SCA).
• Restaurant liable for damages and attorneys’ fees.
• Lesson: It matters how you get it.
NLRB and Social Media Policies and Practices

Per the NLRB’s webpage, major concerns are:

- **Breadth**: “Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.”

- **Griping**: “An employee’s comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.”
The NLRB and Social Media

• Under Section 7 of the NLRA, employees have the right to choose to engage in union activities and in “protected concerted activity” – activity involving two or more employees to effect changes in “terms and conditions of employment.”

• This includes the right to discuss wages, benefits and other terms and conditions of work with other employees.

• “Individual gripe” is not “concerted activity.”
Overbroad Social Media Policy: Example (Triple Play Sports Bar)

• Employer’s policy prohibited “engaging in inappropriate discussions about the company, management, and/or co-workers.”

• The term “inappropriate” was “sufficiently imprecise” to be impermissibly overbroad.
Triple Play Sports Bar: NLRB Likes Facebook Likes

- August 22, 2014 NLRB ruling: Employee “liking” a status on Facebook is engaging in protected concerted activities under the NLRA.
Triple Play Sports Bar (cont’d)

• Employer a non-union bar and restaurant in Connecticut.

• While preparing their tax returns, several employees discovered that they owed money to the State of Connecticut.

• Suspecting a withholding mistake by the bar’s owners, some employees complained.

• Owners organized a staff meeting with the payroll provider to discuss the issue.
Triple Play (cont’d)

• Former employee Jamie posted on Facebook: “They [the employer] can’t even do the tax paperwork correctly!!!! Now I OWE money… Wtf!!!!”

• Co-Worker Vincent “liked” Jamie’s post.

• Another co-worker and a customer both posted supportive comments.

• Jamie added a comment accusing one of the owners of being “shady” and “pocketing” money from employee paychecks, adding “ha ha ha” to the comment.

• Jamie said she might report it to “labor board.”
• Another employee, Jillian, added “I owe too. Such an as*****.”

• Still another co-worker commented that she planned to raise the issue at an upcoming staff meeting.

• Jamie and Vincent both fired; Boss told Vincent it was “apparent” that he wanted to work elsewhere since he “liked the disparaging and defamatory comments.”
Triple Play (cont’d)
Triple Play (cont’d)

• Facebook discussion about allegedly incorrect tax withholdings protected under NLRA – related to terms of employment and intended for employees’ mutual aid and benefit.

• Despite being disloyal and disparaging, comments did not lose NLRA protection – because they did not mention the employer’s products or services.
Triple Play (cont’d)

• Despite the fact that Facebook is at its core a public place – and despite the fact that a customer was among those commenting – the Board found that the conversation was “comparable to a conversation that could potentially be overheard by a patron or other third party.”

• “Not directed to the general public.”

• No “actual malice” in comments by those fired.
Communications were outside the workplace, and were not directly with the employer.

Therefore, question was whether the employees’ speech was so disloyal, reckless or maliciously untrue as to lose protection under the Act.
Lessons from Triple Play Case

• Closely scrutinize any discipline resulting from Facebook or other social media posts

• Negative or disparaging comments may be protected under NLRA

• “Likes” and other minimalist expressions or comments could also be protected

• But also remember that defamation and other policy violations may still support disciplinary action
FLSA Issues: Off-The-Clock Work via Technology

- FLSA requires strict compliance
- Employees increasingly working in “virtual offices”
- If non-exempt employee takes the laptop home and does work using that device – what are the implications?
Rulli v. CB Richard Ellis, Inc. (E.D. Wisconsin)

• Wisconsin maintenance worker claimed he and other nonexempt employees were required to use company-issued BlackBerries after-hours, without compensation, in violation of the FLSA.

• Employees told to respond within 15 minutes.

• Case settled in 2011 (after two years of litigation).
• T-Mobile workers alleged they “were required to review and respond to T-Mobile e-mails and text messages at all hours of the day, whether or not they were punched in to T-Mobile’s computer-based timecard system.”

• Plaintiffs claim Company “requires employees to carry Company-owned cell phones and Blackberries ... and encourages employees to provide this number to customers” for work purposes.

• Settled in 2010.
**Allen v. Chicago:**
The City Never Sleeps

- Sergeant Allen claimed he received numerous telephone calls, e-mails, voice mails, and text message work orders on his Blackberry while off the clock, and was expected to respond to these communications throughout the night and into the early morning hours while off duty.

- City moved to dismiss Allen’s complaint based partially on the theory that any time Allen spent on his PDA off-duty was *de minimis* and did not require compensation under the FLSA.

- Federal District Court denied the City’s motion to dismiss, holding that Allen had stated a claim for violations of the FLSA.
Allen v. Chicago (cont’d)

• Lawsuit (collective action) filed in May, 2010
• Notice to potential class members: April, 2013
• Bench trial concluded August 24, 2015
• Allen meanwhile was promoted to Sergeant… and no longer uses a Blackberry.
Lessons Learned

• Ask: who gets offsite access, and why?
• If offsite access to systems is given to non-exempt associates – why?
• Ensure non-exempt associates record all hours worked.
• Educate managers: Off-hours work is still work, and must be compensated.
• Monitor / enforce policy.
Recommendations

• Review policies including those on remote access and confidentiality.

• Review mobile device management and remote access software – does it give you what you need?

• Make sure each employee with remote access has written agreement regarding rights of access to device, wipe and swipe, etc.

• Equally important: Training for managers and HR to understand the policy and its boundaries.
Questions?