BARNES & THORNBURG LLP

Law of Corporation Information

New Issues on Old Foundations

William A. Nolan · bill.nolan@btlaw.com · (614) 628-1401

Game plan

- An anecdotal history of law and technology in 4 acts
- Objectives
  - Summarize several areas of the law
  - Draw parallels and connections
  - Some organizational strategies
- Themes and variables
  - Core: reasonableness / business alignment / job relatedness
  - Enforcement environment
  - Cultural issue or one that can be fixed with documents?

The 4 acts

- Workplace monitoring
- Trade secrets
- Employee electronic communications outside the organization
  - Specifically the NLRB and social media
- Preventing and responding to data breaches

BARNES & THORNBURG LLP

Act I: Workplace Monitoring

Workplace privacy overview

- Workplace privacy law is based on reasonableness and job relatedness
- Start with lockers and desks, fast forward to mid-90s
- Examples
  - U.S. Constitution
  - Invasion of privacy tort
  - Consideration of criminal records in hiring
  - ADA/FMLA regs on confidentiality
  - Regulating workplace appearance

Workplace privacy overview (cont.)

- Exceptions to reasonableness theme
  - Typically statutory
    - Public records laws
    - Procedural layers : FCRA / HIPAA / drug testing laws
    - Polygraph testing
  - Also: subpoenas / court orders

Workplace privacy overview (cont.)

- What's this all mean?
  - "Privacy" and "technology" have always been somewhat cutting edge
  - But litigation historically was relatively rare
    - At first, even with sharper focus brought on by technology
  - "Reasonableness" is a makeable standard
  - Potential plaintiffs in monitoring cases may not be ones who get close calls

This drives certain policy elements

- For example: acceptable use policy
  - No expectation of privacy
  - Expect monitoring
  - No excessive personal use
- Remarkably timeless

Reflect on variables

- Not an enforcement-heavy environment
- Generally not a cultural issue – can address it by documentation

BARNES & THORNBURG LLP

Act II: Trade Secrets

What is a Trade Secret?

- Information that:
  - derives independent **economic value**, actual or potential, **from not being generally known** to the public or to others who could derive economic value from its disclosure or use; and
  - is the subject of **reasonable efforts** under the circumstances to **maintain its secrecy**.

What is a Trade Secret?

- "Information" can broadly include:
  - formulas
  - patterns
  - compilations
  - programs

What is a Trade Secret?

- Specific Examples of Information That **May** Constitute a Trade Secret:
  - customer and supplier lists
  - recipes/formulas
  - computer source code
  - manufacturing methods
  - business plans and marketing strategies
  - pricing and costs

Information that is “Generally Known”

- Observable or apparent product features
- Scientific principles and laws of nature
- Standard industry practices

What are "Reasonable Efforts" to maintain secrecy?

- no hard and fast rules
- must be **reasonable** under the circumstances
  - Changes with technology

Information Not Subject to Reasonable Secrecy Measures

- disclosed in patents
- disclosed in SEC filings
- disclosed on websites
- observable on plant tours
- disclosed in speeches and articles
- not secured internally

Trade Secret Program: Workplace Controls

- Restricted distribution
- Off-limits areas
- Visitor access procedures
- Disposal of sensitive materials

Trade Secret Program: Electronic Security

- Access cards
- Encryption of transmissions
- Password protection

Trade Secret Program: Employment Practices

- Intake procedures – importance of confidential business information
- Non-disclosure and intellectual property agreements
  - Good to re-sign periodically
- Identify specifics?
- Reinforce upon departure

Trade Secret Program: Social Media

- Not permitted to comment publicly on confidential business projects or issues

- Customer contact and preferences maintained on social medial sites fall within non-disclosure policies and agreements – and must be set to “private”

Our 3 variables

- Very much the reasonable core
- Enforcement: private litigants
- Much more of a cultural: plenty of key documents but starting to get more into human behavior

Trade Secret Program: Social Media

- Expressly assert ownership interest over social media accounts and content (LinkedIn, Twitter, Google Plus)
- Company owns content developed on the job, using company resources, or confidential business information
- Customer information and goodwill are company property even if posted on employee's own account

Enforcement – LinkedIn and social media

- *Sasqua Grop, Inv. V. Courtney*, 2010 WL 3613855 (E.D. Mich. Sept. 30, 2010) (because customer contact list information readily available through LinkedIn, it cannot constitute a trade secret
- *Eagle v. Morgan*, No 11-4303 (E.D. Pa. March 12, 2013) (acquiring company that appropriated former executive's LinkedIn account liable for state law misappropriation)

Enforcement – LinkedIn and social media

- *KNF&T Staffing, Inc. v. Muller*, No. SUCV201303676BLS1 (October 24, 2013) Massachusetts state court held that updating a LinkedIn profile to reflect a new job (triggering contact notification) did not violate non-solicitation agreement.

BARNES & THORNBURG LLP

Act III: Limitations on Employee External Communications

Two key pieces of background

- Obvious: technological explosion enables employees to do rotten things they have always done on a more rapid and widespread basis → employers want to respond
- Card check, the Great Recession, and the NLRB

"Protected Concerted Activity"

- Section 7 of the National Labor Relations Act
  - NLRA is the ultimate old foundation: one of original New Deal L&E laws
  - "Employees shall have the **right** to:
    - self-organization,
    - form, join, or assist labor organizations,
    - bargain collectively through representatives of their own choosing, and
    - **engage** in other **concerted activities for the purpose** of collective bargaining or other **mutual aid or protection** "

What is "Protected Concerted Activity?"

- engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself
- individual actions that are the "logical outgrowth of concerns expressed by the employees collectively"
- "individual employees seek to initiate or to induce or to prepare for group action," including where employees discuss shared concerns among themselves prior to any specific plan to engage in group action.
- most common employer mistake: talking about your pay
- but: comments made "solely by and on behalf of the employee himself" are not concerted.

NLRB – Social Media

- This emerged as an issue since 2009 when a GC memo blessed a Sears policy of non-disparagement of the company.
- 2010 – NRLB reversed positions and we have been on that course ever since.
- The issues have focused on both situations dealing with employee discipline and general challenges to social media policies

Acting General Counsel Memos

- In a somewhat unusual act, the Acting General Counsel of the NLRB issued three memos in August 2011, January 2012 and May 2012 summarizing Advice Memoranda issued by the Board staff regarding the issues emerging over employee use of social media and protected activity.

NLRB Decisions—Social Media

Costco Wholesale Corp.

First NLRB Social Media Decision

Any communication transmitted, stored or displayed electronically must comply with the policies outlined in the Costco Employee Agreement. Employees should be aware that statements posted electronically (such as [to] online message boards or discussion groups) that damage the Company, defame any individual or damage any person's reputation, or violate the policies outlined in the Costco Employee Agreement, may be subject to discipline, up to and including termination of employment.

NLRB Decisions—Social Media

Costco Wholesale Corp. (Sept. 7, 2012)

- Held that rule violated Section 8(a)(1) because employees would reasonably construe the language in the rule to prohibit their Section 7 rights

- No disclaimer in policy to show it did not apply to protected concerted activity

NLRB Decisions: Knauz case

- A BMW dealership fired a salesperson after he posted comments and photographs on Facebook criticizing a sales event and an incident in the Land Rover lot.

- The employee criticized the concessions at the event:
  - "I was happy to see that [the dealership] went 'All Out' for the most important launch of a new BMW in years … the new 5 series. … The small 8 oz bags of chips, and the $2.00 cookie plate from Sam's Club, and the semi fresh apples and oranges were such a nice touch … but to top it all off … the Hot Dog Cart. Where our clients could attain a over cooked wiener and a stale bun. … No, that's not champagne or wine, it's 8 oz. water. Pop or soda would be out of the question. In this photo, [a coworker] is seen coveting the rare vintages of water that were available for our guests."

.

NLRB Decisions—Social Media

- NLRB found employee's post was *not* protected concerted activity because it was posted "as a lark"

Knauz BMW

- While the NLRB upheld the termination, it held that the company's "Courtesy Policy" was unlawful:
  - *Courtesy: Courtesy is the responsibility of every employee. Everyone is expected to be courteous, polite and friendly to our customers, vendors and suppliers, as well as to their fellow employees. No one should be disrespectful or use profanity or any other language which injures the image or reputation of the Dealership.*

Knauz BMW

- "Courtesy" rule unlawful because employees would reasonably construe its broad prohibition against "disrespectful" conduct and "language which injures the image or reputation of the Dealership" as encompassing Section 7 activity (i.e. statements objecting to working conditions)
- The NLRB ordered the company to remove this language and re-publish the policy

NLRB Decisions—Social Media/Unlawful

1. Prohibition of employees posting pictures of themselves in any media depicting the Company including wearing Company uniform violated NLRA.
2. Prohibition of employees making disparaging comments when discussing the Company or the employee's superiors, co-workers or competitors violated the NLRA.

NLRB Decisions—Social Media/Unlawful

3. Prohibiting "unprofessional communication" that could negatively impact Company's reputation.

4. Confidentiality agreements prohibiting employees from discussing terms and conditions of employment through social media.

NLRB Decisions—Social Media/Unlawful

5. Confidentiality terms that are non-specific and touch on items that may not be technically confidential. (prohibiting employees from "using any social media that may violate, compromise, or disregard the rights and reasonable expectations as to privacy or confidentiality of any person or entity")

6. Rules that prohibit untruthful content ("statements that lack truthfulness or that might damage the reputation or goodwill of the hospital, its staff, or employees.")

NLRB Decisions—Social Media/Unlawful

- 7. Prohibition against using Company logos or trademarks. ("Precluded the use of the Employer's logos and photographs of the Employer's store, brand or product, without written authorization.")

- 8. Provisions that threaten employees with discharge or criminal prosecution for failing to report unauthorized access to or misuse of information. ("We're serious about the appropriate use, storage and communication of confidential information. A violation of [Employer] policies regarding confidential information will result in corrective action, up to and including termination. You also may be subject to legal action, including criminal prosecution.")

NLRB Decisions—Social Media/Unlawful

9. Rules suggesting employees review their posts before the post them. ("When in doubt about whether the information you are considering sharing falls into one of the [prohibited] categories, DO NOT POST. Check with [Employer] Communications or [Employer] Legal to see if it's a good idea.")

10. Rules that prohibit employees from commenting on legal disputes or legal matters. ("Don't comment on any legal matters, including pending litigation or disputes.")

NLRB Decisions—Social Media/Unlawful

11. Play nice policies. ("Adopt a friendly tone when engaging online. Don't pick fights. … Remember to communicate in a professional tone. … but also proper consideration of privacy and topics that may be considered objectionable or inflammatory")

12. Use internal communications to resolve disputes first. ("You are encouraged to resolve concerns about work by speaking with co-workers, supervisors, or managers. [We think] individuals are more likely to resolve concerns about work by speaking directly with co-workers, supervisors or other management-level personnel than by posting complaints on the Internet.")

NLRB Decisions—Social Media/Lawful

1. Any rule that makes clear an exception exists for employees engaging in protected concerted activity (some disclaimers have been rejected).
2. Prohibiting employees from posting anything on the internet that could be construed as an act of unlawful harassment, a threat, or other evidence of discrimination.
3. Requiring employees to make personal internet postings during nonworking hours, meal periods and/or rest breaks.

NLRB Decisions—Social Media/Lawful

4. Healthy suspicion policy ("Employees should 'develop a healthy suspicion,' [which] cautions against being tricked into disclosing confidential information, and urges employees to 'be suspicious if asked to ignore identification procedures.")

5. No disclosure of safety performance of systems or components for vehicles and secret or Attorney-Client Privileged Information.

NLRB Decisions—Social Media/Lawful

6. Not the Company's Opinion ("Represent any opinion or statement as the policy or view of the [Employer] or of any individual in their capacity as an employee or otherwise on behalf of [Employer].")

7. Just my opinion. ("Any comments directly or indirectly relating to [Employer] must include the following disclaimer: 'The postings on this site are my own and do not represent [Employer's] positions, strategies or opinions.")

GC Upheld Wal-Mart's Social Media Policy in Whole

- Few examples of where the Wal-Mart Policy was found to be legal.
- Generally, the NLRB has found policies overbroad when they instruct employees not to share confidential information with coworkers.
- However, the GC upheld the *Wal-Mart* Confidentiality Provision as Lawful:
  - "Maintain the confidentiality of [Employer] trade secrets and private or confidential information. Trades secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications."

Wal-mart's Social Media Policy

- Compare: the NLRB found *Wal-Mart* Provision to be Lawful:
  - "Always be fair and courteous to fellow associates, members, suppliers or people who work on behalf of [Employer]. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers or by utilizing our Open Door Policy than by posting complaints to a social media outlet. **Nevertheless, if you decide to post complaints or criticism,** avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy."

Wal-Mart's Social Media Policy

- Employer Provision:
  - "Unless you are specifically authorized to do so, you may not: Participate in these activities with [Employer] resources and/or on Company time."
- The NLRB found Unlawful:
  - "[W]e concluded that the prohibition on participating in these activities on Company time is unlawfully overbroad because employees have the right to engage in Section 7 activities on the Employer's premises during non-work time and in non-work areas."
- Compare: the NLRB found the *Wal-Mart* Provision to be Lawful:
  - "Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by your manager or consistent with Company Equipment Policy. Do not use [Employer] email addresses to register on social networks, blogs, or other online tools utilized for personal use."

Triple Play Sports Bar

Is Hitting "Like" Protected Concerted Activity?

- A sports bar and restaurant discharged employees who participated in a Facebook conversation about tax withholding practices.
- A former employee posted a statement on her Facebook page when she discovered she owed money and noted the employer's inability to complete paperwork properly, including a choice expletive.
  - Another employee responded by clicking, "Like."
  - Two of the Employer's customers joined in the conversation, one referring to the owner as "such an asshole."

Triple Play Sports Bar

- The NLRB determined the Facebook conversation related to "shared concerns about a term and condition of employment--the Employer's administration of income tax withholdings."
- Additionally, the employer threatened to sue the parties for their remarks, which the NLRB held violated Section 8(a)(1) because it threatened suit for engaging in protected concerted activity.

Social Media Policy Tips

- **Disclaimer of responsibility.** Require employees to state in their social networking profiles that any opinions they express about work-related matters are their own and are not attributable to the company

- **Confidential Information.** Prohibit employees from posting confidential, copyrighted, or otherwise legally protected information or materials on their social networking profiles. Prohibit disclosure of any information regarding clients, suppliers or business partners without consent

Social Media Policy Tips

- **Ownership / No Right to Privacy.** State, in no uncertain terms, that the Company owns its electronic communications systems and its content, and that employees have no right to privacy with respect to any information sent, received, accessed, viewed, stored, or otherwise found at any time on the company's systems. State that any such information may be monitored or viewed by the employer in its sole discretion, at any time

- **Your Handbook Applies.** Inform employees that their use of social networking sites at work is subject to your general policies, including your policies prohibiting harassment, discrimination, and disclosure of confidential information. Employees may not use social networking sites or other electronic media to harass, threaten, libel, malign, defame, disparage or discriminate against co-workers, managers, customers, or anyone else

Social Media Policy Tips

- **Work time.** Remind employees that your technology is designed for work, not for personal use
- **Identification.** Inform employees that, if they choose to identify themselves as your employees in their personal social networking profiles, they must state explicitly that any views expressed are their own and not those of the employer
- **Photographs.** Consider prohibiting employees from posting photographs taken at the company's premises or events, without permission. (Be careful.)

Review 3 variables

- While many of us find it unreasonable in one sense, rules still based on that business alignment core
- But – intense enforcement environment
- Certainly strong cultural/behavioral aspects

BARNES & THORNBURG LLP

Act IV: Data Privacy and Preventing Data Breaches

U.S. Legal Authorities: Federal

- Federal Trade Commission (FTC)
  - *Section 5 FTC Act:* Empowers agency to bring enforcement actions against businesses for *unfair* or *deceptive* trade practices
- Federal Communications Commission (FCC)
- Dept. of Commerce (DoC)
- Dept. of Health and Human Services (HHS)

The Federal Trade Commission

- FTC Section 5: broad authority against *unfair* or *deceptive* trade practices
- FTC requires companies maintain **"reasonable"** procedures to protect sensitive information of consumers & must not misrepresent how they collect, use, and transfer the data they collect
- "Reasonableness" standard requires companies:
  - Deliberate and thorough approach to securing sensitive information
  - Truthfully convey practices to consumers
- FTC increasingly initiating enforcement actions based upon inadequate data privacy and security measures, and failure to meet "reasonable" standards
  - Fines, consent orders, long term audits
- States and sectoral regulators with similar laws and regulations may also bring legal actions

U.S. Legal Authorities: Sectoral

- **HIPAA / HITECH**
  - "Health Insurance Portability and Accountability Act"
  - Privacy of protected health information, personal health records
- **GLBA**
  - "Gramm-Leach-Bliley" Financial Services Modernization Act
  - Financial institutions required to adopt comprehensive data security programs.
- **FCRA**
  - "Fair Credit Reporting Act"
  - Credit/Insurance/Employment

U.S. Legal Authorities: Sectoral

- **CAN-SPAM**
  - "Controlling the Assault of Non-Solicited Pornography and Marketing Act"
  - All commercial e-mail messages
  - No false headings. Include notice message is an ad, opt-out notice (Unsubscribe), post address
- **TCPA**
  - Telephone Consumer Protection Act
  - No robo/auto phone calls/texts

U.S. Legal Authorities: State

- State laws
  - *47* State Data Breach Notification Statutes
- State Attorneys General
  - Breach investigations/enforcement actions

Culture & Employees

- Privacy is *everyone's* responsibility
- Create a culture of security
- Reinforce at every stage of the employment relationship
  - Hire
  - During
  - Termination

Culture & Employees

- Employee handbook: Review/update annually
- Require compliance with specific written policies governing the handling and confidentiality of sensitive data, and make it a part of the employee intake process
  - On-boarding + *off*-boarding
  - Specific requirements around employee access to data
- Include restrictive covenants in agreements restricting employee and business partner use of confidential data during and after employment

Culture & Employees

- Require and *encourage* employees to immediately report data security events, incidents, and breaches
  - Key is to ensure they feel they may do so without fear of retribution, even (especially) if it was their fault

- Educate to spot "inside jobs": Big risks to companies. Properly educate and train employees to help defend against the inside attack threat

- Design BYOD, COPE, CYOD, Social Networking, and other policies to address data privacy and security

Culture & Employees

- Train, train, and re-train
  - Privacy procedures & organizational principles
  - Have good "digital hygiene"
    - Do the security basics
- Monitor + Teach to monitor
  - Your company's first line of defense
  - Sensitize your entire staff to helping spot potential security issues

Data is a core asset

- **Does your business treat it as such?**
- **Do you know exactly what you have?**
- **Do you know who has access to it?**
- **Data security is a core business procedure**

What Do You Collect Now?

- What data do you create and collect, *and why*?
- *Precisely i*dentify the data within your organization
  - Where does the reside? (computers, mobile devices, flash drives, other digital devices and physical docs)
  - Who has access to that data, *exactly*?
  - How is that data collected? How is the data used?
- Map the data flow within/without the business
  - Put technical alarms in place to identify irregularities

What *Should* You Be Collecting?

- *Why* are you collecting what you're collecting?
- Is the data worth the responsibilities of collection?
- Or just creating unnecessary risk when it's stolen?
  - Compelling business need to collect it?
  - Used consistent with permission granted for collection?
- What processes are in place to assess new products/services and their privacy implications?
  - Whose job is it?

What Do You Keep?

- If you don't need it, *don't keep it*!
  - *They can't steal what you don't have →*
- If you *do* keep it, do so only as long as you *need* it
  - *Is the value of the data worth the risk of its retention?*

What Do You Keep?

- What data are you keeping?
  - *Social Security Numbers? Financial account info?*
- What data are your partners keeping?
  - *What does their contract say about it?*
- Why are you keeping this data?
  - *Compelling business need?*

What Do You Keep?

- How are you storing this data?
  - *Encrypted? Plain text?*
  - *Who has access? Who has access to partners' data?*
  - *Compliant with industry obligations?*
    - *HIPAA – Health; GLBA – Financial; COPPA – Children; etc.*
- How long are you keeping this data?
  - *Maintain a written Data Retention Policy describing your company's collection, use, storage and disposal practices*
- Not all data are created equal
  - *Evaluate risk level of data, prioritize accordingly*

Electronic Security

- Skilled IT staff, network security, limit network access, encryption, anti-virus, firewalls, complex passwords, two-factor authentication, remote access, offline digital storage, patches(!)
- Data export policies/protection critical
  - Monitor systems/security for intrusion
  - Monitor access to and use of sensitive data
  - Have a hard outer shell; don't let them get out with data

Three Variables

- Still a lot of reasonableness out there
  - But violation of codification may itself be a violation
- Enforcement-heavy environment
  - These plaintiffs are sympathetic
- Very much a cultural/behavioral matter

BARNES & THORNBURG LLP

Law of Corporation Information

THANK YOU

William A. Nolan · bill.nolan@btlaw.com · (614) 628-1401