Employee Privacy and Social Networking: Can Your Trade Secrets Survive?

Presented by:

Gary Glaser
Scott Schaefers
Jessica Mendelson

March 19, 2013
Social Media in the Workplace
The Number of Users and the Amount of Content Is Increasing Rapidly

- Facebook currently has over one billion users
  - more than half use Facebook on a mobile device

- LinkedIn has 161 million users
  - two new members every second
  - half of the members from the United States

- Google+ has over 400 million users

- YouTube has hundreds of millions of users
  - over 800 million unique visits per month

- Twitter currently has over 517 million users
  - including over 141.8 million users in the United States
  - Over 340 million tweets daily
Social Media In the Business World

• Use of social media for business purposes has increased exponentially in the past few years

• Social media has become ubiquitous in marketing

• Worldwide survey:
  ► Over 75% of respondents used social media for business purposes.
  ► Less than 2/3 of businesses monitored employees’ use of social media.
Why worry about social media?

- Valuable trade secrets can be easily disclosed and other IP rights infringed

- The speed at which businesses use social media is growing

- Not always clear who will have access to and the right to use information injected by the company into social media
Trade Secrets & Misappropriation
What is a Trade Secret?

► Information
  • includes but not limited to formulas, patterns, compilations, devices, methods or designs

► Derives independent economic value from not being generally known or reasonably ascertainable

► Subject of reasonable efforts to maintain secrecy
6 Factors to Determine Whether Information Constitutes a Trade Secret:

1. Extent known outside the company
2. Extent known by employees and others inside company
3. Measures taken by company to protect secrecy
4. Value of trade secret to company and competitors
5. Time, effort, and money expended in development.
6. Ease of difficulty which it can be properly acquired or duplicated by others
Protection Against Misappropriation

- Uniform Trade Secrets Act, the Economic Espionage Act, Computer Fraud and Abuse Act
  - UTSA largely codified common law, enacted in 47 states in the United States
- This prevents the illegal or unauthorized acquisition, disclosure, or use of information
- No protection against accidental disclosure or reverse engineering
- Third parties liable if they knew or had reason to know
Trade Secrets: Who Is Stealing Data?

• Most common misappropriator = rogue employees and business partners
  ► Statistics suggest that over 90% of trade secret misappropriation is done by employees, former employees, and business partners
  ► Vast majority of misappropriation is achieved by electronic means

• Why employees and business partners?
  ► They have access to and familiarity with computer systems and information stored within

• Technology makes it easy
  ► Many tools for exfiltration of data
  ► Technology allows for remote and cloud computing
Protection Against Misappropriation

• Have coherent company policies in place regarding intellectual property

• Take reasonable steps to ensure confidentiality and secrecy of information
  ▶ Ensure employees are aware of responsibilities to safeguard confidential information,
  ▶ Ensure new employees are not bringing confidential information from their former employees

• Have employees sign non-disclosure agreements with specific language regarding what can and cannot be disclosed

• Consider implementing data prevention policies to ensure intellectual property is not being used inappropriately
NLRB has recently issued three reports which describe the types of social media cases the NLRB is seeing and summarizing the results of these cases.

- These reports reviewed 20 companies policies, and of these, 16 were found to be overly broad.
- Several decisions addressing employee use of Facebook and Twitter found employees were engaged in protected concerted activity.

May 30, 2012 memorandum on social media policies:
- The report stressed the importance of careful drafting to avoid any broad language which employees could reasonably construe to prohibit “protected concerted activities.” Must provide specific definition of Confidential Information.
Labor-Management Relations and Trade Secrets: *Almost Total Strangers*
• General Discussion: **A Look At 2012**

1. **Social Media:** Traditional notions of “Protected Concerted Activity” Applied to the *(Not-So-New)* Frontier

   • **Protected Activity in the “good old days. . .”**

   • **The continued expansion of “PCA”: From Social Media to “Stirring Things Up” as the new “recipe” for engaging in protected concerted activity**

A. **The Evolution of “Protected Concerted Activity”**

B. **The “Tryptic” of the Acting General Counsel’s Memos on Social Media and Protected Concerted Activity**

   • May 30, 2012 “Updated Report”: How to Lose 6 Social Media Cases before the NLRB, and How to Win One
General Discussion:  *A Look At 2012 (Social Media cont’d)*

C.  **Employer and Union Conduct:**

- *Hispanics United of Buffalo, Inc.:* Facebook at the NLRB – Venting On-Line for “Mutual Aid or Protection”

- *The Other Side of the Coin: Amalgamated Transit Union Local 1433 -* Union’s Facebook Page Not an “Electronic Extension” of its Picket Line, NLRB ALJ Rules (“Oh, it’s a ‘CB’ Case. . .”)
D. *Employee Handbooks and Work Rules:* The NLRB’s further in-roads into Employers’ attempts to maintain a civil workplace, to comply with fair employment practice laws, and to protect its Trade Secrets:

1. **Acting NLRB G.C.’s 5/30/12 Memo:**

   - Employee Handbook provision, “Don't release confidential guest, team member or company information. . .” is **unlawful.**

   - Provision instructing employees not to share confidential information with co-workers unless they need the information to do their job, and not to have discussions regarding confidential information in breakroom, at home, or in open areas and public places are **overbroad** and thus **unlawful.**
Acting NLRB G.C.’s 5/30/12 Memo (cont’d):

- Provision threatening employees with discharge or criminal prosecution for failing to report unauthorized access to or misuse of confidential information - - is unlawful.

- Portion of work rule is unlawful insofar as it instructs employees not to “reveal non-public company information on any public site” and then explains that non-public information encompasses “[a]ny topic related to the financial performance of the Company”; “[i]nformation that has not already been disclosed by authorized persons in a public forum” and “personal information about another employee. . .”
General Discussion: **A Look At 2012 (cont’d)**

*The Board itself “speaks”:

2. **Banner Health System and the Confidentiality of Internal Investigations:**

   Can the Board’s approach co-exist with that of the EEOC’s emphasis on the importance of confidentiality as part of any non-harassment policy?

3. **September, 2012:** the NLRB issued its first decision focusing on the issues covered by the Acting General Counsel in his 5/30/12 Memo – that is, an Employer’s Social Media Policy and its impact on employees’ right to engage in “protected concerted activity”. In that case, the Board held that:

   - A Company policy providing, among other things, that “[s]ensitive information such as membership, payroll, confidential financial, . . .may not be shared, transmitted, or stored for personal or public use without prior management approval” was unlawful, particularly where the rule also stated that employees are responsible for ensuring that “all” information relating to the Company and its employees is secure and not to be disseminated (emphasis supplied). . .
General discussion: **A Look Forward – What can we Expect in 2013?**


*The NLRB’s Response: “the Board has important work to do. . .”*
Trade Secrets, Restrictive Covenants and Social Media: Who Owns What and What Can One Do?
Eagle v. Morgan, (E.D. Pa.)

- Company promoted itself using employee’s LinkedIn account.
- After she left, company seized the account and transferred it to another employee.
- Employee regains control of account. Both sides sue.
- LinkedIn account not a trade secret because the information in question is “generally known in wider business community” or can be “easily derived from public information,” (and in fact E/er disclosed much of it on its website) and E/er did not take reasonable steps to maintain its secrecy. – Note “word to the wise. . .”
- But, issues of fact exist as to whether employee’s use of account supported common law claim for misappropriation of an idea” by employer. (After bench trial, Court said it did not, because: E/er never had a policy requiring e/ees to use LinkedIn; didn’t dictate precise contents of an e/ee’s LinkedIn account, and didn’t pay for its employees’ LinkedIn accounts; indeed, E/er didn’t even maintain any separate account and E/er presented no evidence that Plaintiff’s contact list was developed and built through the investment of the E/er’s time and money as opposed to her own, plus her extensive past experience.)
Eagle v. Morgan, (E.D. Pa.)

**So what happened??**

- After bench trial, the judge concluded that Plaintiff owned her LinkedIn profile. Plaintiff won her claims for unauthorized use of name, invasion of privacy by misappropriation of identity, and misappropriation of publicity.

- **But**, the judge awarded Plaintiff (who appeared *pro se*) **no damages**, because it found her evidence of damages was too speculative.

- **Additionally**, the judge rejected Plaintiff’s claims for identity theft (because no “unlawful purpose” and lack of “identifying information”), conversion (since no “tangible property” converted), tortious interference (since no actual legal damage proven), civil conspiracy (on multiple grounds), and civil aiding and abetting (since no evidence presented as to actions by individual defendants).
PhoneDog v. Kravitz, (N.D. Cal.)

- Employee helps manage company’s Twitter account — “@PhoneDog_Noah”
- Employee leaves, seizes account, and changes the account handle to “@noahkravitz”
- The company sues.
- Court denies the employee’s motion to dismiss, finding that employee’s theft of Twitter account stated claim for misappropriation of trade secrets.
- **So what happened??** -- The parties settled.
Christou v. Beatport, LLC

- Plaintiff alleged that defendant misappropriated MySpace login info and stole MySpace “friends” list.
- The Court denied defendant’s motion to dismiss.
- The Court found that the MySpace “friend” relationship *could* be a trade secret, so that the trade secret claim survived at the motion to dismiss stage.
- However, what’s protectable isn’t the *list* of “friends” (which is public), but the “friend” relationship, because it lets you view your “friends” contact information, interests and preferences.
- The litigation is ongoing.
Invidia, LLC v. DiFonzo (Mass. Sup. Ct.)

• This is a non-compete case, not a trade secrets case.

• Employee signed non-solicitation agreement.

• During her employment, she became Facebook “friends” with at least 8 clients.

• Employee leaves and joins a competitor. Information about her new job is posted on her Facebook page.

• Former employer sues, claiming that that employee solicited customers by staying “friends” with them, and through posting about new job.
Invidia, LLC v. DiFonzo (Mass. Sup. Ct.)

- Court denies former employer’s motion for a preliminary injunction.
- Staying Facebook “friends” with customers isn’t “solicitation.”
- Posting about your new job on Facebook isn’t “solicitation.”
Sasqua Group, Inc. v. Courtney, (E.D.N.Y.)

- Recruiting firm maintained database that included client contact information, profiles, hiring preferences, and descriptions of previous interactions.

- When employee left to start competing company, recruiting firm sued, alleging that she had misappropriated trade secrets from the database.

- Adopting a Magistrate Judge’s R&R, the Court held that the database should not be afforded trade secrets protection, and denied the plaintiff’s motion for an injunction.
Sasqua Group, Inc. v. Courtney, (E.D.N.Y.)

• Most of the information could be reconstructed from publicly available sources, such as LinkedIn.

• A client’s hiring preferences wasn’t publicly available, but defendant “may simply have asked the clients about their preferences.”

• Plaintiff “failed to take even basic steps to protect the secrecy of the information” – this was the key. . .the rest is “commentary”: a lesson to be learned

• The info was “exceedingly old and stale,” and may have been stolen from plaintiff’s previous employer.

• The parties settled shortly thereafter.
Mandatory Account Info

Turnover Bans:

Good or Bad?
States with Turnover Ban Legislation in Effect

- California
- Delaware
- Illinois
- Maryland
- Michigan
- New Jersey (Higher ed only; employer bill pending)

Uncle Sam? No.

- First died in committee, second on its deathbed.
What these Laws say

• No requesting or requiring employees to provide account passwords or “related information.”

• “Social networking website” broadly defined.

• Some pending legislation would even prohibit asking ‘whether’ employee has account.

• No retaliation for refusing to provide, whistleblowing, or remedial process participation.

• Stiff (though discretionary) damages and penalties for employer breaches (including attorneys’ fees).
What’s the Idea?

• Prevent unfair world collision: personal vs. work life.

• Prevent unfair adverse employment action based in whole or in part on out-of-context content.
What are some Exceptions / Exemptions?

• Employer-owned devices;

• “Non-personal” accounts (???)

• Good-faith investigations of compliance or security breaches;

• Public domain information.
What other States are Thinking About It?

• Around 25 other states have considered or are considering similar legislation.

• Some states (i.e. Washington state) have broadly-worded bills with few carve-outs.
• Baseless lawsuits (fee-shift provisions whet the bars’ appetites)
  ▶ What does ‘require’ or ‘request’ mean?
  ▶ What is a ‘personal’ vs. ‘non-personal’ networking account?

• Increase in Information Theft or Leakage
  ▶ More difficult to detect employee info or IP misuse;
  ▶ I.e. company logos, customer lists, pricing data.

• Interstate Minefield
  ▶ Same interstate employer has different hiring / retention practices in different states.
  ▶ How to deal with interstate employees?
Some recent decisions give or suggest employer ownership in employee networking profiles.

- *Eagle v. Morgan* (re: LinkedIn account);
- *PhoneDog v. Kravitz* (Twitter account);

Employer obligations re: hiring and retention

- Negligent hiring / supervision / retention claims.
- Networking profile reveals reckless behavior or tendencies;
- Will abundance-of-caution employers be protected?
**WWOD (What Would Obama Do)?**

- **White House 2/20/13 Five-Point Plan to Combat Trade Secret Theft**
  - Point 2: Promoting voluntary best practices in private sector;
  - Point 3: FBI, ODNI, DOJ prevention efforts with private sector
  - Point 4: Improving domestic legislation.
  - Point 5: Public outreach and awareness efforts.

- **2012 Trade Secret Clarification Act**
  - Expanded reach of Economic Espionage Act
    - Filled hole per *U.S. v. Aleynikov* (2nd Cir. 2012), where code-stealer’s conviction overturned due to EEA’s archaic language.
      - Any product AND internal IP asset would be covered.
    - Significantly increased fines and penalties for violations.
Moral of the Story:
If You’re Gonna Do It, Do it Right.

• Exempt employer-device policies;

• Exempt good-faith investigations of misconduct or IP theft;

• Heighten evidentiary requirements for fee recovery, and make fee-shift a two-way street.
THANK YOU!

Questions?

Stay current on trade secret issues by visiting our blog at:

www.tradesecretslaw.com
How You Can Reach Us

Gary Glaser, Partner
New York
gglaser@seyfarth.com
(212) 218-5575

Jessica Mendelson, Associate
San Francisco
jemendelson@seyfarth.com
(415) 544-1058

Scott Schaefers, Partner
Chicago
sschaefers@seyfarth.com
(312) 460-5647