Strafford

presents

Employee Privacy in Electronic Communications: New Threat to Employers?

Crafting and Enforcing Policies for Work Computers and Mobile Devices

A Live 90-Minute Teleconference/Webinar with Interactive Q&A

Today's panel features:

Lauren E. Schwartzreich, **Outten & Golden**, New York

Philip L. Gordon, Shareholder, **Littler Mendelson**, Denver

Nick Akerman, Partner, **Dorsey & Whitney**, New York

Thursday, July 8, 2010

The conference begins at:

1 pm Eastern

12 pm Central

11 am Mountain

10 am Pacific

You can access the audio portion of the conference on the telephone or by using your computer's speakers.
Please refer to the dial in/ log in instructions emailed to registrations.

For CLE purposes, please let us know how many people are listening at your location by

- closing the notification box
- and typing in the chat box your company name and the number of attendees.
- Then click the blue icon beside the box to send.

- If the sound quality is not satisfactory and you are listening via your computer speakers, please dial **1-866-871-8924** and enter your PIN when prompted. Otherwise, please send us a chat or e-mail sound@straffordpub.com immediately so we can address the problem.
- If you dialed in and have any difficulties during the call, press ***0** for assistance.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Employee Privacy in Electronic Communications

Quon and Beyond – Implications for Workplace Technology Policies

Strafford Webinar– July 8, 2010

Presentation by
Lauren E. Schwartzreich, Esq.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Two Major Cases – Quon and Stengart

City of Ontario v. Quon – City employer reads police officer's text messages.

Stengart v. Loving Care Agency – Private employer forensically images former employee's laptop computer and reads her web-based emails.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Quon – 9th Circuit and SCOTUS

Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).

City of Ontario v. Quon, No. 08-1332, __ S. Ct. __ , 2010 WL 2400087 (June 17, 2010).

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Quon (9th Cir.)

Background

- City Employer maintained broad policy stating that electronic communications were not confidential and not for personal use.
- Supervisor deviated from policy and permitted limited personal use.
- Employer obtained and reviewed Employee's text messages and subsequently terminated Employee.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Quon (9th Cir.) (continued)

Ruling:

- Wireless provider violated Stored Communications Act.
- Employer violated Employee's Fourth Amendment rights.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

City of Ontario v. Quon,
No. 08-1332, __ S. Ct. __ , 2010 WL 2400087 (June 17, 2010).

Supreme Court declines to decide whether Employee had reasonable expectation of privacy out of concern that doing so "might have implications for future cases that cannot be predicted."

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Quon (S. Ct.) (continued)

Even assuming expectation of privacy existed, Court found search to be reasonable and held that City did not violate Employee's Fourth Amendment rights.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Lessons to be learned from *Quon*

Broad Lesson:

Society will set parameters for reasonableness of employee's expectation of privacy.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Lessons to be learned from *Quon*

Role of Societal Factors

- Employers tolerating personal use of technology;
- Emergence of laws protecting persons from monitoring of electronic communications; and
- Pervasive use of particular technology.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Lessons to be learned from *Quon*

Role of Individual Factors

- Ambiguity in technology policy;
- Whether technology used is "personal" (and if not, whether "personal" technology could have been used); and
- Where employee uses technology.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Stengart v. Loving Care Agency

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

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Stengart v. Loving Care (continued)

Background:

- Employee communicated with attorney via personal web-based email account.
- Employer forensically retrieved emails.
- Employer's counsel refused to return emails to Employee.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Stengart v. Loving Care (continued)

- Trial court found that the technology policy placed Employee on notice that her emails would be considered company property.
- Appellate Division disagreed, finding that an objective reader could reasonably conclude that not all personal emails are company property.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Stengart v. Loving Care (continued)

Supreme Court of New Jersey:

- Reasonable expectation of privacy existed.
- Employers cannot use otherwise lawful policies to engage in conduct that is against public policy.
- Even explicit policy permitting monitoring of attorney-client communications would not be enforceable.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Lessons to be learned from *Stengart*

Factors impacting reasonableness of expectation of privacy:

- Permitting personal use;
- Absence of express language;
- Employee efforts to maintain privacy of electronic communications;
- Innocuous communication content; and
- Legitimate purpose of policy.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Where employers usually go wrong…

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Selective Enforcement of Policies

Selective enforcement of technology policy against employee in discriminatory manner.

Guard Publishing Co. v. NLRB, 571 F.3d 53, 60 (D.C. Cir. July 7, 2009) (employer discriminated against employee in violation of the National Labor Relations Act where "in practice the only employee emails that had ever led to discipline were the union-related emails at issue here."). *See also Gorzynski v. JetBlue Airways Corp.*, 596 F.3d 93, 2010 U.S. App. LEXIS 3424 (2d Cir. Feb. 19, 2010).

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Retaliatory Enforcement of Policies

Monitoring technology use as a form of unlawful retaliation.

- *Zakrzewska v. The New School,* 543 F. Supp. 2d 185 (S.D.N.Y. 2008) – Employer monitored internet usage in response to employee's complaint of discrimination.

- *Dotson v. City of Syracuse,* No. 5:04-CV-1388, 2009 U.S. Dist. LEXIS 62174 (N.D.N.Y. July 21, 2009) – After employee complained of sexual harassment employer retaliated by eavesdropping on her telephone conversations.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Employer Doesn't Mean What it Says

Selective treatment of employees' electronic communications as "private" may discredit technology policy.

U.S. v. Hatfield, No. 06-CR-0550, 2009 U.S. Dist. LEXIS 106269 (E.D.N.Y. Nov. 13, 2009) – Employer's actions indicated that it viewed *other employees'* electronic communications as private, thereby discrediting its argument that *this* employee's communications were not private.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Lessons from *Quon*, *Stengart* and others…

- Unambiguous language;
- Consistent enforcement;
- Specified types of monitoring and retrieval;
- Identification of nexus between policy and legitimate interest;
- Factoring society's views on technology and privacy; and
- Enforcement of policy in non-discriminatory and non-retaliatory manner.

OUTTEN & GOLDEN LLP

Advocates for Workplace Fairness

Thank you.

Lauren E. Schwartzreich, Esq.
Outten & Golden LLP
3 Park Avenue
29th Floor
New York, NY 10016

Visit our Practice Group blog:
www.workplaceprivacycounsel.com

A Littler Webinar

Employee Privacy in Electronic Communications: *New Threat to Employers?*

Philip L. Gordon
Littler Mendelson, P.C.
1200 17th Street
Suite 1000
Denver, CO 80202
303.629.6200
PGordon@littler.com

A Littler Webinar

EIGHT IS ENOUGH: EIGHT TOUGH ISSUES IN WEB 2.0

Issue #1: On-Line Background Checks

Natalie Boyce has downloaded the background check app, "Been Verified," to her iPhone. After interviewing Tom Jones, she checks Jones' criminal history, finds two convictions, and prepares a negative evaluation.

- Boyce's employer is exposed to potential liability under the Fair Credit Reporting Act if it relies on Boyce's negative evaluation to reject Jones' job application

Fair Credit Reporting Act

- **Prohibits employers from obtaining criminal history on a job applicant from a "Consumer Reporting Agency" (CRA) without providing notice to the subject and obtaining the subject's consent**
  - CRA = A third party who, for a fee, assembles information bearing upon a consumer's creditworthiness, character, general reputation, or mode of living
- **Employer that relies on a report from a CRA must provide pre-adverse action notice and final adverse action notice in connection with any adverse employment action**

Solution #1

Prohibit employees from conducting <u>any</u> form of background check

Background checks may be conducted only through the employer's authorized vendor

Issue #2: Customer–Facing Company Sites

- **Establish a social media structure**
  - Create a social media steering committee
  - Establish guidelines
  - Provide training
  - Who is authorized to post?
  - Who will review content?

Solution #2: Affirmative Guidelines

1. **You are responsible; Take it seriously**
2. **Create excitement; Add value**
3. **Be respectful; Use good judgment**
4. **Be a leader; Admit mistakes**
5. **Report misuse to Human Resources**

Solution #2: Prohibited Conduct

1. **Disclosing confidential information**
2. **Discussing internal company matters**
3. **Violating company policy**
4. **Soliciting for non-company activities**
5. **Posting anonymously or pseudonymously**
6. **Slacking**

Issue #3: Individual Employee Sites For Business Purposes

Who "owns" employee's LinkedIn contacts and Facebook fan pages created for work-related purposes? <u>Policy</u> <u>Responses</u>:

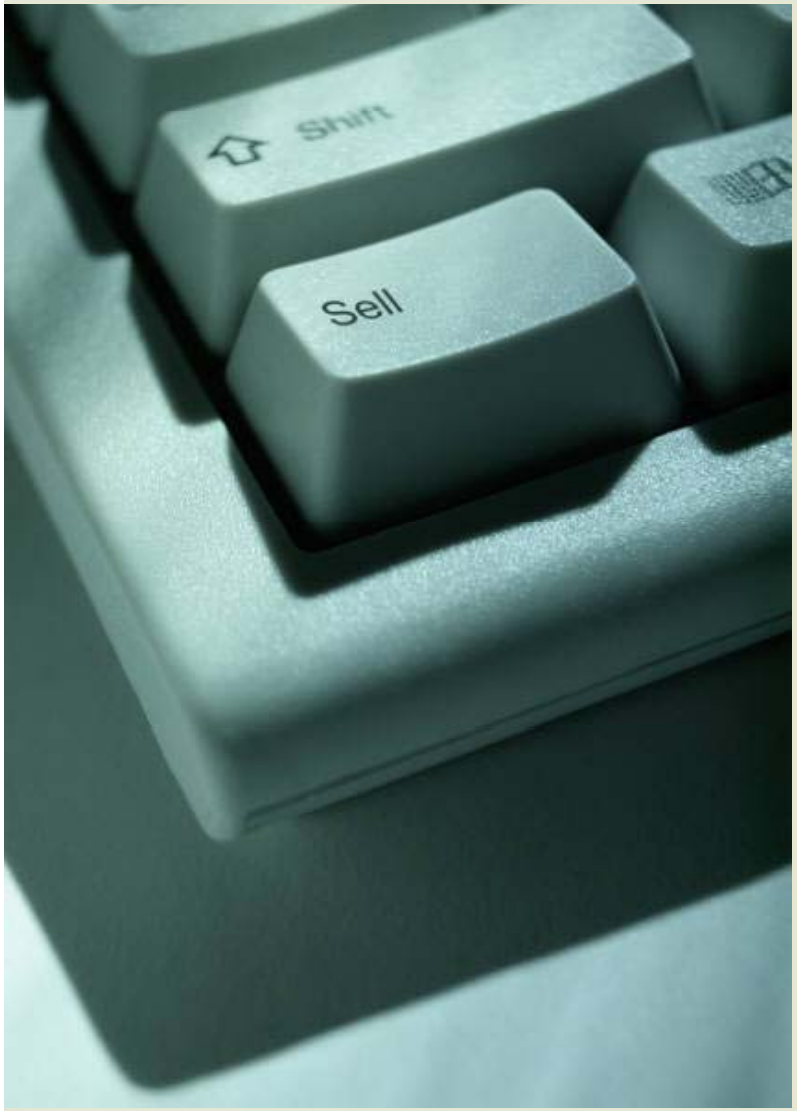
- Employees authorized to engage in social media activity on the company's behalf must use a corporate e-mail address when registering and establish the account in the company's name
- Employees may not use a personal account to establish a social media presence on the company's behalf

Solution #3: Individual Employee Sites For Business Purposes

Agreement with Employee:

1. **Employee will disclose each social media account established for business purposes and provide any password to HR**
2. **Employee will provide any new password to HR**
3. **Employee acknowledges that company owns the account, and all information in it, and consents to company's access**
4. **Employee will use the account only for business purposes**
5. **Employee will adjust privacy settings to protect company information**
6. **Employee will deactivate the account upon termination of employment**

Issue #4: The Overeager Salesperson



- **Company establishes a Facebook fan page for product launch**
- **“Fans” trash the product**
- **Unattributed posts turn the tide of negative opinion**
- **Product manager is outed**

New FTC Guidance

Employees who "endorse" their organization's products or services on Web 2.0 must disclose the employment relationship (Dec. 2009)

- Endorsement = a message "that consumers are likely to believe reflects the opinions, beliefs, findings or experiences of a party other than the sponsoring advertiser, even if the views expressed are identical to the sponsoring advertiser."

➢ **Solution #4: "Disclose your employment by the Company if your posting expresses opinions, beliefs, findings, or experiences concerning the Company's products or services."**

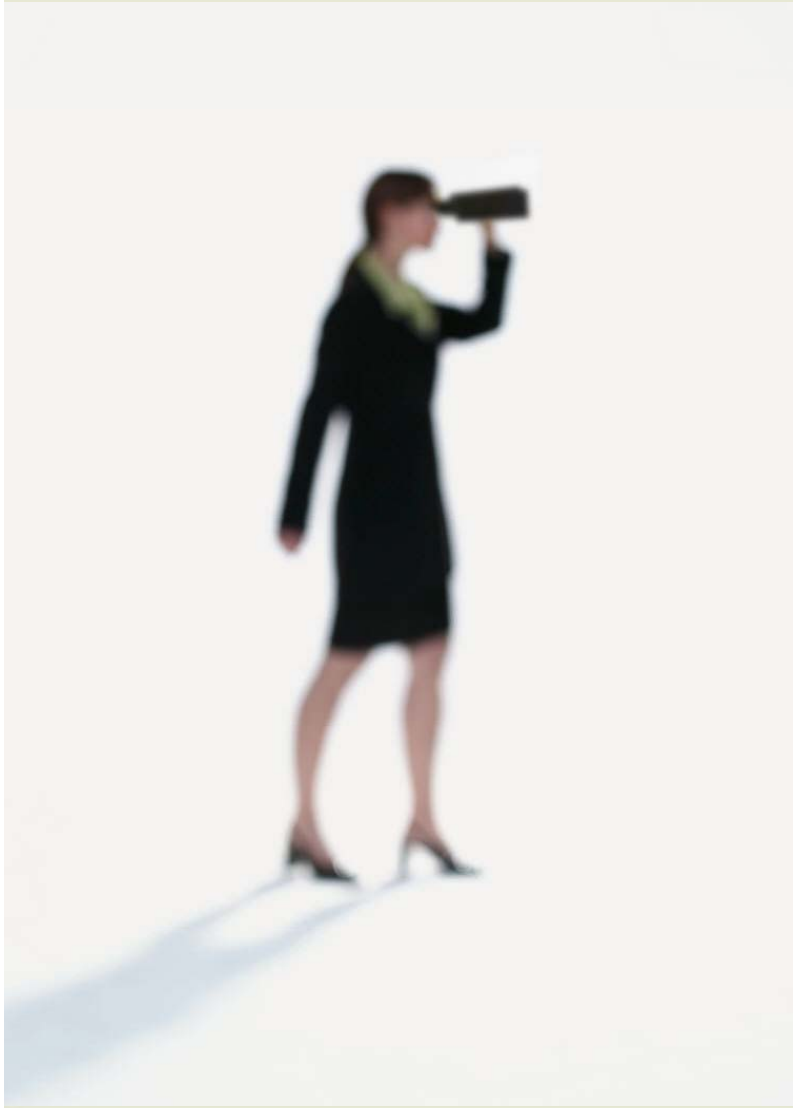
Issue #5: Who Is Your Friend?

What should employers do about managers' "friending" subordinates?

<u>Solution #5</u>:

- **Managers should not send "friend" requests to subordinates**
- **Any employee may reject any friend request without any retaliation**

Issue #6: Monitoring Employees' Social Media Activities



Employers do not have a duty to monitor employees' social media activity, but they now have the technological ability to do so

"Social Sentry," a software-as-a-service product launched in April, provides alerts of employee activity on Facebook, LinkedIn, Twitter, and YouTube.

- Selected employee or the entire workforce
- Keyword searches

NLRA Protections For Employees

1. **Activity must be "concerted"**
   - E.g., blog for co-workers
2. **"Concerted activity" must be "protected," i.e., related to the terms and conditions of employment**
3. **Existing union is not required**

Unfair Labor Practice?

- **Viewing protected, concerted activity that is readily accessible to the general public is not lawful if done in a way that will not intimidate protected activity.**
- **Viewing protected, concerted activity that is purposely shielded from the employer likely will be deemed unlawful surveillance.**

Issue #7: Access To A Restricted Page

Key Facts:

- **Houston's employee creates a group MySpace page**
- **Purpose: "To vent about any BS while at work without any outside eyes spying in on us"**
- **Houston's managers asked hostess for her password**
- **Two group members are fired**

Pietrylo v. Hillstone's Restaurant Group, d/b/a Houston's, (D.N.J. 2009)

Illegal Hacking?

<u>Claims</u>: Violation of Stored Communications Act invasion of privacy

<u>Result</u>: Verdict for employees on SCA claim, but for employer on invasion of privacy claim

<u>Jury Questionnaire</u>:

1. Managers knowingly accessed the group page without hostess' authorization
2. The group page was private, but plaintiffs had no reasonable expectation of privacy in their statements

Solution #7

- **Employee provides screen shots of offending posts**
- **Employee executes consent form**
  - Explain reasons for access to site
  - Affirm voluntary nature of access
  - Consent may be revoked
  - No retaliation

Issue #8: Venting By Former Employees

There are dozens of vent sites on the Web. What are the response options?

1. Demand removal of posts that violate the site's terms of use

2. Internal PR offensive

3. Threaten lawsuit, but don't sue

4. File a lawsuit

5. Ignore

Lawsuits Against Anonymous Posters

Krinksy v. Doe 6, 159 Cal. App. 4th 1154 (Cal. App. 2008) (refusing to enforce subpoena to unmask anonymous blogger whose "rude and childish posts" were "intemperate, insulting and often disgusting," but were non-actionable "crude, satirical hyperbole")

In re Liskula Cohen, Case No. 100012/09 (N.Y. Sup. Ct. Aug. 17, 2009) (enforcing subpoena to unmask author of the "Skanks of NYC" blog because reference to Cohen as "skank," "skanky," "ho," and "whoring" were factual, and if proven false, would support a defamation claim)

Visit our Practice Group blog:
www.workplaceprivacycounsel.com

A Littler Webinar

THANK YOU

Philip L. Gordon
Littler Mendelson, P.C.
1200 17th Street
Suite 1000
Denver, CO 80202
303.629.6200
PGordon@littler.com

Formulating Corporate Policies for the Computer Fraud and Abuse Act

Nick Akerman
Dorsey & Whitney LLP
akerman.nick@dorsey.com
http://www.computerfraud.us

Computer Fraud and Abuse Act Provides Proactive Tool to Protect Data

- Title 18 U.S.C. § 1030 – Enacted in 1984
- Criminal statute
- Civil remedy in 1994 amendment
- Computers used in interstate commerce
- Amended in 2001 and 2008
- Provides for damages and injunction

Various Causes of Action

- Stealing valuable computer data
- Schemes to defraud
- Trafficking in a computer password or similar information with intent to defraud
- Damaging computer data
- Hacking
- Extortion
- Sending computer viruses

Legal Requirements

- Protected computer
- Lack of authorization or exceeding authorization to access computer
- Theft of information or anything of value
- Damage to data permanent
- $5,000 loss
- Limited to economic damages
- Compensatory damages
- Two-year statute of limitations

The $5,000 Jurisdictional Limit

- Loss during any 1 year period aggregating at least $5,000
- Loss defined by statute as cost of responding to offense, restoring data or system or costs from interruption of service
- Must relate to computer
- Forensic review counts

Key Issue: Unauthorized Access

- Section 1030(a)(4) - Whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value…

EF Cultural Travel v. Explorica

- Ex-employees set up competing student travel company
- Information was accessed through public website
- Robot created with confidential information
- Used robot to download pricing data
- First Circuit upheld injunction based on confidentiality agreement
- Authorization established by contract
- Pricing data was valuable

Authorization Established by Company

- First Circuit: the CFAA "is primarily a statute imposing limits on access and enhancing control by information providers."
- Companies can set predicate for CFAA violation
- Rules on authorized access
- Agreements can set limits
- Similar to criminal trespass

International Airport Centers LLC v. Citrin (7th Cir.)

- Employee destroyed data on company computer
- Authorization based on law of agency
- Authorization terminates with disloyal act
- Judge Posner found that authorization terminated when employee "resolved to destroy files that incriminated himself and other files that were also the property of his employer."

LVRC Holdings LLC v. Brekka (9th Cir.)

- Employee emailed to himself competitively sensitive data
- Refused to adopt *Citrin*
- Employee cannot access company computers without authorization because employer gave him permission
- Does not address rules or agreements limiting access

Ways to Establish Lack of Authorization

- Hacking by outsider who breaks into computer
- Exceeds expected norms of intended use
- Terminates Agency relationship with employer by disloyal conduct
- Violates company policies and rules
- Breaches contractual obligation

Two Conflicting District Court Decisions

U.S. v. Nosal (N.D. Ca. 2010)

- Authorization cannot be based on corporate policies
- Thrust of *Brekka* not to look at motive in accessing

Kal-Tencor Corp. v. Murphy (N.D. Ca. 2010)

- Employee used Evidence Eliminator to delete all emails, files and internet history
- Authorized access predicated on employee agreement requiring return of records at termination
- No reference to *Brekka*

Company Rules

- Employee Handbook
- Compliance Code of Conduct
- Terms of Use on company Web site
- Training

Website Terms of Use

- Require users to provide accurate registration information
- Limit use of account to registered user at one computer at a time
- Prohibit use of web crawlers, robots and similar devices
- Post acceptable use guidelines that prohibit abuse, harassment and similar conduct
- Specify limitations on use of materials obtained (e.g., no commercial use)

Agreements

- Officers/Employees/Third Parties
- Among related companies
- Confidentiality/Non-Disclosure
- Post employment restrictive covenants
- Agreement to search personal computers
- Permissions re use of the computers
- Customer agreements
- Data vendor agreements

Snap-On Business Solutions, Inc. v. O'Neil & Associates

- Snap-On and Mitsubishi entered into a license agreement whereby both contributed to electronic auto database
- Mitsubishi approached O'Neil two years into contract to replace Snap-On
- O'Neil used robot to copy database
- Issue: was O'Neil authorized to access the database?

Use of Technology

- Password protection is simplest
- Access based on need to know
- Risks re transportable media
- Encryption
- Audit trail
- Coordinating with document retention and e-discovery