Perkins Coie | Legal Counsel to Great Companies

Privacy in the Electronic Workplace

Kevin J. Hamilton
February-March 2007

Perkins Coie Educational Seminar
February - March 2007

Seattle, Washington

This PowerPoint is not intended to be and should not be used as a substitute for specific legal advice, since legal opinions may be given only in response to inquiries regarding specific factual situations. Subsequent legal developments after the date of specific briefings may affect some of the legal standards and principles discussed. If legal advice is required, the services of counsel should be sought.

Electronic Information Systems Have Changed Everything

- Email: the gift that keeps on giving

- Blogging

- Workplace investigations—video surveillance, GPS tracking, and "pretexting"

- Medical records

- Lost laptops and personnel records

Electronic Communications and Data: Everywhere You Look (and Several Places You Don't)

- **Collaboration and communication:** email, blogs, text messages, wikis, instant messaging
- **Network security:** Intranets, servers, remote access
- **Storage media:** laptops, hard drives, iPods, CDs, DVDs, flash drives

Regulating Employee Use of Electronic Communications and Resources

- Efficiency offered by electronic communications and resources are double-edged swords
  - Makes sharing info and conducting business easier
  - Leads to novel legal risks – failure to manage can expose employer to a variety of costly disasters

Why Monitor Employee E-mail?

- E-mail creates a *permanent* record: "delete" key is no panacea
  - 24% of organizations have had e-mails subpoenaed
  - 15%: have been involved in litigation triggered by e-mail
- Single most common form of discovery in litigation
  - People say the darndest things
  - And the plaintiffs' lawyers know it

Email #1

From: Hunsaker, Kevin
Sent: Monday, January 30, 2006 2:32 PM
To: Gentilucci, Anthony R.
Subject: phone records -- privileged communication

Hi Tony,

How does Ron get cell and home phone records? Is it all above board?

Kevin

Kevin T. Hunsaker
Senior Counsel
HP Legal Department
650 857-3079 (phone)
650 857-3710 (fax)
1220 8573079 (voicemail network number)

Email #2

-----Original Message-----
From: Gentilucci, Anthony R.
Sent: Monday, January 30, 2006 12:00 PM
To: Hunsaker, Kevin
Subject: RE: phone records -- privileged communication

The methodology utilized is social engineering, he has investigators call operators under some ruse, to obtain the call record over the phone, its verbally communicated to the investigator, who has to write it down. In essence the Operator shouldn't give it out, and that person is liable in some sense, Ron can describe the operation obviously better, as well as the fact that this technique since he, and others, have been using it, has not been challenged. I think its on the edge, but above board. We use pretext interviews on a number of investigations to extract information and/or make covert purchases of stolen property, in a sense, all under cover operations.

Tony

Email #3

From: Hunsaker, Kevin <kevin.hunsaker@hp.com>
Sent: Monday, January 30, 2006 12:33 PM
To: Gentilucci, Anthony R. <tony.gentilucci@hp.com>
Subject: RE: phone records – privileged communication

I shouldn't have asked . . . .

Kevin T. Hunsaker
Senior Counsel

Email That Should Never Have Been Sent

"As we are now preparing for potential litigation, I would recommend that we delete all emails relating to these topics as soon as possible after we read them, on both the sender and receiver levels. Emails are subject to legal discovery. The last thing we need is to have an incriminating email or note (like this one) fall into the wrong hands."

2005 Arizona whistleblower case
Verdict: $4.75 million

Payoff Investigation Involving Nevada Governor Jim Gibbons

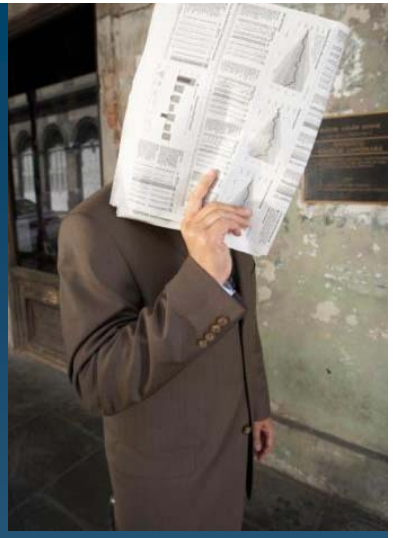
- Helpful spouse reminds software businessman not to forget the bribe:

  "Please don't forget the money you promised Jim and Dawn."

- His reply:

  "Don't you ever send this kind of message to me! Erase this message from your computer right now!"

Case Law Regarding Employee Privacy



- **General Rule: Comprehensive Policy will Defeat Expectation of Privacy**
  - No invasion of privacy where explicit policy stated computers were not for personal use and would be monitored "as deemed appropriate." *Thygeson v. U.S. Bancorp*
  - No invasion of privacy where employee signed acknowledgement of policy that company computer would be subject to monitoring/review "as necessary." *TGB Ins. Svcs. Corp. v. Superior Court*

BUT: Deficient Polices and Lax Enforcement Can Create a Right to Privacy!

- What about a policy displayed in log-in banner (employee sees it every time she logs in) ***explicitly*** stating that use of employer's system = consent to monitoring?

GOOD ENOUGH?

Not Necessarily!
Policy Failed to Defeat Expectation of Privacy Where…

- Policy described limited circumstances for monitoring
- Policy did not prohibit personal use
- Policy did not expressly disclaim right to privacy
- Practice did not put employee on notice of unannounced monitoring – U.S. v. Long, 64 M.J. 57 (CAAF 2006).

The Law is Unsettled

- *Even the Ninth Circuit has refused to weigh in!* (*Ziegler*)

Special Concern: Child Pornography and Other Criminal Behavior

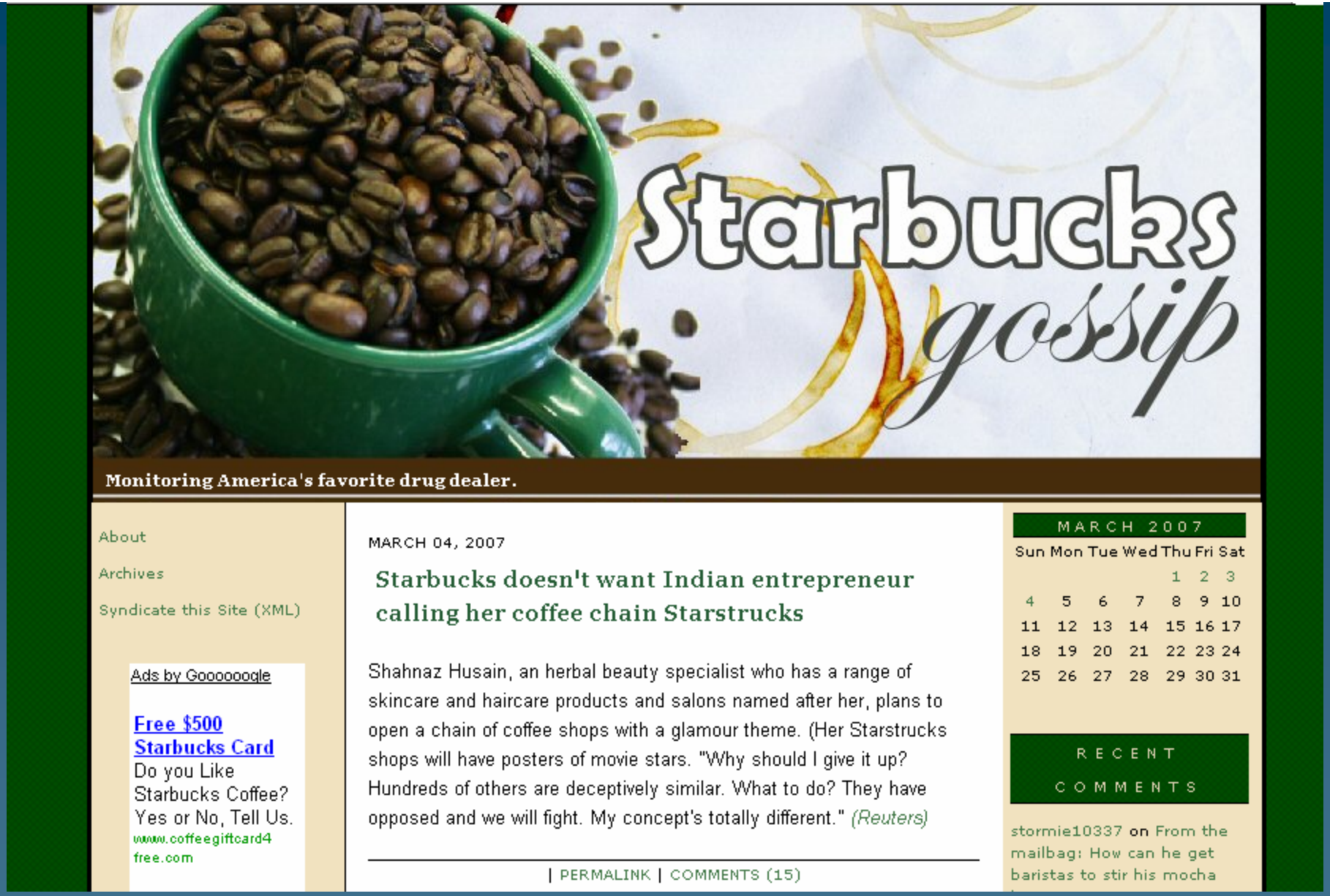
- No obligation to monitor employee computer use for specific purpose of detecting illegal activity
- May discover it during the routine monitoring
- Specific obligations with respect to child pornography – contact counsel immediately and do not handle it or send it anywhere

Use of Employer's Systems and Resources for Union Matters

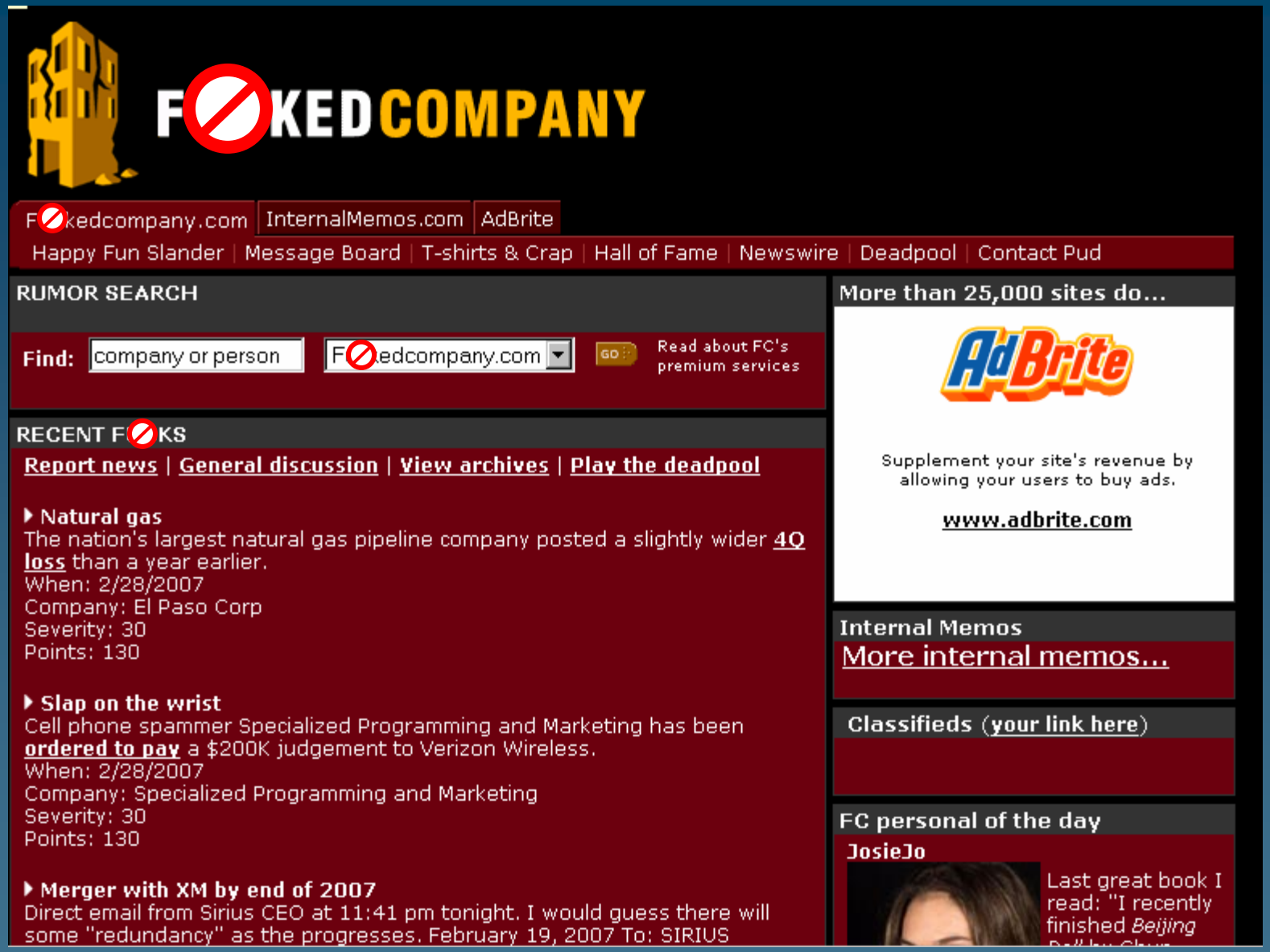
- Section 7 of NLRA: Right to Engage in Concerted Activity
- Section 8 of NLRA: Prohibits Employers from Infringing on Section 7 Rights
  - Does this give employees the right to use employer's computer system to communicate about union matters despite a general non-solicitation policy?
  - **Stay Tuned**: NLRB will address this issue on March 27, 2007

Employee Blogging

- Currently 68.9 million blogs
- With an estimated 1.6 million posts per day
- **Huge** potential for employer liability
  - Lost productivity
  - Leaked trade secrets and other information
  - Lawsuits
- Yet, only 7% of organizations have policies governing blog use and content!



Perkins Coie



Perkins Coie

INTERNALMEMOS

THE INTERNET'S LARGEST COLLECTION OF CORPORATE MEMOS AND INTERNAL COMMUNICATION

SUBMIT NEW MEMO | VISIT F[redacted]EDCOMPANY.COM

Find: Company or keyword GO

Memos online: 2401 | Next Page

COMPANY	MEMO	SIZE	DATE
GMAC	$ No 2006 bonus or raise!! The below memo was released today (2/15/07) from Bruce J. Paradis, CEO GMAC ResCap. What a piece of [redacted]liar and piece of [redacted] company.	2007	2/15/2007
Sprint Nextel	$ Top brass should walk the plank ASAP SPRINT NEXTEL MANAGEMENT SHOULD S TEP DOWN; REITERATE NEUTRAL RATING Date: January 16, 2007 Analyst: Patrick J. Comack, ...	28176	2/10/2007
Neteller	$ Neteller offers voluntary resignation packages In anticipation of this reduction, we would like to extend to IT/Product departmental employees the option of voluntarily resigning from NT ...	1177	2/7/2007
KodakGallery.com	$ Kodak Blurry on Protecting user photos On Friday, Kodak Gallery notified numerous users that due to their Web marketing campaign, 25 thumbnail photos belonging to a number of thei...	2762	2/4/2007
Dell	$ Dell Aborts Bonuses, Warns of Tough Times To: Dell Team Members Worldwide From: Michael We held a meeting this morning with our Vice Presidents and Dire...	6587	2/2/2007
EMAP plc	$ Possible Closures on the Way Back in November last year, I wrote to all of you regarding Magazines 2010 and I promised to update you in January. For the past ...	1779	1/24/2007
Bitpass	$ Bitpass is Discontinuing Service Dear Valued Bitpass Buyer, We want to thank you for your past business, however due to circumstances beyond our control, we are d...	1014	1/19/2007

Even the CEO Is Not Immune

PUGET SOUND Business Journal

JANUARY 26-FEBRUARY 1, 2007 · VOL. 27, NO. 41 · SEATTLE.BIZJOURNALS.COM · $2.00

Business Leaders Get It.

Blogofear

CEO blogs spark rumors by telling way too much

By ERIC ENGLEMAN
STAFF WRITER

Andy Sack, the chief executive of Seattle shopping Web site Judy's Book Inc., once attended a board meeting of a company that was deciding whether to raise more venture capital or sell itself.

Intrigued, Sack wrote about the meeting later that day in his personal blog. He figured it was OK as long as he didn't name the company.

But someone who knew Sack served on the board saw the post, and soon rumors of a sale began to fly.

"Within four hours, I got a phone call from the CEO, going 'What the (heck) are you doing?'" Sack recalled. "He was really upset."

Sack quickly deleted the offending entry.

A handful of CEOs of young, local Internet companies are embracing the Web's spirit of openness by maintaining their own Web logs, or blogs, to record their thoughts on everything from business matters to favorite films and music.

"I got a phone call from the CEO, going 'What the (heck) are you doing?'"

Andy Sack, Judy's Book CEO, on the response to his blog post revealing that another company might put itself up for sale

▼

But many CEOs are finding that the desire [illegible] parency and accessibility isn't always with an execu[illegible] Indeed, just have lea[illegible] post[illegible]

Perkins Coie

Best Practices: Employee Use of Communications and Electronic Resources

- **Notice**
  - Comprehensive policy addressing ALL forms of electronic communication and use of electronic resources (blogs, IMs, e-mail)
  - Explicitly disclaiming a right to privacy in the employer's electronic communication systems
- **Consent**
  - Signed acknowledgment
- **Implementation**
  - Regular training and routine enforcement

Workplace Investigations and the FCRA

- Investigations by third-party credit reporting agencies must comply with FCRA
- **Proper notice to employee?** *See chart in handout…*
  - Background check
    - Consumer Report vs. Investigative Consumer Report
  - Workplace investigation
- **Proper destruction of information?**

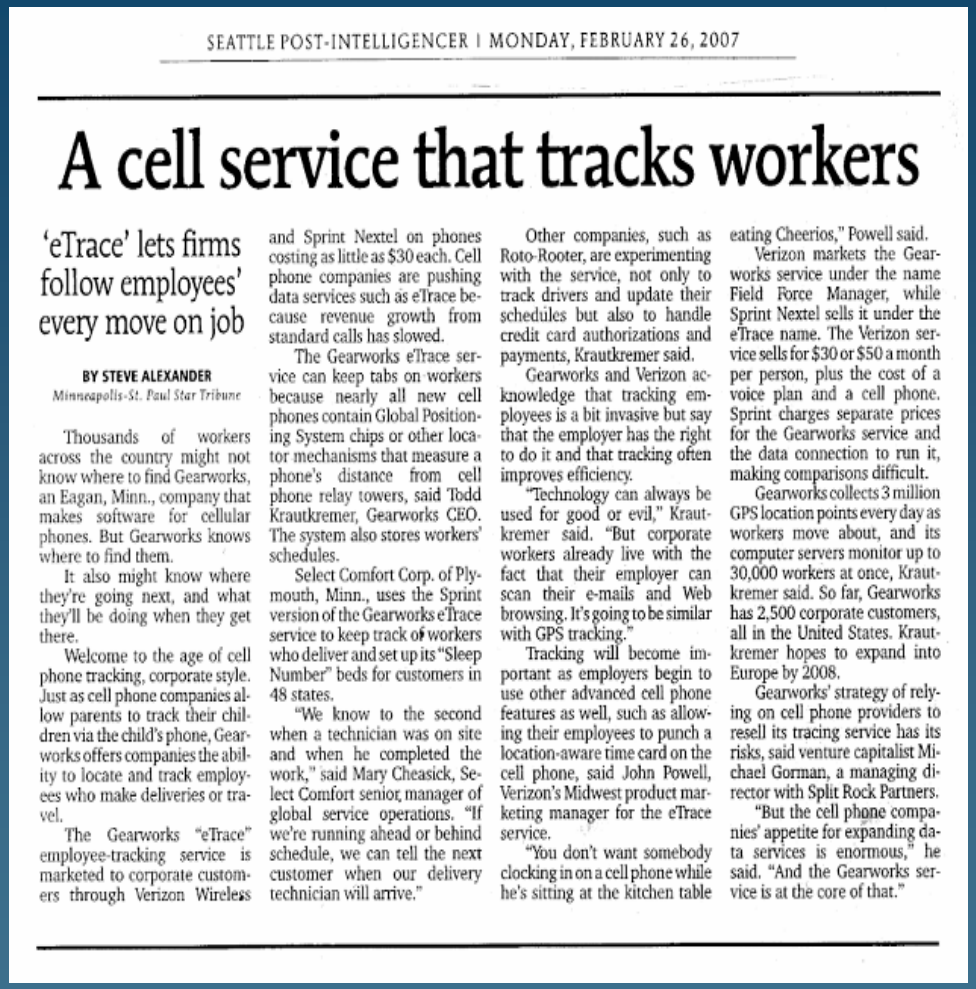
Electronic Surveillance

- Why?
  - Convenient, cost effective and generally effective way to evaluate performance, investigate misconduct, monitor productivity
- Potential Liability
  - Fourth Amendment to the U.S. Constitution
  - Common law tort of invasion of privacy

How Can You Monitor? You May Be Surprised ...

- Companies are no longer limited to video and photos! They can also:
  - Locate employee vehicles
  - Locate employee phones, Blackberries and other wireless devices
  - Track employees with RFID tags (tiny tracking devices in cards, badges and anything else)
  - Use event data recorders in vehicles
  - Use advanced photo integration techniques

Example of Cell Phone Tracking: eTrace



SEATTLE POST-INTELLIGENCER | MONDAY, FEBRUARY 26, 2007

A cell service that tracks workers

'eTrace' lets firms follow employees' every move on job

BY STEVE ALEXANDER
Minneapolis-St. Paul Star Tribune

Thousands of workers across the country might not know where to find Gearworks, an Eagan, Minn., company that makes software for cellular phones. But Gearworks knows where to find them.

It also might know where they're going next, and what they'll be doing when they get there.

Welcome to the age of cell phone tracking, corporate style. Just as cell phone companies allow parents to track their children via the child's phone, Gearworks offers companies the ability to locate and track employees who make deliveries or travel.

The Gearworks "eTrace" employee-tracking service is marketed to corporate customers through Verizon Wireless and Sprint Nextel on phones costing as little as $30 each. Cell phone companies are pushing data services such as eTrace because revenue growth from standard calls has slowed.

The Gearworks eTrace service can keep tabs on workers because nearly all new cell phones contain Global Positioning System chips or other locator mechanisms that measure a phone's distance from cell phone relay towers, said Todd Krautkremer, Gearworks CEO. The system also stores workers' schedules.

Select Comfort Corp. of Plymouth, Minn., uses the Sprint version of the Gearworks eTrace service to keep track of workers who deliver and set up its "Sleep Number" beds for customers in 48 states.

"We know to the second when a technician was on site and when he completed the work," said Mary Cheasick, Select Comfort senior manager of global service operations. "If we're running ahead or behind schedule, we can tell the next customer when our delivery technician will arrive."

Other companies, such as Roto-Rooter, are experimenting with the service, not only to track drivers and update their schedules but also to handle credit card authorizations and payments, Krautkremer said.

Gearworks and Verizon acknowledge that tracking employees is a bit invasive but say that the employer has the right to do it and that tracking often improves efficiency.

"Technology can always be used for good or evil," Krautkremer said. "But corporate workers already live with the fact that their employer can scan their e-mails and Web browsing. It's going to be similar with GPS tracking."

Tracking will become important as employers begin to use other advanced cell phone features as well, such as allowing their employees to punch a location-aware time card on the cell phone, said John Powell, Verizon's Midwest product marketing manager for the eTrace service.

"You don't want somebody clocking in on a cell phone while he's sitting at the kitchen table eating Cheerios," Powell said.

Verizon markets the Gearworks service under the name Field Force Manager, while Sprint Nextel sells it under the eTrace name. The Verizon service sells for $30 or $50 a month per person, plus the cost of a voice plan and a cell phone. Sprint charges separate prices for the Gearworks service and the data connection to run it, making comparisons difficult.

Gearworks collects 3 million GPS location points every day as workers move about, and its computer servers monitor up to 30,000 workers at once, Krautkremer said. So far, Gearworks has 2,500 corporate customers, all in the United States. Krautkremer hopes to expand into Europe by 2008.

Gearworks' strategy of relying on cell phone providers to resell its tracing service has its risks, said venture capitalist Michael Gorman, a managing director with Split Rock Partners.

"But the cell phone companies' appetite for expanding data services is enormous," he said. "And the Gearworks service is at the core of that."

- Just one of several companies – can monitor up to 30,000 employees at once
- Inexpensive – approximately $30-50 per employee per month

Perkins Coie

What Does Monitoring Actually Look Like?

- Maps and reports
- Detailed reporting: when, where, for how long
- Mobile time reporting
- Location-based clock-ins

Perkins Coie

Limits on Electronic Monitoring

- Does the employee have a reasonable expectation of privacy?
- If so:
  - Private employers: is it highly offensive to a reasonable person?
  - Public employers: Is it not for work-related purposes, or "unreasonable?"
- If yes to both questions: liability

Did the Employee Have a Reasonable Expectation of Privacy?

- Employees did have a reasonable expectation of privacy in:
  - Locker room, restroom stall, nurse's office
- Employees did not have a reasonable expectation of privacy in:
  - Shared office space, public place, open and undifferentiated work area, area accessible to others, car in public view

Special Concerns: Audio Surveillance

- Generally – Employers free to use video surveillance as long as the employee does not have a reasonable expectation of privacy
- **But:** *Adding audio increases employer liability dramatically*
  - Electronic Communications Privacy Act
  - Washington Privacy Act
- **TIP:** Nearly all video surveillance equipment includes audio capabilities – ensure (either self-check or contact company responsible for overseeing surveillance) audio function is disabled before commencing surveillance

Special Concerns: Surveillance and the NLRA

- According to the National Labor Relations Board
  - It is an unfair labor practice to engage in surveillance (or appear to engage in surveillance) of employees' organizing activities
- This could impact an employer's general right to monitor open and undifferentiated work areas
- **TIP**: Surveillance during union organizing campaigns should be reviewed with labor counsel

Special Concerns: "Pretexting"

- What is it?

-----Original Message-----
From: Gentilucci, Anthony R.
Sent: Monday, January 30, 2006 12:00 PM
To: Hunsaker, Kevin
Subject: RE: phone records -- privileged communication

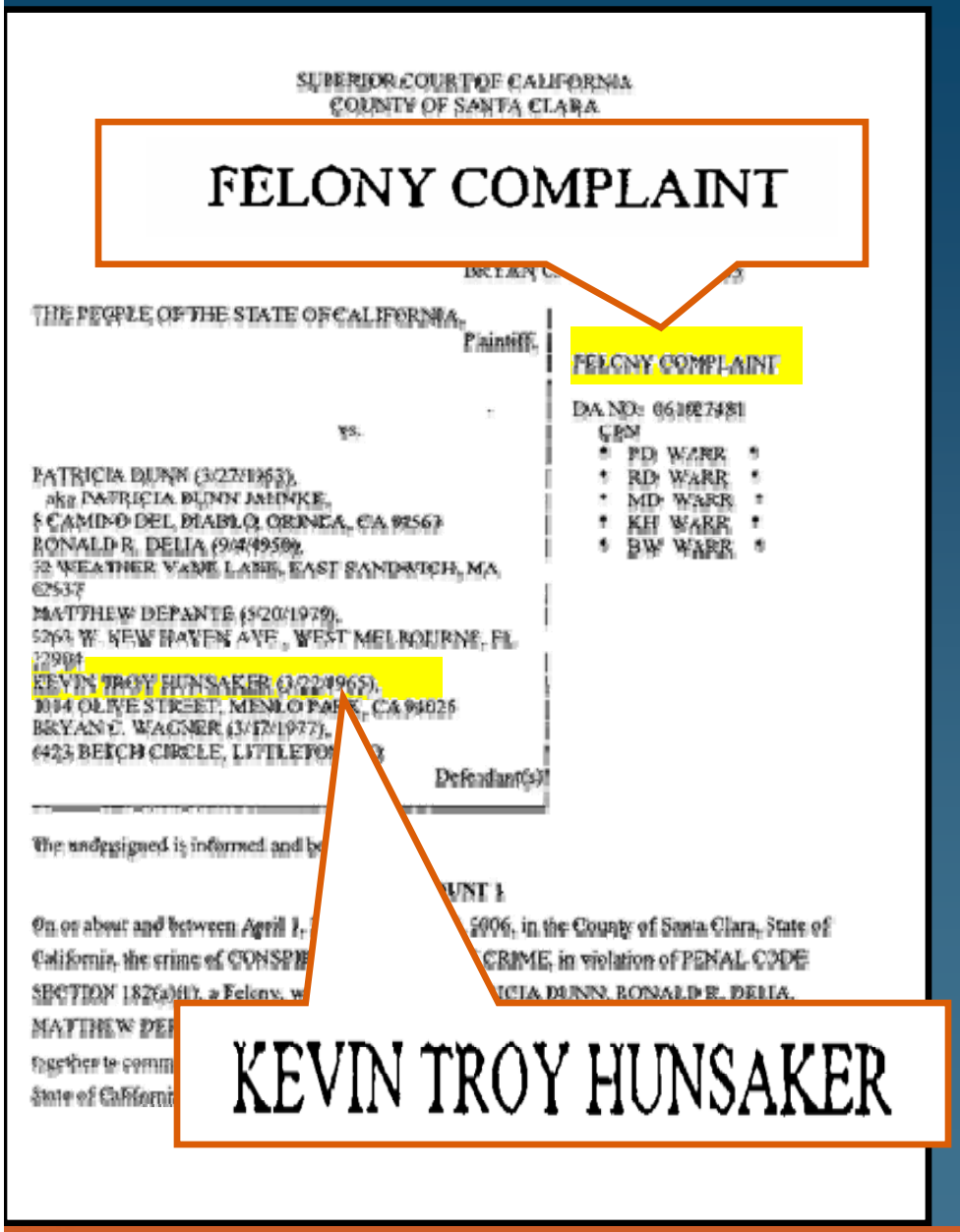
The methodology utilized is social engineering, he has investigators call operators under some ruse, to obtain the call record over the phone, its verbally communicated to the investigator, who has to write it down. In essence the Operator shouldn't give it out, and that person is liable in some sense, Ron can describe the operation obviously better, as well as the fact that this technique since he, and others, have been using it, has not been challenged. I think its on the edge, but above board. We use pretext interviews on a number of investigations to extract information and/or make covert purchases of stolen property, in a sense, all under cover operations.

Tony

Special Concerns: "Pretexting"

- Why do employers need to worry about pretexting?
  - HP Scandal -- huge damage to reputation, civil and criminal lawsuits
  - Congressional hearings, civil and criminal charges brought under general theories
    - $14.5 Million Settlement
    - Criminal Charges Still Pending

"Pretexting"


SUPERIOR COURT OF CALIFORNIA
COUNTY OF SANTA CLARA

FELONY COMPLAINT

THE PEOPLE OF THE STATE OF CALIFORNIA,
Plaintiff,

vs.

PATRICIA DUNN (3/27/1963),
aka PATRICIA BLOOM JAHNKE,
5 CAMINO DEL DIABLO, ORINDA, CA 94563
RONALD R. DELIA (9/4/1958),
32 WEATHER VANE LANE, EAST SANDWICH, MA 02537
MATTHEW DEPANTE (8/20/1979),
5263 W. NEW HAVEN AVE., WEST MELBOURNE, FL 32904
KEVIN TROY HUNSAKER (3/22/1965),
1014 OLIVE STREET, MENLO PARK, CA 94025
BRYANT C. WAGNER (3/17/1977),
6423 BEECH CIRCLE, LITTLETON
Defendant(s).

FELONY COMPLAINT

DA NO: 06102481
CRN
PD WARR
RD WARR
MD WARR
KH WARR
BW WARR

The undersigned is informed and

UNT 1

On or about and between April 1, 2006, in the County of Santa Clara, State of California, the crime of CONSPI CRIME, in violation of PENAL CODE SECTION 182(a)(1), a Felony, w ICIA DUNN, RONALD R. DELIA, MATTHEW DE together to comm State of Californi

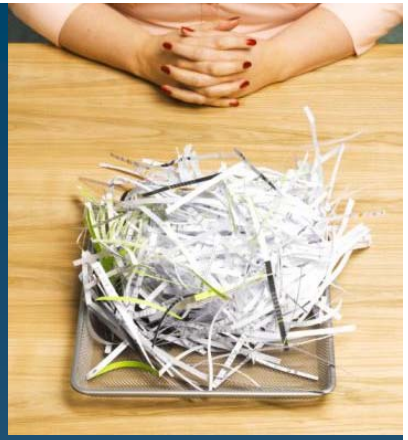
KEVIN TROY HUNSAKER

- Felony arrest warrants tend to be unpleasant. Don't let this happen to you!
- New federal law, several state laws prohibit pretexting
- Also be defensive – implement appropriate means to authenticate those requesting access to personal information

Privacy and Security of Employees' Personal Information

- Businesses must protect personal information of employees from unauthorized use, collection and disclosure
- Security obligations arise from:
  - Statutory/regulatory requirements
  - Industry guidelines
  - General duty of care to employees

Security Policies and Safeguards Necessary, But Not Sufficient



- Recent survey:
- 84% of respondents' companies have information security policies, BUT:
  - 88% who transfer customer data outside organization use email to do so
  - 22% lend portable devices on which they store work documents to colleagues
  - Significant percentage of companies don't scan outbound email

Medical Records Confidentiality

- General principles for collecting, storing, and disclosing employee medical information:
  - Collect only for authorized purposes
  - Store in separate medical file (no email, no flash drives, no laptops)
  - Restrict access and disclosure to statutorily authorized recipients
  - Shred paper and wipe hard drives

Social Security Numbers

- Social Security numbers are one of the most sensitive pieces of personal information
- Employers need to collect them (benefits, taxes, etc.), but they need to be protected
- Various state laws impose specific requirements

What Practices Are Prohibited?

- More than most companies think!
- Under state laws, the following are just a few examples of prohibited practices (exceptions may apply):
  - Printing SSNs on ID cards, badges, etc.
  - Requiring transmission of a SSN (including by email) unless encrypted or over secure connection
  - Printing an SSN on any materials that are mailed to an individual unless law requires it
- More state laws in pipeline

Stolen Laptops, Hackers and Security Flaws:
Responding to Data Theft and Unauthorized Access

- Not just your customers' personal information
- More a question of <u>when</u> than <u>if</u>
- When a breach occurs, the maelstrom will take all of a company's attention
- Prepare incident response team *now*

Not Just Hackers ...

Ten most recent posted incidents on site tracking data losses (attrition.org):

- **Japan Post** (Bag containing personal information on 290,000 customers stolen)
- **National Australia Bank** (Names and account numbers of 397 people sent to wrong addresses)
- **Worcestershire County Council** (Banking details, names, and addresses of 19,000 on stolen laptop)
- **Rabun Apparel** (1,006 names and SSNs of former employees posted to internet)
- **Speedmark** (35,000 notified about SSNs, names, and addresses on stolen computer)
- **Georgia Tech University** (SSNs, names, and addresses of 3,000 accessed through compromised account)
- **Back and Joint Institute of Texas** (Hundreds of medical records with SSNs found in trash behind building)
- **Stop & Shop** (Unknown number of consumers' credit and debit card data stolen by skimmers)
- **Seton Family of Hospitals** (SSNs, names, and dates of birth for 7,800 on stolen laptop)
- **Clarksville-Montgomery County Schools** (TN) (633 SSNs inadvertently placed on web site)

What? The CFO's Laptop Was Stolen?

Perkins Coie

Initial Security Breach Response

- Close off the breach; initiate incident response plan
- Notify, cooperate with law enforcement
- Prepare employee liaisons/PR/management to address it
- Preserve evidence
  - Recommendation: involve legal counsel
- Document everything

Security Breach Notification Laws

- If any unauthorized access to certain types of personal information takes place – not not just by third parties, and not just if your systems are "hacked" – 37 state laws now require notice to affected persons
- Financial companies: interagency guidelines for breach notification
- Federal legislation likely

Trigger for Notice Obligations

- Generally: name + SSN, driver's license or ID card number, or financial account number with PIN (or other code)
- No breach if encrypted (all states) or redacted (several states)
- **HINT: encrypt!**
- Only applies to "electronic" information in all but a handful of states

Notice Obligations

- Notice may not be required for all employees
- State AGs: possible unfair practice if fail to notify residents of those states
- Best practice: if required to notify some, notify all
- Most states: postal mail, email (E-SIGN compliance required) or, if enough persons affected, "substitute notice" (generally email + notice to media + notice on Web site)

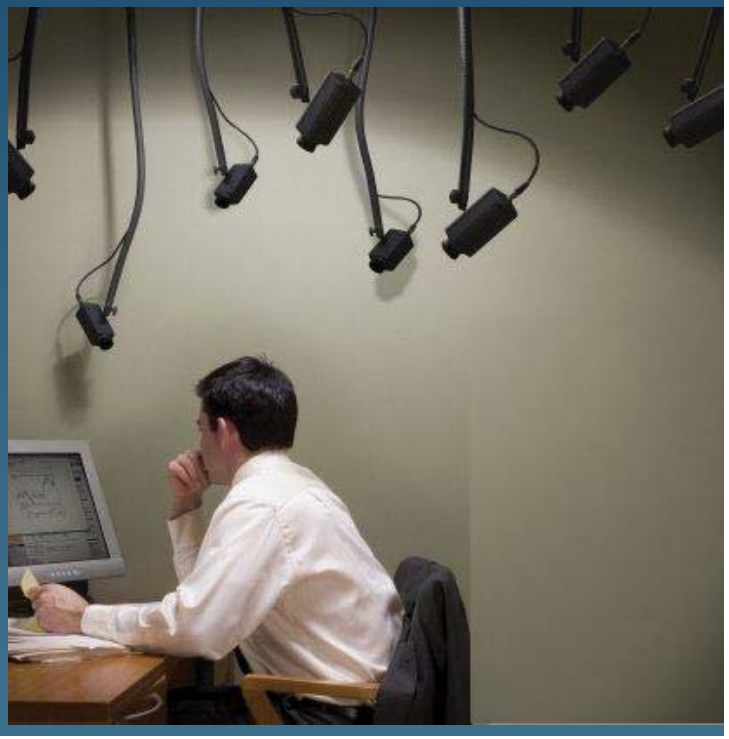
Other Notice Considerations

- Others you may need to notify:
  - Credit card brands (e.g., Visa/MasterCard)
  - State AGs and state agencies
  - Credit reporting agencies
  - Secret Service (financial/payment information)
- Wording of notice
  - Expect it to be posted online within hours
  - Exhibit A in negligence suit

Employee Relations

- Maintain workplace morale
  - Make sure all concerns are addressed
  - Assist with all claims of ID theft
  - Consider fraud protection insurance for employees
  - Inform them of fraud alerts or victim alerts
  - Credit freezes
- Maintain a record of dealings with employees

ANY QUESTIONS?



Perkins Coie