SIDLEY AUSTIN LLP

SIDLEY

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

Employee Homework:

The Next Compliance Frontier

Alan Charles Raul

Sidley Austin LLP

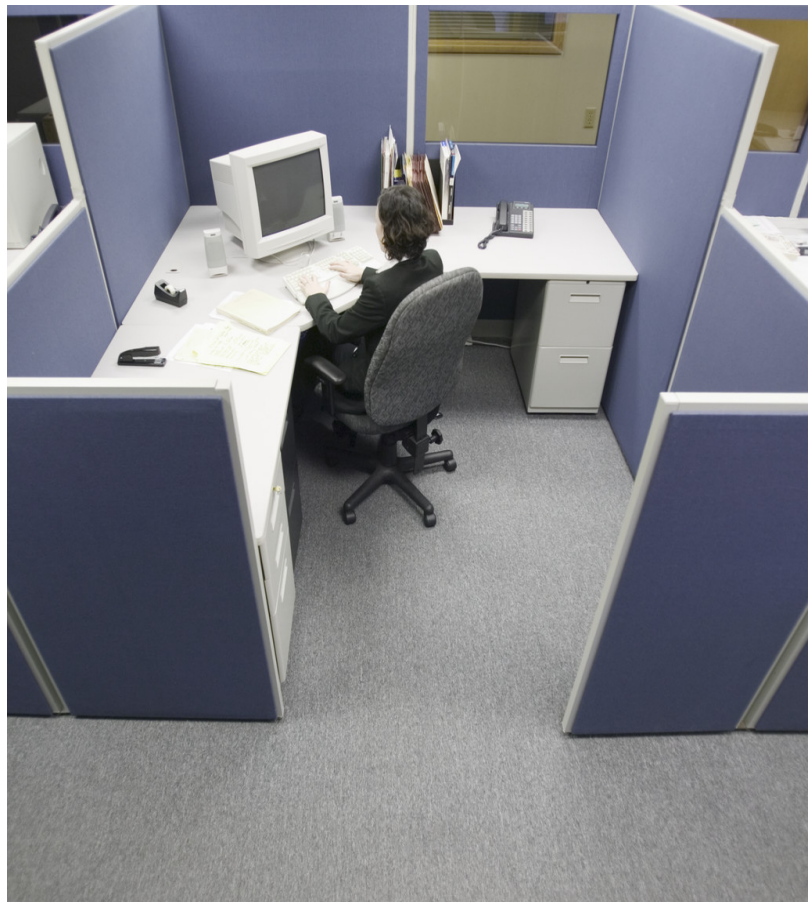
January 18, 2008

What's Going On?

- 19.8 Million Americans work from home at some point during the week. (Bureau of Labor Statistics)
  - 15% of Total Workforce
- Telecommuting occupations typically involve information handling and professional/knowledge-related tasks. (US GAO)
- Flexible workforce = Productive workforce = Happy workforce?
- Dep't of Labor "strongly supports telecommuting and telework. Family-friendly, flexible . . . benefit . . . employees, families, employers, and society as a whole." OSHA 2/25/00

The Traditional Office

- All resources, supplies, equipment and “time” belong to employer
  - Personal activity not facilitated or tolerated in workplace
  - All work performed “in the office” or “on the road” during business travel
  - Permissible applications carefully prescribed and governed by all-knowing, super-helpful IT Department.
  - Coats, ties, dresses . . . .



The new workplace squeezes personal and professional lives closer together

ABC News: *From Pensions to Parenthood: Working at Home: Tips, Tricks and Solutions on Finding a Balance While Working at Home*, July 25, 2007.

Is It a Brave New World, or a Diffident One?

- The home office is *terra incognita* for privacy explorers
- Top issue for HR professionals in 2008
- Subset of workplace privacy but not much existing guidance
- Compromises are inevitable
- Less discipline at home?
- Murky answers for both sides because of mutual interest in promoting efficiency and convenience, and not getting too creepy about what goes on at home

The movable workplace is a function of:

- Operating in the space between business casual and pajamas . . .
- Universal imperatives of flexibility, efficiency, convenience and productivity
- Power of Internet
- Device and service hopping
  - Laptops
  - Cell phones
  - Home broadband connections
  - Portable media like USB drives
  - VPNs
  - BLACKBERRIES! (. . . and other PDAs)
- Superiority of personal resources over bureaucratic IT
  - GOOGLE!
- Multi-tasking, Balancing, Juggling . . . . .

Questions Raised by the Merger of Professional and Personal

- Where does professional sphere intersect with personal?
- What are risks to employers?
- What are risks to employees?
- What are current applicable legal rules?
- Are there any new rules on the horizon?
- Who should be responsible for preserving employee privacy in shared space?
- Are best practices apparent?
- What policies should companies adopt?
- What should employees do to protect themselves?

What Are The Risks To Employers?

- **Unsecured Networks / WiFi Hot Spots**
  - Vulnerable to Hackers

"Computing in the Cloud"?

Provider's data center holds data traditionally stored on end user's computer.

- Does third party access compromise:
  - confidentiality
  - security
  - privilege
  - 4th Amendment rights

More risks.

- Loss of productivity
  - Web-surfing, online shopping, personal networking sites
- Wasted Bandwidth
- Computer and Data Security
    - Malware, Viruses, Hackers, Unintended transmissions
- Ensuring compliance with law and company policies
- Trade secret and proprietary leaks

The risks arise because . . . .

- Challenges to Information Security:
  - Mobility of intangible assets
  - Easy replication of data
  - Easy deletion of data
- Home is inherently less secure
  - No badges
  - No property tags
  - No peer pressure
  - No guards (just dogs waiting to eat homework)
  - No single-minded focus on best interests of employer

The risks are not hypothetical

- Pfizer Data Breach
  - Employee takes work laptop home.
  - Spouse downloads file sharing software/malware.
  - Company information assets uploaded to thieves.
- Veteran's Affairs Data Breach
  - Employee takes laptop home (in violation of VA policies).
  - Employee's home burglarized, computer stolen.
- Ohio Data Breach
  - Intern instructed to take Backup Tapes home each night for business continuity.
  - Tapes stolen from intern's car

Still more risks:

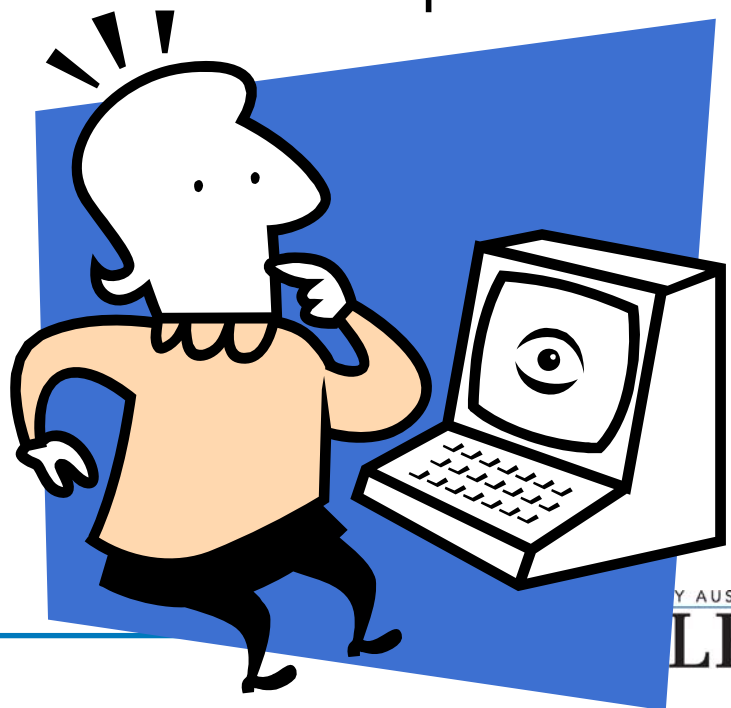
- Loss of control over matters for which employer legally responsible
- Losing track of responsive documents
- Spoliation
  - Court dismissed employee's claims for erasing data on a hard drive, even though he knew he had a duty to preserve, to get rid of traces of porn. Leon v. IDX Systems. (9th Cir. 2006)

Risks are definitely NOT hypothetical!

- Employee's Misconduct
  - 26% of employers fired workers for misusing the internet
  - 25% fired employees for e-mail misuse
  - 76% of employers monitor worker's website connections
    - AMA/ePolicy Institute, 2005 Electronic Monitoring & Surveillance Survey.
  - Consider: Employer of child pornographer liable to victims.
    - Company's discovers employee accessing porn on company computer, investigates, fails to discover child porn
    - Company has a duty to thoroughly investigate, notify authorities
    - (Doe v. XYZ Corp.)

What Are The Risks To Employees?

- Surveillance at home is especially creepy
- Monitoring cannot easily distinguish what is personal
- Commingling office and personal confidential information is inevitable
- Compromising confidential information of spouses and family members is possible



Confusing situation for employees too.

- Recurring Theme of Modern Life: Privacy v. Efficiency
  - Amazon, targeted advertising, GPS, and now: the home office
- Employer has obvious interest and right to monitor its network and protect information assets regardless of location
  - How do company policies apply at home?
  - Is employer obligated to manage home “worksites”?
    - OSHA guidance does not require employer inspections of home offices and “will not hold employers liable for employees’ home offices.” OSHA 2/25/00

There are many tricky situations

- Employee sends personal emails to attorney from work: No automatic waiver of privilege. Depends on reasonable expectation of privacy based on company's email policies and actual monitoring
  - *In re Asia Global Crossing*
- Employee emails attorney on home office computer used for company business: Employee retained privilege because computer was not connected to employer server and not located at employer's office; employer could not monitor at any time.
  - *Curto* v. *Medical World Communications*

Reasonable Expectation of Privacy

- Employer must not invade privacy by committing tort of "intrusion upon seclusion" (which would be highly offensive to reasonable person)
- Expectation of privacy depends on employee's subjective expectation of privacy that is objectively reasonable
- Employer's policies can defeat expectations of privacy, but practices must be consistent with policies
- In absence of clear policy, legitimacy of privacy expectation will depend on circumstances and "operational realities"
- Employee's actions to protect privacy would tend to subjective expectations
- Working from home will allow greater expectations of privacy to develop

What Are The Key Questions?

- What media are being investigated?
- Real time or stored communications?
- Bona fide business purpose?
- What techniques are used?
- Did employer policies provide notice and advance warning?
- Was employee consent obtained? Coerced?
- Reasonable purposes? Reasonable scope?
- Are there minimization procedures and good controls on access, use and disposal?
- Is employee in Europe (or outside US)?

What Legal Rules Apply To Employee Privacy?

- **Basic Rule:** Employers may access employee communications on company systems.
  - *Fraser* v. *Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d. Cir. 2003).
- **Variations on Rule:** Employee's reasonable expectation of privacy can undermine employer rights
  - Employee brings personal computer to work, connects to network and takes no measures to prevent 3rd party access: no reasonable expectation of privacy. *U.S*. v. *Barrows.*
  - Fact that employee owns or personally uses a computer not enough to make expectation of privacy reasonable
  - Employer policies and practices can defeat privacy expectations.
  - Lack of a policy or failure to routinely monitor computer usage can support expectation of privacy. *Leventhal* v. *Knapek*.

Legal Rules.

- Rules blur where personal equipment involved
  - "We hold that he also had a legitimate, objectively reasonable expectation of privacy in his personal computer."
  - "The salient question is whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network. We conclude under the facts of this case that the act of attaching his computer to the network did not extinguish his expectation of privacy..."
  - ***U.S.* v. *Heckenkamp*, 482 F. 3d 1142 (9th Cir. 2007).**

Legal Rules.

- Policies can defeat reasonable expectations of privacy

  – "[D]efendant must prove that he had a legitimate expectation of privacy in the place searched. …[B]ecause of the … 'Internet policy, [defendant] lacked a legitimate expectation of privacy in the files downloaded from the Internet. ... The policy clearly stated that FBIS would 'audit, inspect, and/or monitor employees' use of the Internet, including all file transfers, all web sites visited and all e-mail messages, as deemed appropriate....' [T]he warrantless remote search of defendant's computer and copying of files from his hard drive did not violate his Fourth Amendment rights." *United States* v. *Simons*, 206 F.3d 392, 398-401 (4th Cir. 2000)

What Do Employees *Expect*?

- **Read My E-Mail:** Low Expectations of Privacy: Only 38% expect privacy on corporate network. >50% expect privacy in Web-based emails used for work, even if used at home. (e.g., Gmail)
- **Social Networking:** Over 3/4ths expect privacy in corporate sponsored networking sites
- **It's called *My*Space:** Most employees believe it would violate privacy to check personal networking sites before employment decisions
- **Records:** Younger employees virtually unanimous that employers should not use legal/court history without prior consent
- **Consent Also Expected for:** Passwords, Health, Performance History, Sexual Orientation, Religion & Social Security Numbers
  - Ponemon Institute Survey, 2007-2008

Good consent vitiates rights, but . . .

- **Consent to a Search:**
  - In tort claim for intrusion upon seclusion, employee's consent to search home was invalidated because consent not informed, voluntary and free of coercion. Company liable for intrusion upon seclusion
  - *Wal-Mart Stores, Inc.* v. *Lee*, 74 S.W.3d 634 (Ark. 2002)
- EU laws strictly limit employee surveillance and rarely uphold employee consent (which is considered coerced)

Federal Legislation Affecting Employee Privacy

- **The Wiretap and Stored Communications Acts** (ECPA, 18 U.S.C. § 2510 *et seq.)* creates separate regimes for intercepted "real time" and stored communications, and forbids interceptions of electronic communications without party's consent
  - *But see*, *Fraser* v. *Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d. Cir. 2003).
- **FCRA** (15 U.S.C. § 1681 *et seq)* amended to allow employers to investigate employees suspected of misconduct without notifying in advance they are obtaining 'consumer report'
- **NRLA** (29 U.S.C. § 151 *et seq.*) preserving collective bargaining power of unions, and creating NLRB which stated employee surveillance is subject to collective bargaining

State Laws Affect Employee Privacy

- **State Constitutions**
  - *See, e.g.,* Cal. Const. art. I, § 1
  - State action not required to invoke constitutional right.
- **2-party Consent Wiretap Laws**.
  - *See, e.g.*, Cal Penal Code § 632.
  - Requiring both parties recorded consent to wiretap.
- **Employee Notice Requirements**
  - Conn. Gen. Stat. Ann. § 31-48d; Del. Code Ann. tit. 19 § 705.)
- **Wrongful Discharge liability**
  - Termination of at-will employee for reasons violating public policy.

State Laws.

- **State Law re: Employee Monitoring**
  - **CT and DE have statutes requiring employers to notify employees of workplace monitoring.**
    - Conn. Gen. Stat. Ann. § 31-48d; Del. Code Ann. tit. 19 § 705.
- **Tort Law**
  - **Privacy Torts:**
    - Intrusion Upon Seclusion
    - Publicity Given To Private Facts
    - Appropriation
    - False Light
  - **Intentional Infliction of Emotional Distress**
  - **Trespass to Chattels**

EU Limitations on Employee Monitoring

- French Law prohibits unannounced access to employee computers and e-mails, even where the employer owns the computer employees are advised against personal use of company equipment.
  - *Phillippe K.* v. *Cathnet-Science* (Cass. soc. 2005); *Nikon France SA* v. *Frederic O.* (Cass. soc. 2001).
- Unannounced monitoring of employee e-mails or Internet use is illegal in Greece, and can be criminally prosecuted.
  - See Christine Pirovolakis, *Greece Puts Stop to E-mail Snooping in Decision by Data Protection Authority*, Privacy Kaw Watch (BNA) (Feb. 7, 2005)

HIPAA Security Guidance for Home-Based Computers, PDAs, USB Drives, Etc. (12/28/06)

- Conduct risk assessment of remote access/offsite use of data
- Develop risk management policies and procedures to address vulnerabilities
- Three General Risks: Access, Storage & Transmission
- Ensure adequate:
  - Authorization/Authentication
  - Security for mobile devices & media
- Proper disposal
- Don’t leave devices unattended
- Prevent contamination of systems; use firewalls
- Security Awareness & Training.
- Create Security Incident Procedures

Best Practices

- Coordinate CPO, Legal, IT and HR
- Conduct risk assessment
- Establish express policies addressing personal/professional intersection
  - Manage expectations of privacy
  - Provide effective notice
  - Conform practices to policies
  - Establish practical boundaries
- Monitor employee privacy laws of relevant jurisdictions
  - Understand that US law may evolve
  - EU approach could be contagious
  - Determine whether labor or works council issues apply

Homework Policies

- Establish what equipment may be used
- Establish how and whether web mail and “cloud” applications may be used
  - Google Desktop? Online storage?
- Establish when and how data may be taken out of office
- Articulate right to access/monitor company assets, data and resources at non-office locations including home
- Establish tailored security measures and safeguards for home computing
  - Store data on encrypted USB drives
  - No work on computers with P2P software
- Consider obtaining written consent to policies in exchange for flexibility of working remotely

Homework Policies

- Consider periodic inventories of employee data at home
- Minimize movement of sensitive data
- Ensure proper disposal of home computers, PDAs, etc.
- Lock down computers at home, in cars, everywhere
- Remind employees that working at home is . . . work, and work information is subject to litigation demands
- Sensitize employees to security and behavioral risks
- Insist on compliance with incident notification and response obligations
- Provide employee training
- Manage privacy expectations
- Make sure employees know *they* are responsible to segregate home and office if they want to preserve privacy

Best Practices: For Workplace Searches (Home or Office)

- Provide advance notice of investigation/litigation uses when possible
- Document legitimate business purpose
- Do not monitor or search where not reasonably necessary to investigation (reasonable scope)
- Eschew real-time access unless legal compliance assured
- Do not use packet-sniffers or keystroke loggers unless well justified
- Restrict access to personal information acquired during investigation
- Limit data retention
- Provide clear instructions and controls to investigators
- Avoid disparate treatment of employees
- Allow as much transparency as possible
- Act reasonably; act in good faith
- Don’t shock anybody’s conscience

SIDLEY AUSTIN LLP

SIDLEY

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

Alan Charles Raul

Sidley Austin LLP

(202) 736 – 8477

araul@sidley.com