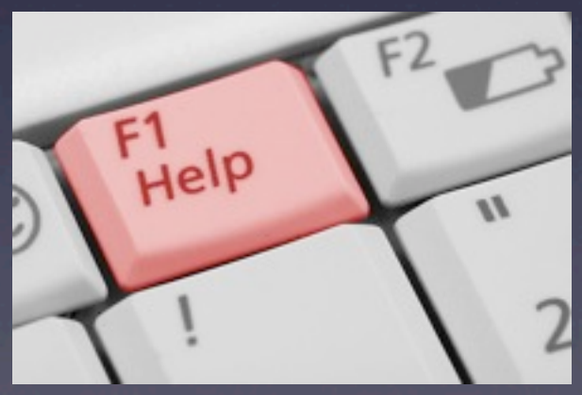
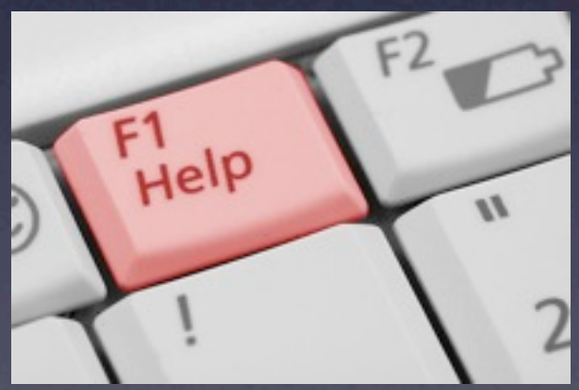
YOUR CORPORATE COMPUTER POLICIES



DORSEY
DORSEY & WHITNEY LLP

DO THEY ADDRESS RECENT LAW AND CURRENT TECHNOLOGY?



DORSEY
DORSEY & WHITNEY LLP

Four Key Areas

- Policies that enable companies to address recent changes in the law and technology so they can:
  - seek court intervention to protect their computer data and to prevent its dissemination
  - conduct expansive computer investigations
  - minimize labor and employment risks posed by the new social media
  - Cloud Computing

DORSEY
DORSEY & WHITNEY LLP

Computer Fraud and Abuse Act

- Title 18 U.S.C. § 1030 – Enacted in 1984
- Federal computer crime statute including data theft
- Civil remedy added in 1994 amendment
- Computers used in interstate commerce
- Amended in 2001 and 2008
- Computers in foreign countries
- Provides for damages and injunction

DORSEY
DORSEY & WHITNEY LLP

Key Element: 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…

DORSEY
DORSEY & WHITNEY LLP

Ways to Establish Lack of Authorization

- Violates company policies and rules
- Hacking by outsider who breaks into computer
- Exceeds expected norms of intended use
- Employee terminates Agency relationship with employer by disloyal conduct
- Access for non-business purpose

DORSEY
DORSEY & WHITNEY LLP

U.S. v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010)

- Court affirmed the CFAA conviction of a Social Security Administration employee
- Accessed social security information for personal reasons
- Violated Agency's policy against "obtaining Information from its databases without a business reason."

DORSEY
DORSEY & WHITNEY LLP

Authorization as Defined by Company Policies

- 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 limiting authorized access
- Agreements can set limits
- Similar to criminal trespass

DORSEY
DORSEY & WHITNEY LLP

Company Rules on Scope of Computer Access

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

DORSEY
DORSEY & WHITNEY LLP

Web Site 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)

DORSEY
DORSEY & WHITNEY LLP

Doe v. Darthmouth Hitchcock Medical Center (D.N.H. July 19, 2001)

- Hospital's Graduate Training Manual prohibited intern from accessing patient records absent need to know
- Hospital and resident sued
- Court dismissed hospital holding that it had been victimized by its "own policies" and that it would be inconsistent with the purpose of the CFAA to find the hospital vicariously liable for resident's actions

DORSEY
DORSEY & WHITNEY LLP

U.S. v. Nosal, 676 F.3d 854 (9th Cir. 2012)

- Korn Ferry executive indicted for stealing confidential information before leaving to join competitor

- CFAA does not extend to violations of use restrictions but is limited to circumvention of technological barriers

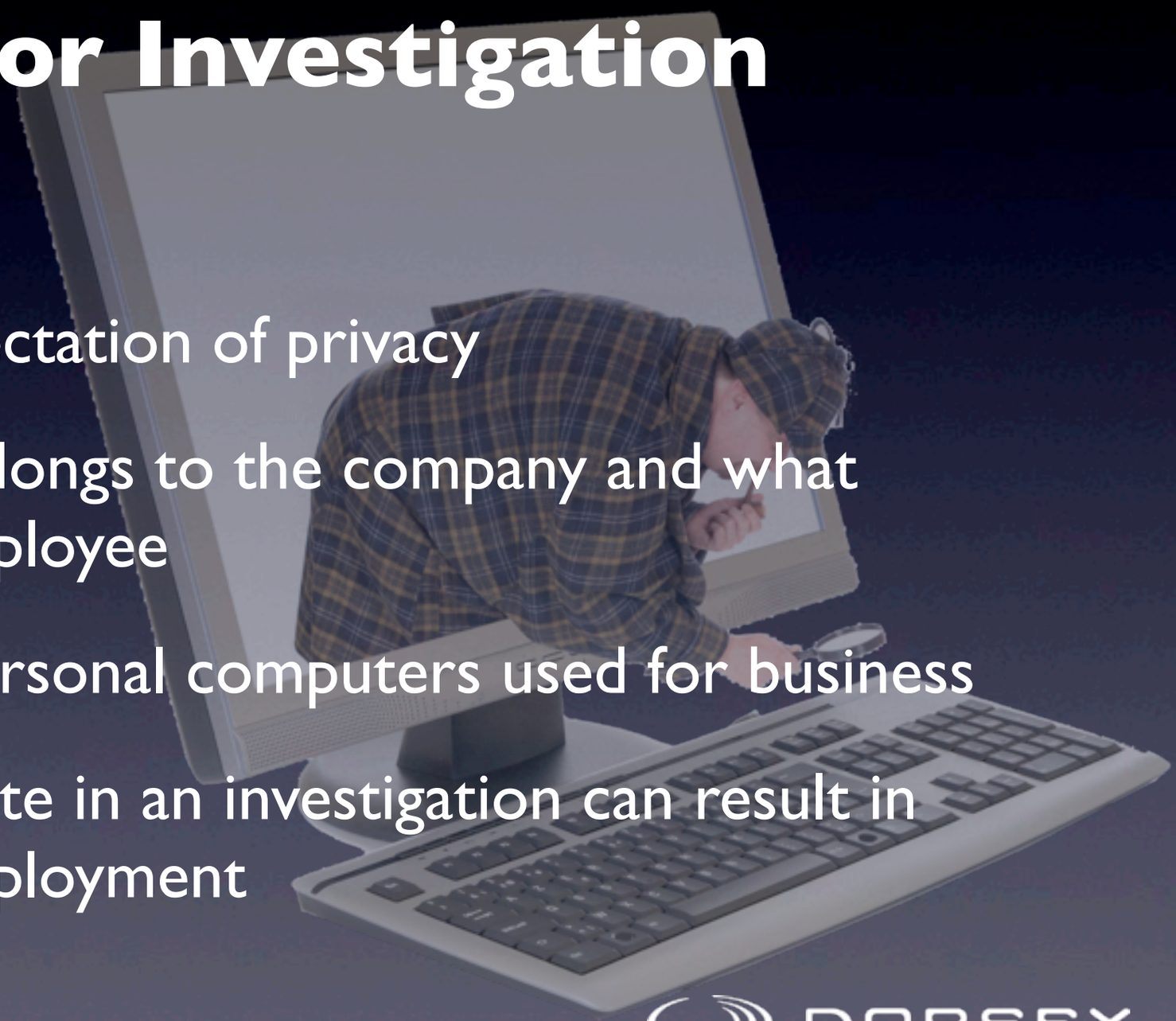
- Concern over criminalizing common violations of terms of use and rules

- Employees cannot access without authorization since they are authorized to use the company computers

- CFAA limited to outside hackers

DORSEY
DORSEY & WHITNEY LLP

Policies for Investigation



- Eliminate any expectation of privacy
- Delineate what belongs to the company and what belongs to the employee
- Right to review personal computers used for business
- Failure to cooperate in an investigation can result in termination of employment

DORSEY
DORSEY & WHITNEY LLP

City of Ontario, Ca. v. Quon (S.Ct. 2010)

- City's computer policy stated email and Internet usage would be monitored
- Police officers texted messages on City pagers
- Quon exceeded character limit and reimbursed the City rather than be audited
- An audit found Quon had texted sexually explicit messages and was disciplined

DORSEY
DORSEY & WHITNEY LLP

City of Ontario, Ca. v. Quon (S.Ct. 2010)

- 9th Circuit held there was a reasonable expectation of privacy based on employer's "operational realities"
- Supreme Court reversed holding that on the facts the search was reasonable despite expectation of privacy
- Highlights importance of employer's policies on technology use and the need for enforcing the policies

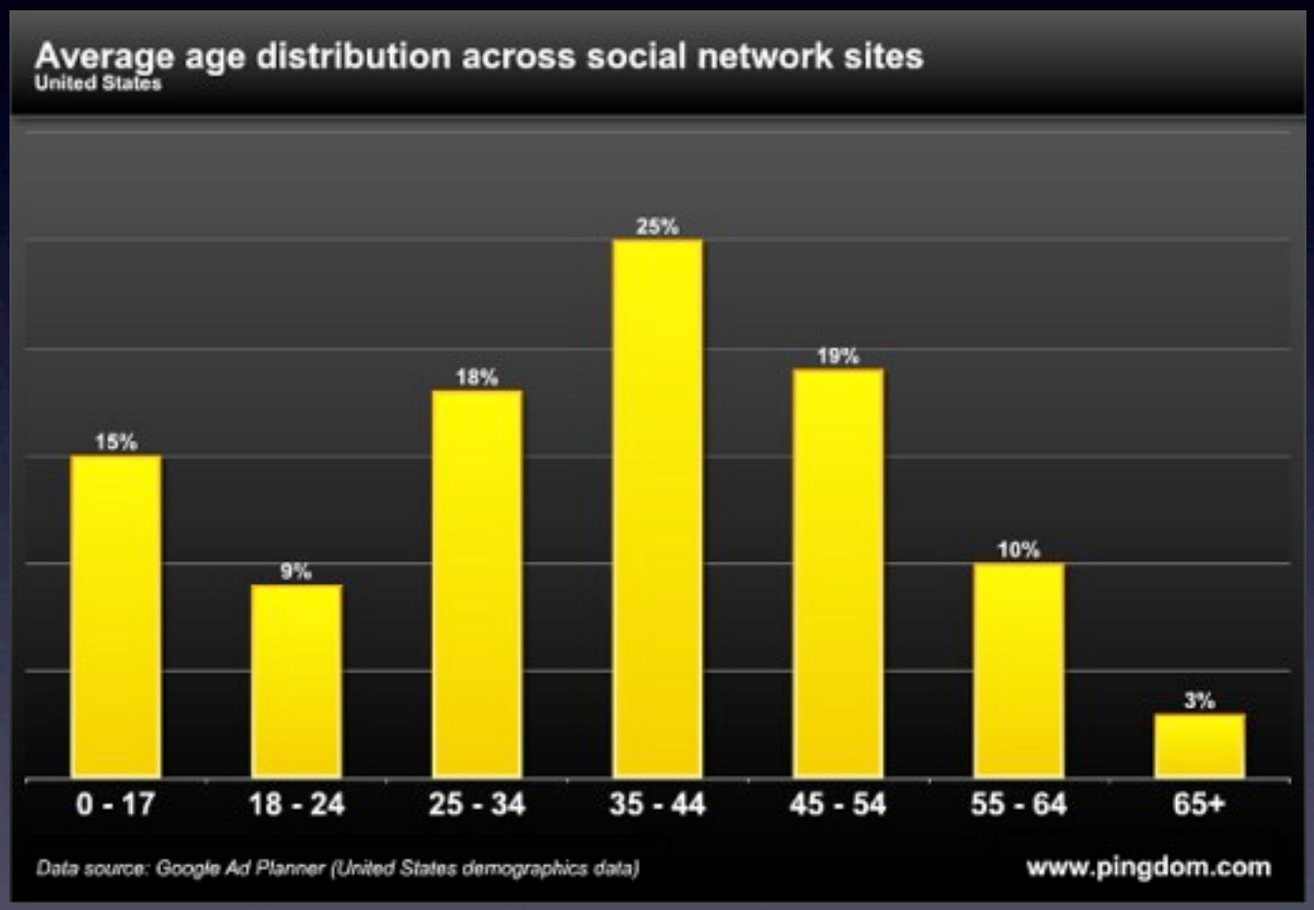
DORSEY
DORSEY & WHITNEY LLP

Policies Must Be Internally Consistent

- *Stengart v. Loving Care Agency*, (NJ Sup. Ct. 2010)
  - Employee emailed with company-issued laptop to personal counsel using personal, password-protected, Yahoo account
  - Policy that all emails were company records and that occasional personal use is permitted could lead employee to conclude personal emails would be private

DORSEY
DORSEY & WHITNEY LLP

Use of Social Networks



DORSEY
DORSEY & WHITNEY LLP

Areas of Legal Risk

- Invasion of Privacy
- Confidentiality
- Disciplining
- Harassment
- Background Checks
- Protected speech for labor organizing

DORSEY
DORSEY & WHITNEY LLP

Checking Employees

- Anti-Discrimination Laws if employment decisions are based on protected information discovered during searches
- Compliance with federal and state background check laws.
- Defamation considerations in providing/re-publishing non-neutral reference or employment information.
- Potential invasion of privacy if accessing non-public information or obtaining/using private information.

DORSEY & WHITNEY LLP

Invasion of Privacy

Yath v. Fairview Cedar Ridge Clinic (Minn. Ct. of Appeals 2009)

- Yath sought treatment at clinic for an STD.
- Clinic employee accessed Yath's records and revealed them to another employee
- Myspace page appeared with Yath's picture announcing that she had an STD
- Court said that the Myspace posting constituted "publicity" for an invasion of privacy claim for publication of private facts
- Clinic not found vicariously liable

DORSEY
DORSEY & WHITNEY LLP

Policies: Background Checks

- Type of information that may be collected
- How information is considered
- Who will conduct the searches
- No false information used to access a site
- Prohibition against discriminatory use of data
- Use as supplement to application process

DORSEY
DORSEY & WHITNEY LLP

Pietrylo v. Hillstone Rest. Grp. (D.N.J. 2008)

- Restaurant employees created an invitation-only Myspace group where employees could vent
- Management found out about,asked for password, viewed the page and fired two employees
- Employer found liable for violation of the Stored Communications Act

DORSEY
DORSEY & WHITNEY LLP

Protected Labor Speech

- NLRB filed complaint on behalf of ambulance company employee fired after using vulgarities to ridicule her supervisor on Facebook
- Company policy generally barred employees from depicting company on social media sites
- Case settled with company agreeing not to prohibit discussions of hours, wages and working conditions

DORSEY
DORSEY & WHITNEY LLP

Critical Policy Components

<u>Warn against postings about:</u>

- Confidential and proprietary information;
- Discriminatory statements;
  - Sexually explicit language or innuendos regarding co-workers, management, customers or vendors;
  - Defamatory statements
- Consider requesting disclaimer language
- Define acceptable use

DORSEY
DORSEY & WHITNEY LLP

Critical Policy Components

- Compliance with other company policies
- Define Organization's expectations for employee's use of his/her personal electronic devices
- Special Provisions regarding Social Media during work hours and outside of work hours

DORSEY
DORSEY & WHITNEY LLP

Critical Policy Components

- Instruct employees to identify themselves and make it clear when they are speaking on behalf of, or about, the Organization
- Define employee versus individual capacity (e.g., are any employees executive officers?) – liability
- Advise employees to seek advice from the law department or management when content is work-related
- Describe information that can or cannot be disclosed

DORSEY
DORSEY & WHITNEY LLP

Critical Policy Components

- Define Acceptable Use of company name
  - Appropriate references to the company, its clients,partner, customers and competitors
- Use of company's name, trademarks and other information
- Guidance regarding references to the company's products or services

DORSEY
DORSEY & WHITNEY LLP

33

CLOUD COMPUTING

DORSEY
DORSEY & WHITNEY LLP

CLOUD COMPUTING

DORSEY
DORSEY & WHITNEY LLP

Record Retention

DORSEY
DORSEY & WHITNEY LLP

Record Retention

- Schedule for retaining documents
- Inventory type, locations and format
- Cloud provider must be able to conform to company's document retention policy
- Cloud provider must be able to permanently delete obsolete records on a schedule

DORSEY
DORSEY & WHITNEY LLP

Electronic Discovery

- Ensure third party accessibility
- Avoid spoliation during pending lawsuit
- Enforce document holds
- Protect metadata
- Retrieve and search for relevant data
- Protect attorney client privilege
- Be aware of country where data is stored

DORSEY
DORSEY & WHITNEY LLP

Contract Protections

- Protection of data, auditing and security
- Customer control over data
- Provider control over data
- Responsibilities of provider and customer
- Indemnification and liability
- Incidence response for data breach
- Electronic discovery procedures

DORSEY
DORSEY & WHITNEY LLP

Nick Akerman

Dorsey & Whitney

http://computerfraud.us