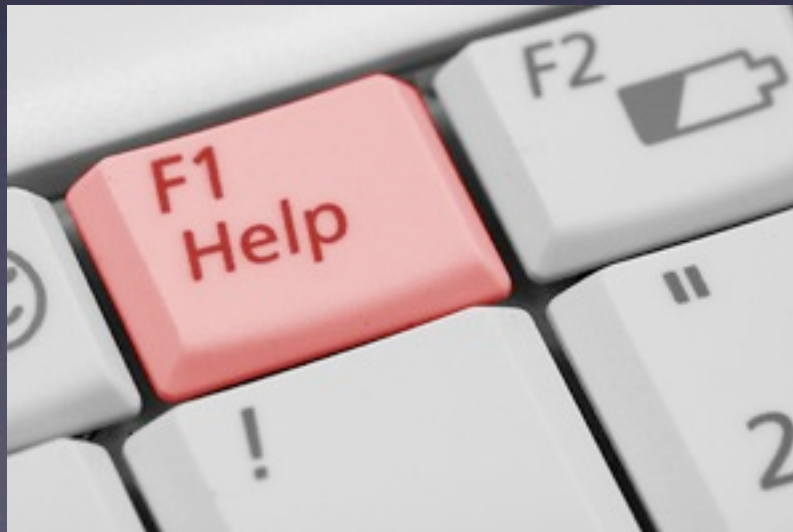
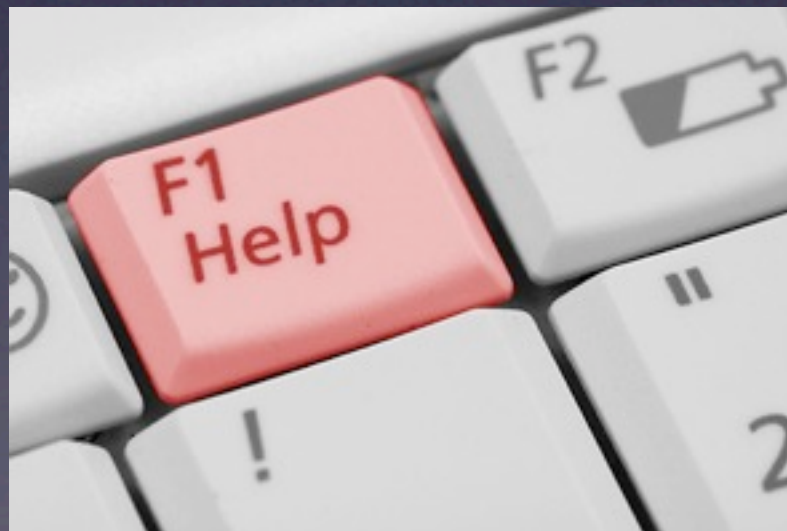




# YOUR CORPORATE COMPUTER POLICIES



# DO THEY ADDRESS RECENT LAW AND CURRENT TECHNOLOGY?





# Four Key Areas

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



# 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





# 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...



# 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





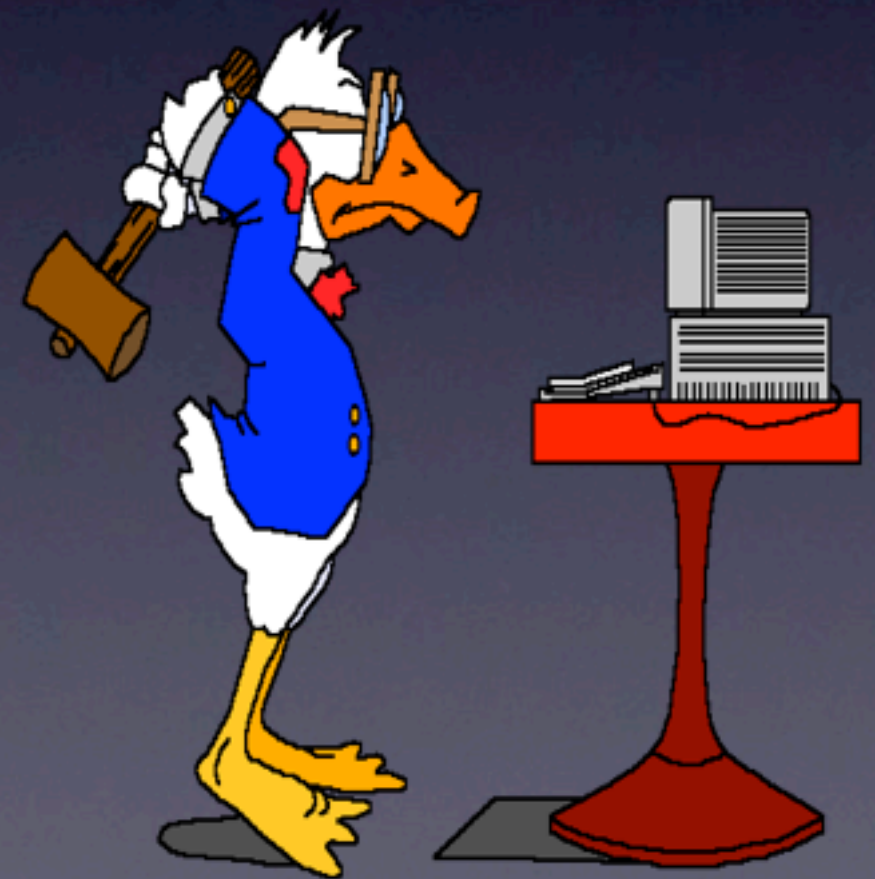
# Ways to Establish Lack of Authorization

- 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



# *International Airport Centers v. Citrin*

- 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.”





# 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

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

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





# ***U.S v. Nosal (9th Cir. 2011)***

- Korn Ferry Executive indicted for stealing confidential information before leaving to join competitor
- District court dismissed indictment based on *Brekka*
- Government appealed relying on Korn Ferry's computer policies, arguing Nosal exceeded authorized access
- 9th Circuit reversed finding violation of employer's computer use policies



# Company Rules

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





# ***Doe v. Dartmouth 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



# 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





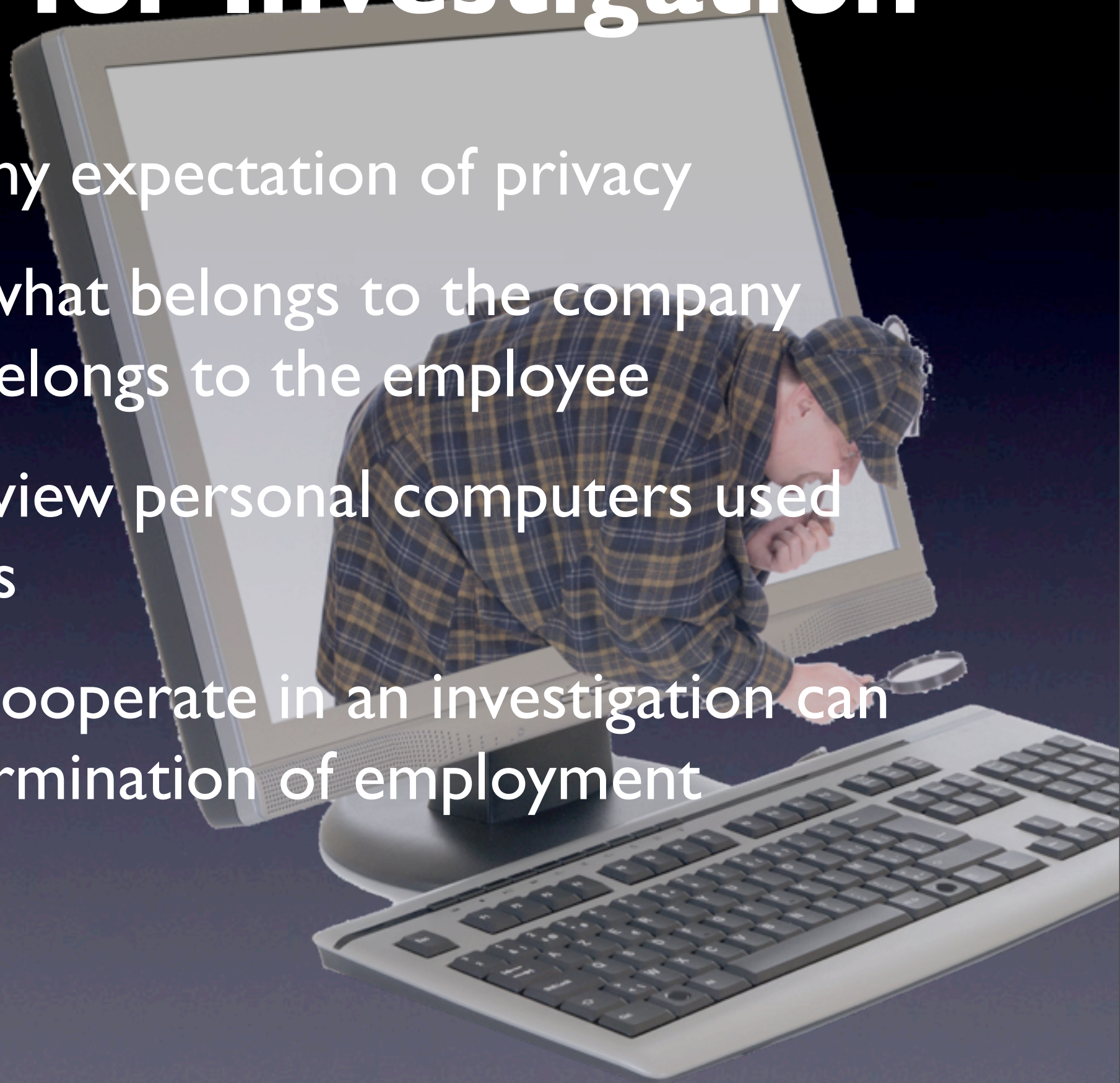
# Agreements

- Define scope of authorized access to company computers
- Confidentiality/Non-Disclosure Agreements
- Officers/Employees/Customers
- Among related companies
- Post employment restrictive covenants
- Anti-Raiding Covenants
- Customer agreements
- Data vendor agreements



# 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





# *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



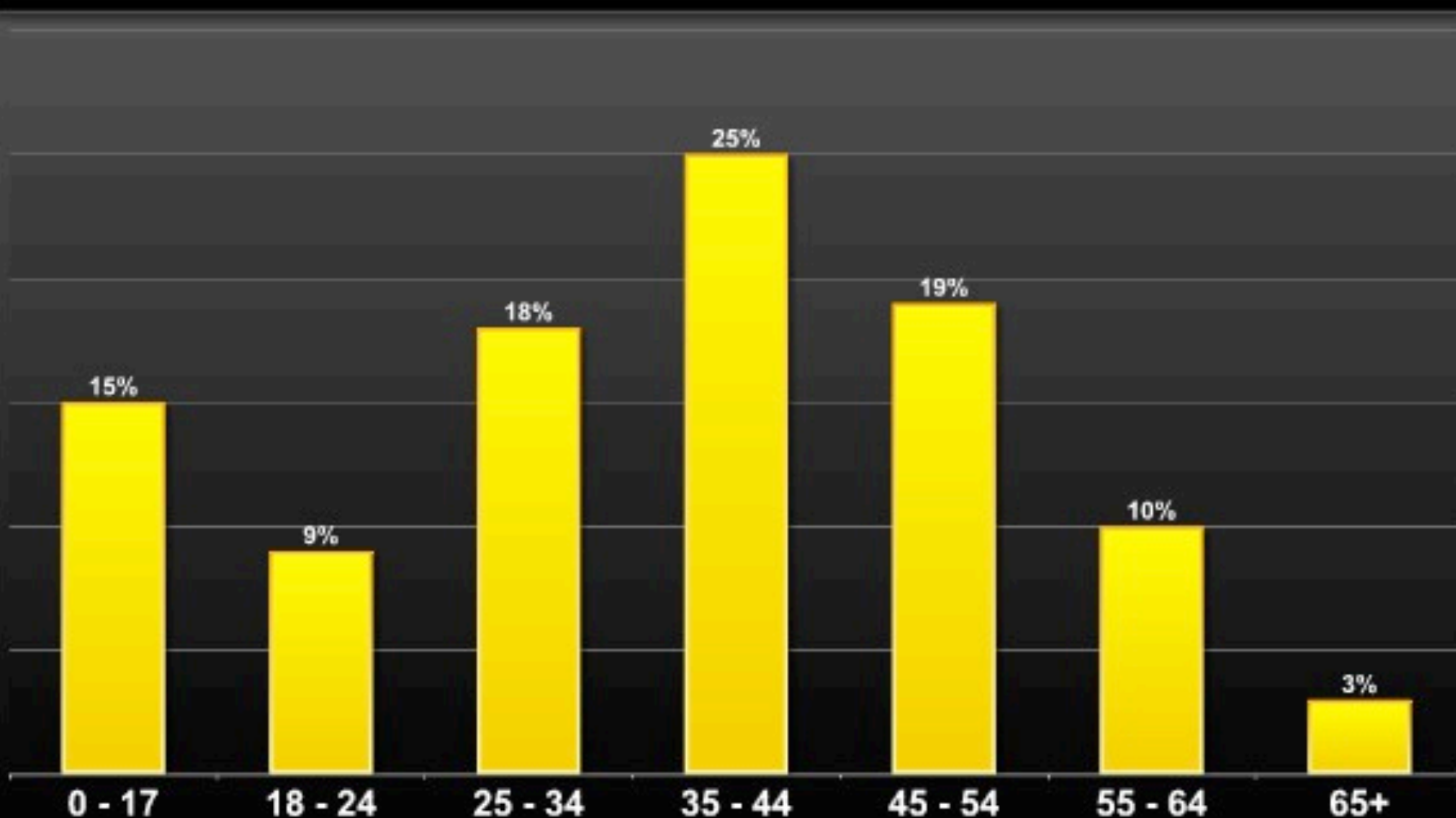
# Policies Must Be Internally Consistent

- *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



# Use of Social Networks

Average age distribution across social network sites  
United States



Data source: Google Ad Planner (United States demographics data)

[www.pingdom.com](http://www.pingdom.com)



**DORSEY**  
DORSEY & WHITNEY LLP

# Top 10 Companies by Number of Fans on Facebook



<b>1. Starbucks</b>	<b>3.7M</b>
<b>2. Coca-Cola</b>	<b>3.5M</b>
<b>3. Nutella</b>	<b>3.2M</b>
<b>4. YouTube</b>	<b>3.2M</b>
<b>5. Pringles</b>	<b>2.8M</b>
<b>6. Windows Live Messenger</b>	<b>2.5M</b>
<b>7. Ferrero Rocher</b>	<b>2.4M</b>
<b>8. Adidas Originals</b>	<b>2M</b>
<b>9. Victoria's Secret</b>	<b>2M</b>
<b>10. McDonalds</b>	<b>1.9M</b>

Source: ALLfacebook.com  
As of 8/26/09



# Areas of Legal Risk

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



# 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.



# 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

# 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



# *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



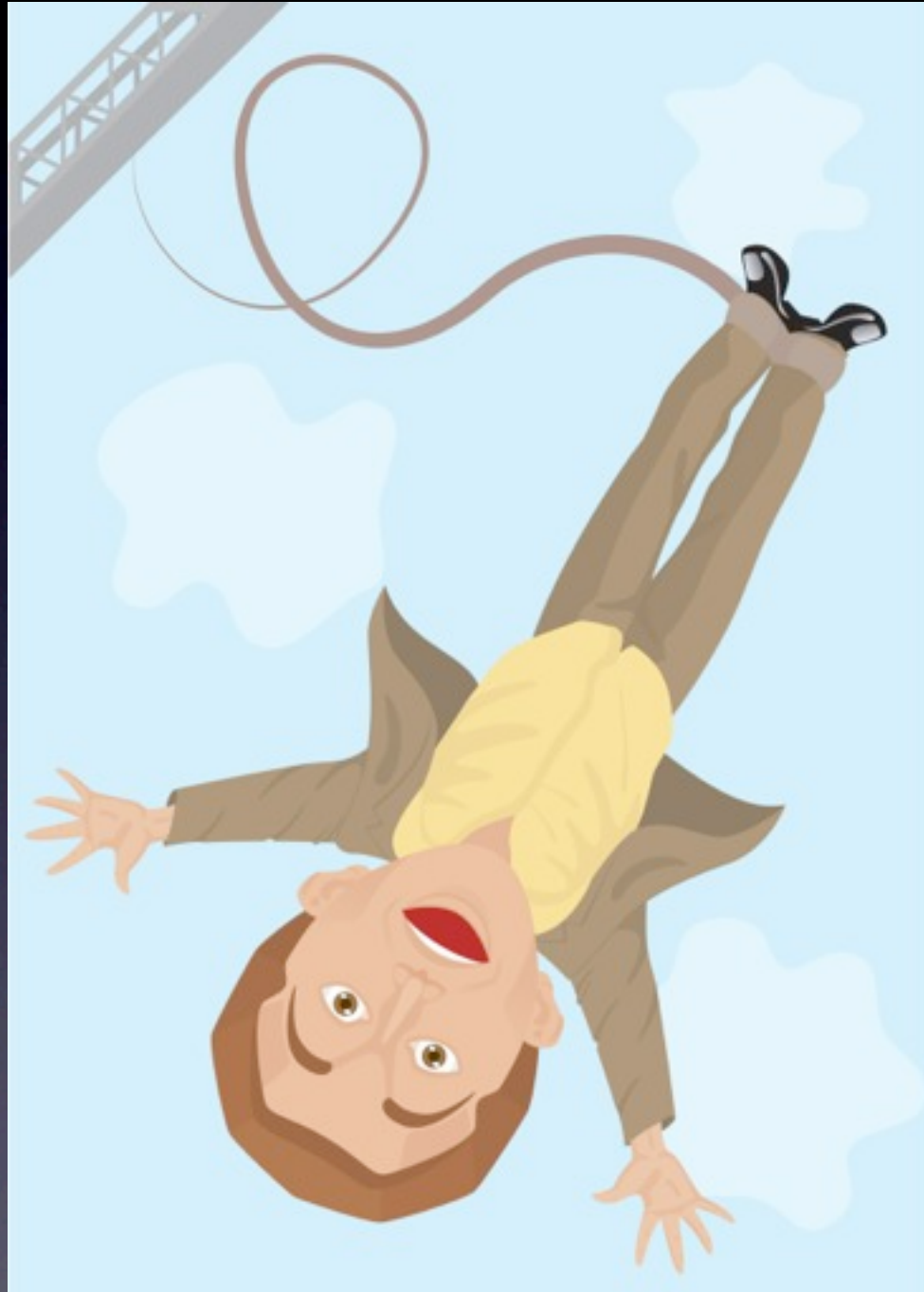
# Protected Labor Speech

- 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





# Critical Policy Components



# Critical Policy Components

## Warn against postings about:

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



# 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



# 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





# Critical Policy Components

- Define Acceptable Use
  - 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



# CLOUD COMPUTING







# CLOUD COMPUTING

# Record Retention





# 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



# 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

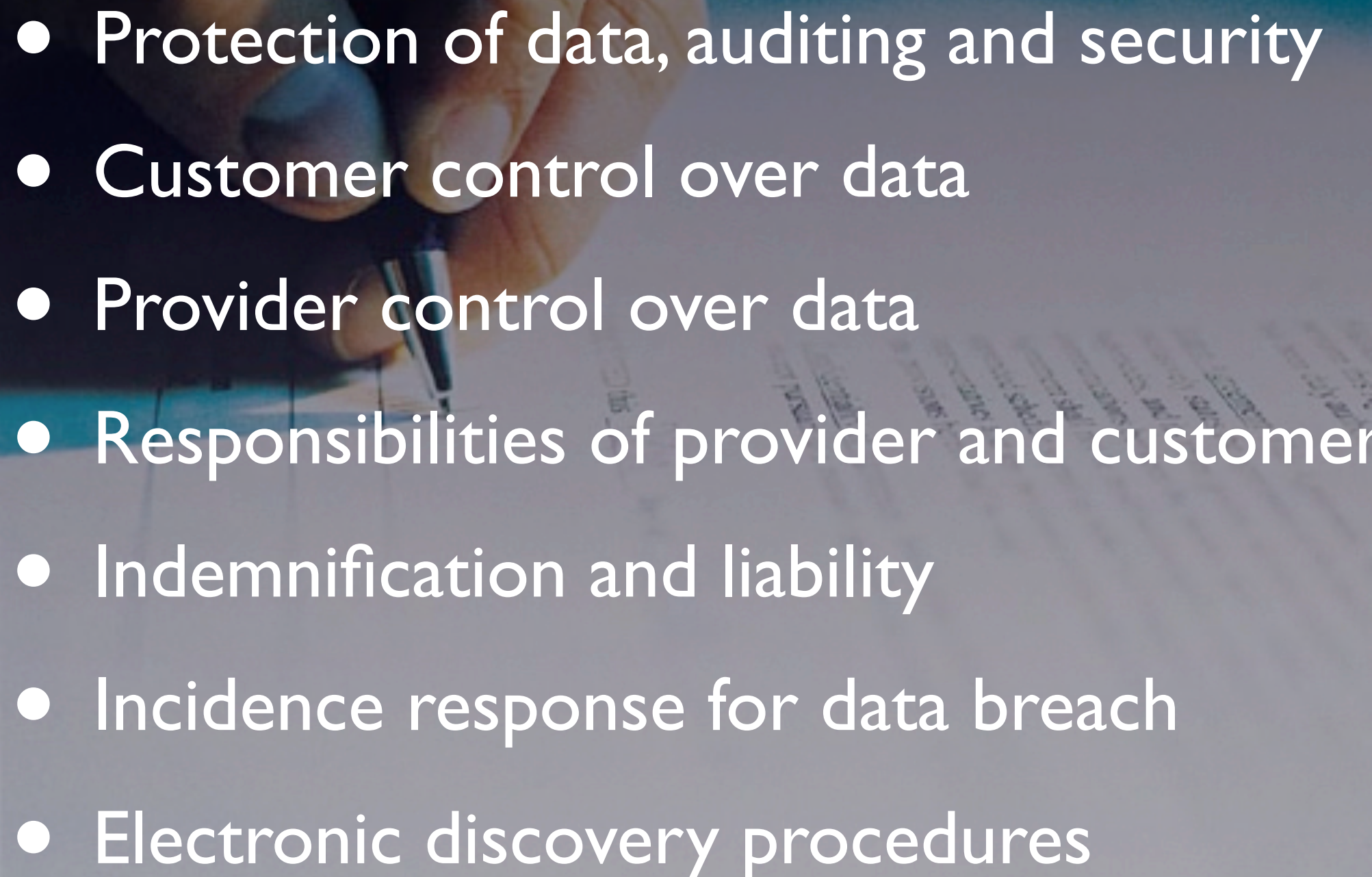


# Choosing a Cloud Provider

- Financial strength
- Insurance coverage
- Merger, acquisition, bankruptcy
- History of security breach
- Responsibility for data processing
- Provider and customer privacy



# Contract Protections

- 
- A background image showing a close-up of a hand holding a black pen, signing a document. The document has some text and lines, but it is out of focus. The hand is positioned in the upper left, and the pen is pointing towards the center of the document.
- 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



# Nick Akerman Dorsey & Whitney

