

# Fifth Twin Cities Chief Legal Officers Group CLE Program: Real World Privacy Issues

Hosted by ***SUPERVALU***

**Employee Privacy: A View Through Multiple Lenses**

**June 28, 2011**

**Melissa J. Krasnow, Partner, Dorsey & Whitney LLP,  
and Certified Information Privacy Professional**

## Common categories of employee personal information covered by federal and state privacy laws

- Social security number
- Financial information (e.g., bank account, broker account and other financial account)
- Health information

## 46 states (including Minnesota) have breach notification laws

- Cover the notification a company is required to make for breach of personal information to affected state residents and, in some cases:
  - state attorney generals
  - state regulators
  - credit reporting agencies

## State breach notification laws

- Personal information typically includes name plus any of the following:
  - Social security number (also consider state social security number laws and federal HIPAA/HITECH Act)
  - Driver's license number
  - Credit card number or debit card number
  - Bank or other financial account number
  - Health information also in a few states (also consider whether protected health information under federal HIPAA/HITECH Act)

## Enforcement of state breach notification laws varies

- State attorney general enforcement in Minnesota
- Private right of action in California
- Administrative fines in Florida

## Litigation

Ruiz v. Gap, Inc. (622 F. Supp.2d 908 (N.D. Cal. 2009), aff'd, 380 Fed. Appx. 689 (9th Cir. 2010))

- Stolen laptop computers containing personal information (e.g., social security numbers) of job applicants
- General rule: plaintiff whose personal information was at risk or compromised must demonstrate present and appreciable harm and compensable damages to survive dismissal

## **30 states (including Minnesota) have social security number laws**

- Could be implicated in a breach involving social security numbers

# Massachusetts privacy law

- Covers Massachusetts resident personal information (excluding health information)
- Requires comprehensive, written information security program:
  - third-party service providers must maintain appropriate security measures, memorialized by written contract
  - requires encryption
- Massachusetts attorney general enforces
- Massachusetts attorney general and Massachusetts regulator must be notified under Massachusetts breach notification law

## Federal HIPAA / HITECH breach notification law

- Applies to covered entities and business associates
- Covered entities: (i) health plan, (ii) health care clearinghouse or (iii) health care provider
- Business associates that (i) on behalf of a covered entity, perform activity involving use or disclosure of individually identifiable health information or (ii) provide legal, actuarial, accounting, consulting, management, administrative, accreditation or financial services for the covered entity involving the disclosure of individually identifiable health information from the covered entity to the person

## Federal HIPAA / HITECH breach notification law

- Protected health information means individually identifiable health information relating to health care treatment, a health condition or payment for the provision of health care
- Covered entity notification to each individual, U.S. Department of Health and Human Services (if breach involves more than 500 individuals) and prominent media outlet (if breach involves more than 500 residents of state or jurisdiction)
- Business associate notification to covered entity

## Enforcement of HIPAA/HITECH Act

- U.S. Department of Health and Human Services enforcement
- Civil penalties
- Criminal penalties
- State attorney generals also can bring civil actions
- No private right of action

## Review information and documentation and determine applicable laws

- Employee personally identifiable information – what, where and in which form is it?
- Which company policies and procedures and agreements have provisions relating to employee privacy and confidentiality?
- Determine which laws apply and what the requirements are (e.g., policies and procedures and agreements)
- Sometimes, policies and procedures are advisable, though not required by law
- Which federal and state laws apply?

## Be prepared

- Prepare policies and procedures and ensure they are consistent and integrated with company policies and procedures
- Devise a roadmap of what to do in the event of a possible breach
- Consider handling of investigations
- How should a company respond internally and externally to media, employees and others about breach circumstances and status?
- Is SEC disclosure required for a public company?

## Hot topics – mobile devices

- Massachusetts privacy law written information security program:
  - employee security policies for personal information outside premises
  - password management
  - encryption of personal information transmitted wirelessly and stored on portable devices
  - security software and measures
- Revisit applicable company policies (e.g., technology and electronic communications):
  - Company access to and monitoring of employee-owned devices
  - Applicability to company and employee-owned mobile devices

# Hot topics – mobile devices

## BYOD Is Riskiest

BYOD = Bring Your Own Device



Source: 2011 ISACA IT Risk/Reward Barometer-US Edition  
([www.isaca.org/risk-reward-barometer](http://www.isaca.org/risk-reward-barometer))

## Hot topics – mobile devices

- 65% of smartphone users are concerned about their location being tracked, while 21% are aware of and 13% experienced this security risk
- 40 percent of smartphone users use their smartphone for social networking

(Smartphone Security Survey, Ponemon Institute and sponsored by AVG Technologies, March 2011)

**Any questions?**

**Melissa J. Krasnow**  
**Partner, Dorsey & Whitney LLP,**  
**and Certified Information Privacy Professional**

**(612) 492-6106**  
**krasnow.melissa@dorsey.com**  
**twitter.com/melissakrasnow**