



# Privacy & Security Crash Course: Questions When Dealing with Employees

June 2, 2015

This presentation has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal, state, and/or local laws that may impose additional obligations on you and your company.

Cisco WebEx can be used to record webinars/briefings. By participating in this webinar/briefing, you agree that your communications may be monitored or recorded at any time during the webinar/briefing.

## Attorney Advertising

# Presented by



**Adam C. Solander**

Member of the Firm

[asolander@ebglaw.com](mailto:asolander@ebglaw.com)

202-861-1884



**Nathaniel M. Glasser**

Member of the Firm

[nglasser@ebglaw.com](mailto:nglasser@ebglaw.com)

202-861-1863

# How to Prevent Data Theft



- Address data privacy in **employment agreements**:
  - Retain the right to inspect all devices utilized by the employee
- Create, update, and implement appropriate **employment policies**:
  - Computer, Tablet, Mobile Phone, Internet, and Email Usage Policy, including BYOD
  - Data Retention Policy
  - New and Departing Employee Procedures/Checklists
- Implement appropriate **technology** to protect data
- Conduct periodic **employee training**
- Issue periodic **security reminders**
- **Discipline** employees for policy violations

# What To Do From A Technical Standpoint



## ■ Eliminate the opportunity

- Employee monitoring software
- Email filtering
- Role based access and audit logging
- Data destruction policy
- Limit paper

## ■ Be as foolproof as possible

- Lockdown USB ports
- Hardware encryption
- Scan local repositories of sensitive information (i.e., shares and local drives)
- Multi-factor authentication
- Eliminate open source file sharing

## ■ Deter bad behavior- cameras, audits, etc.

# What If You Learn Your Employee Has Taken Confidential Information?

---



- Immediately **investigate** the nature and scope of the data breach
- Conduct a **forensic review**, using internal IT or external specialist
- Send a **cease and desist letter**
- Contact **police**
- File a **civil suit**, seeking injunctive relief

# Self-Help Discovery by Current or Former Employees

---



- Within the context of the litigation, self-help discovery may provide basis for:
  - Sanctions for employee's misconduct
  - Assertion of a TRO and/or counterclaim
  - Disqualification of plaintiff's counsel
- Outside of the litigation, self-help discovery may:
  - Support discipline or even termination of the employee
  - Establish foundation for criminal prosecution

# Legal Protections for Data and Employee Privacy

---



- Laws Protecting Against Dissemination of Employee Data:
  - State Law
  - HIPAA and/or FTC
  - *Corona v. Sony Pictures Entmn't, Inc.*, U.S.D.C., C.D. Cal., Dec. 15, 2014
  
- Privacy Rights Granted to Employees:
  - State law, including invasion of privacy
  - Whistleblower protections
  - Contractual obligations
  - Collective bargaining agreements
  - Fourth Amendment (public employees only)



# Questions?

---



**Adam C. Solander**

Member of the Firm

[asolander@ebglaw.com](mailto:asolander@ebglaw.com)

202-861-1884



**Nathaniel M. Glasser**

Member of the Firm

[nglasser@ebglaw.com](mailto:nglasser@ebglaw.com)

202-861-1863

**Thank you.**