RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Practical Legal Aspects of BYOD

SESSION ID: LAW-F01

Lawrence Dietz
General Counsel & Managing Director
TalGlobal Corporation
ldietz@talglobal.net
+1 408 993 1300
http://psyopregiment.blogspot.com

Francoise Gilbert
Founder & Managing Director
IT Law Group
fgilbert@itlawgroup.com
+1 650-804-1235
@FrancoiseGilbrt

BYOD Adoption

	U.S.	U.K.	Canada	Brazil	Russia	India	China
Desktop Computer	47%	38%	47%	56%	10%	55%	54%
Laptop Computer	41%	32%	41%	57%	7%	68%	56%
Standard Mobile Phone	33%	29%	27%	50%	36%	84%	78%
Smartphone	55%	38%	47%	71%	5%	85%	76%

Source: Bring Your Own Device: The Facts and the Future; Gartner Group; April 2013

Common BYOD Problems

- Lost, damaged or stolen devices
- Employees come with or leave with sensitive data
- Inappropriate images or communication
- Introduction of malicious code
- Data inadequately backed-up
- Time consuming maintenance
- Incompatibility between different OS, Apps, different versions

Common BYOD Problems (Continued)

- Minimum level of security products & proper procedures, e.g. passcode
  - Guidance on public Wi-Fi
  - Encryption: at rest and in transit
  - App policy and security evaluation
- Cost sharing and legal responsibilities
- Combined (personal & professional) use
  - Security Issues
  - Data Ownership

Setting The Stage

- Working Definition of BYOD
- The State of BYOD Law Today
- The Future of BYOD

Working Definition of BYOD

- Bring Your Own Device or BYOD simply means that the employee is using his/her own electronic device (smart phone, tablet, laptop, etc.) for company purposes.
- The employee owns the device and pays the bill for its use whether or not the employer reimburses the employee for the cost.
- The device contains personal data about the employee, e.g. PII, PCI, PHI.
- The employee may not be the only person using the device.
- BYOC – Bring Your Own Cloud – where employee keeps some company data on third party's cloud

The State of BYOD Law Today

- No Specific BYOD Laws
- Existing Areas of Law Apply
  - Privacy Law
  - Labor Law* - including employee monitoring laws
  - Laws Relating To:
    - Stored Communications
    - Computer Fraud & Abuse
    - Information Security & Privacy

The State of BYOD Law Today (Continued)

- Laws Relating To (Continued):
  - Electronic Discovery
  - Minors and the Internet
- Government Access to Data
  - Law enforcement Search & Seizure
  - Search warrants, subpoena, court other
- International Travel
- Third party litigation

The State of BYOD Law Today – Foundational Law

- Breach of Contract
- Breach of Fiduciary Duty
- Intellectual Property Loss
  - Unauthorized access, disclosure, modification
  - Unauthorized destruction, deletion
- Labor & Employment Laws

The State of BYOD Law Today – Foundational Law (Continued)

- PII Exposure & Breach Liability
  - Unauthorized access, disclosure, modification, destruction, deletion
  - Security breach disclosure obligations
- E-Discovery Laws and Compliance
- Electronics Communication Privacy Act (ECPA)

The State of BYOD Law Today – Industry Laws

- Industries where laws or industry regulations/standards are likely to apply to BYOD even if not explicitly stated:
  - Government
  - Health Care
  - Finance
  - Electrical and Nuclear Power

Pre-Employment Overview

- Clean hands
- Privacy waiver
- Policy acknowledgement
- IP creation rules
- Keeping own number & making personal calls likely means higher level of privacy post employment
- How much prior employer data or information remains on the device, purposely or inadvertently

Pre-Employment Considerations

- How will the employer know what content is on the device before it is given access to organizational resources?
  - Pornography
  - Nature of personal data & its current protection
  - Data from former employers
  - Employee owned Intellectual Property
  - Malicious code
- PHI and/or PII on others besides the device owner

BYOD Policy Considerations

- Create the policy BEFORE allowing the use of BYOD
- Who is eligible for access (labor law concerns)
- Who pays for what
- Difference between exempt / non exempt personnel
- What technical parameters for the device: what devices supported, what data plans
- Don’t forget the contractor who act in similar capacity as employees

BYOD Policy Considerations (Continued)

- What security measures must be followed
  - What apps are permitted / excluded
  - What data are permitted / excluded
- How and when a mobile device may be used to access the company network
- Acceptable use policies
  - Limits on places and applications

BYOD Policy Considerations (Continued)

- What data are collected from employee's device
  - What data may not be collected from employee's device
- What to do if the device is lost or stolen
  - Geolocation of lost device
  - Remote wipe data on lost device
- Company's ability to access device used for work, including employee's activity on the device, employee's access to social media, web-based personal email

BYOD Policy Considerations (Continued)

- Company's access in connection w. litigation, e-discovery requests, internal or external investigation
- What happens if employee / contractor leaves the company
  - Copy of device content
  - Access to device content after employee / contractor has left the company
- Legal limits on GPS locators or other monitoring software

Company Side Considerations

- Does the company have a policy that specifically addresses BYOD?
- Is the employee or contractor made aware of this policy before accepting an employment or contract offer?
- How to deal with current employees / contractors?
- Does the employee or contractor acknowledge that he/she is aware of these regulations and will follow them?

Considerations During Employment

- Policy familiarization & acknowledgement
- Consent to search device, consent for electronic discovery
- Employer responsibilities: secure device, replace/repair
- Limit what can be stored or accessed on the employee's or contractor's device.
- Employer's security software: encryption, access control.
- Hourly/work records
- Mandatory breach notification responsibilities

Considerations During Employment

- Increase or improve security measures to address the increased risk to the company's data, and the unique circumstances of BYOD or BYOC
- Better, specific technical measures: password control, use of encryption
- Better, more specific physical measures: improve awareness of risk to the device, suggest measure to limit third party access to device
- Better, more adapted, more specific administrative measures: clearer contracts, policies; detailed procedures on how to address loss of device; periodic reminders; targeted exit checklists

Considerations During Employment

- Employee awareness about rules, responsibilities, pitfalls
  - At the time of hire (first day training program)
  - Periodically during employment, e.g. reminder emails several times a year
- Training
  - Legal: understand responsibilities as the holder of important company important
  - Practical / Technical: how to use the device or cloud in order to reduce the risk of errors
  - Security: how to secure the device, proper use of password, encryption

Post Employment Considerations

- Exit interviews
- Ability to swipe the device or clean the personal cloud
- Audit of personal devices
  - IP Theft
  - Data of others: PII, PHI, etc.
- Extended consents for a “reasonable” period of time
- Responsibilities and compensation for participation in post-employment legal procedures.

The Role of the IT / IS Department

- Establish standards for identifying the acceptable device
  - Manufacturers, devices, models, operating platforms
  - Mobile networks and service plans
- Define the procedure for enrollment
  - Configuration of the devices or access to the cloud
  - Password management
- Define the procedure for termination, decommissioning

The Role of the IT / IS Department (Continued)

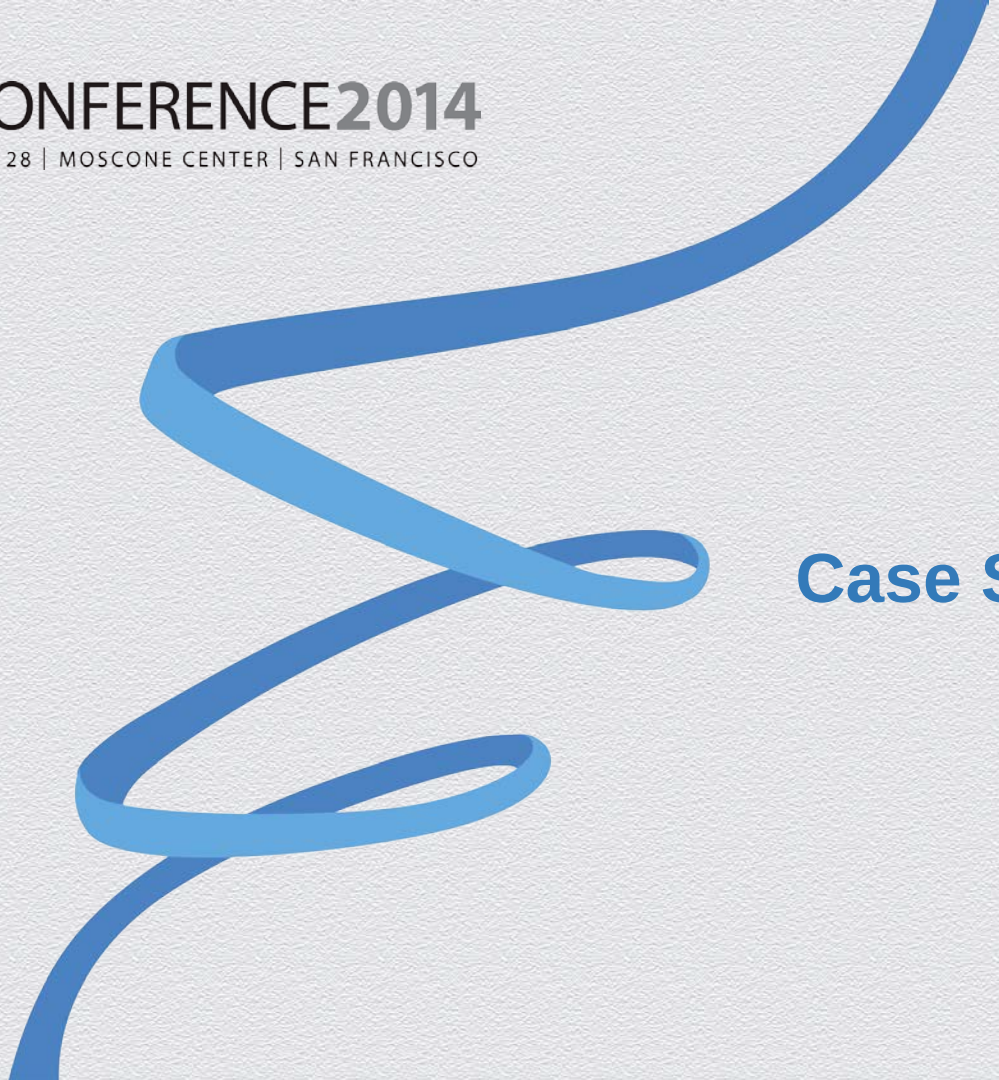
- Define the parameters of assistance to employees
  - Initial activation assistance
  - On-going support
  - Identify relevant security patches, and mechanisms to download them
  - End-of-support
- Communicate, communicate, communicate
  - Interact with the remainder of the company
  - Explain how it works, what can happens

The Role of the IT Department (Continued)

- Define security standards
  - Minimum security standards to be met before accessing network
  - Data categories
  - Authentication
  - Lost password
  - Lost device
- Be available for questions

The Role of the IT Department (Continued)

- Define privacy standards
  - Segregation of company data v. personal data
- Monitor
  - Review server logs to determine what was downloaded



Case Studies

Case Study #1

Eddie is a software engineer who recently joined the company. His former employer is one of your company's major competitors. Your company has adopted Brand A Smart phones because your purchasing department got a great deal.

Eddie insists on using his personal Brand B for company business even though he doesn't get reimbursed for his calls.

You are Eddie's supervisor. HR calls you and you find yourself in an office with the head of HR and your company's General Counsel. Eddie's former employer is suing yours for theft of trade secrets and you have received a subpoena (or your country's equivalent) to turn over Eddie's phone.

Case Study #1 (Continued)

- Is the company responsible for turning over Eddie's phone?
- Do you think your company is liable for Eddie's actions?

Case Study #2

You are sitting in the company cafeteria and you over hear a conversation about a Facebook posting. Seems that a picture of your new prototype appeared on one of your employee's teenage children's pages. The discussion was among your very junior staff, one of whom is friends with the poster.

Upon investigating you find out that the employee-parent allowed his child to take his tablet to school and that the employee had been using the tablet as a convenient way to work at home on the new prototype's design. You also learn that the employee's supervisor was not aware of the tablet's use.

Case Study #2 (Continued)

- What action do you take against the employee?
- Suppose the company had supplied the tablet, would your action be different?

Case Study #3

Your company has settled on Android phones. However, your top sales person, Samantha insists on using her iPhone. Samantha keeps her contact list, a very sought after property since it reflects her five years as top sales person, on her iPhone. She has her passcode taped on the phone.

On one Monday morning a mournful Samantha comes into your office as CSO and tells you that her beloved iPhone was lost over the weekend.

She wants to know what you intend to do about replacing it for her?

Case Study #3 (Continued)

- What do you feel you need to do?
- Would your answer change if the contact list was maintained using an approved company app?

Top Ways to Minimize BYOD Liability

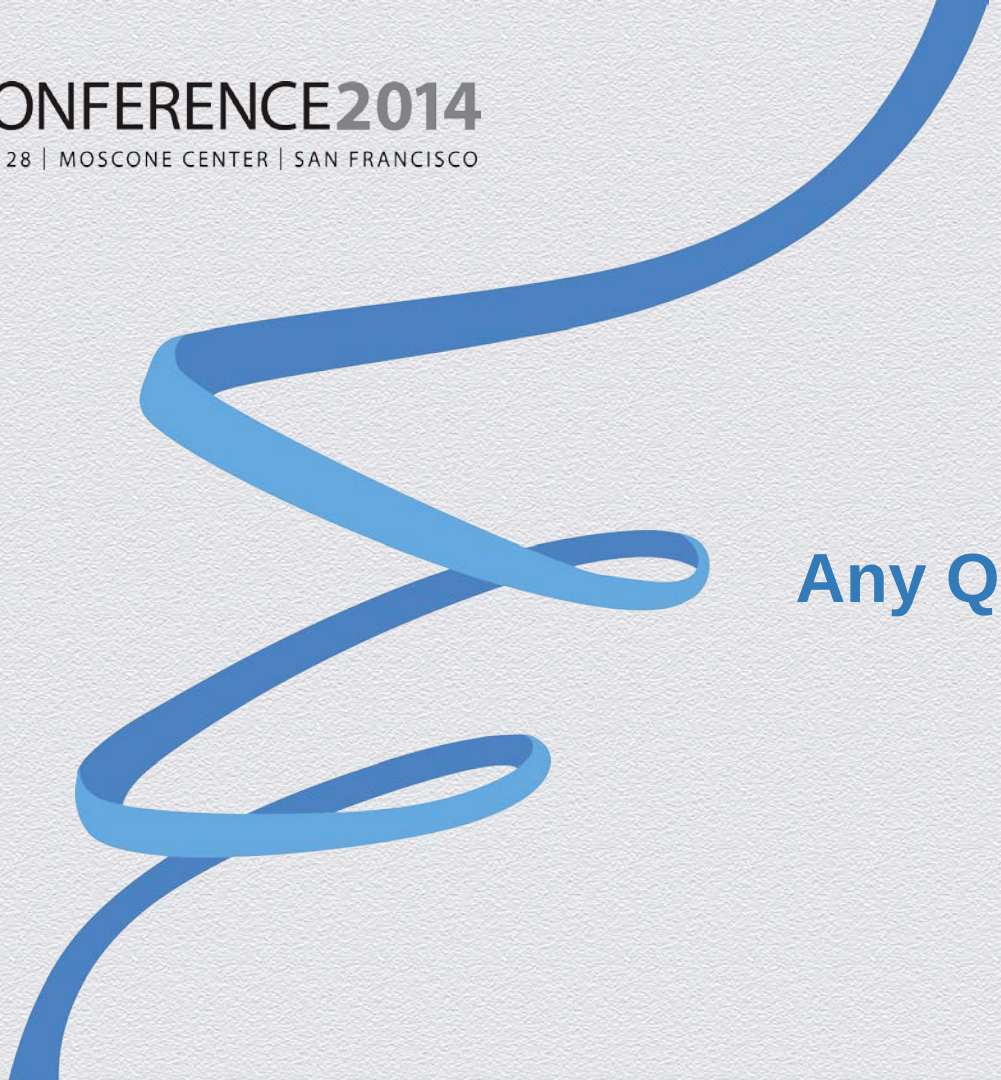
- Thorough evaluation of the potential uses; and of the related risks
- Limiting what data may be used from, or stored in a non-company owned device
- Authentication
- Easy to comply with security measures: policies, procedures, technology
- Frequent audits and monitoring of compliance, and updating of the policies and procedures

Top Ways to Minimize BYOD Liability (Continued)

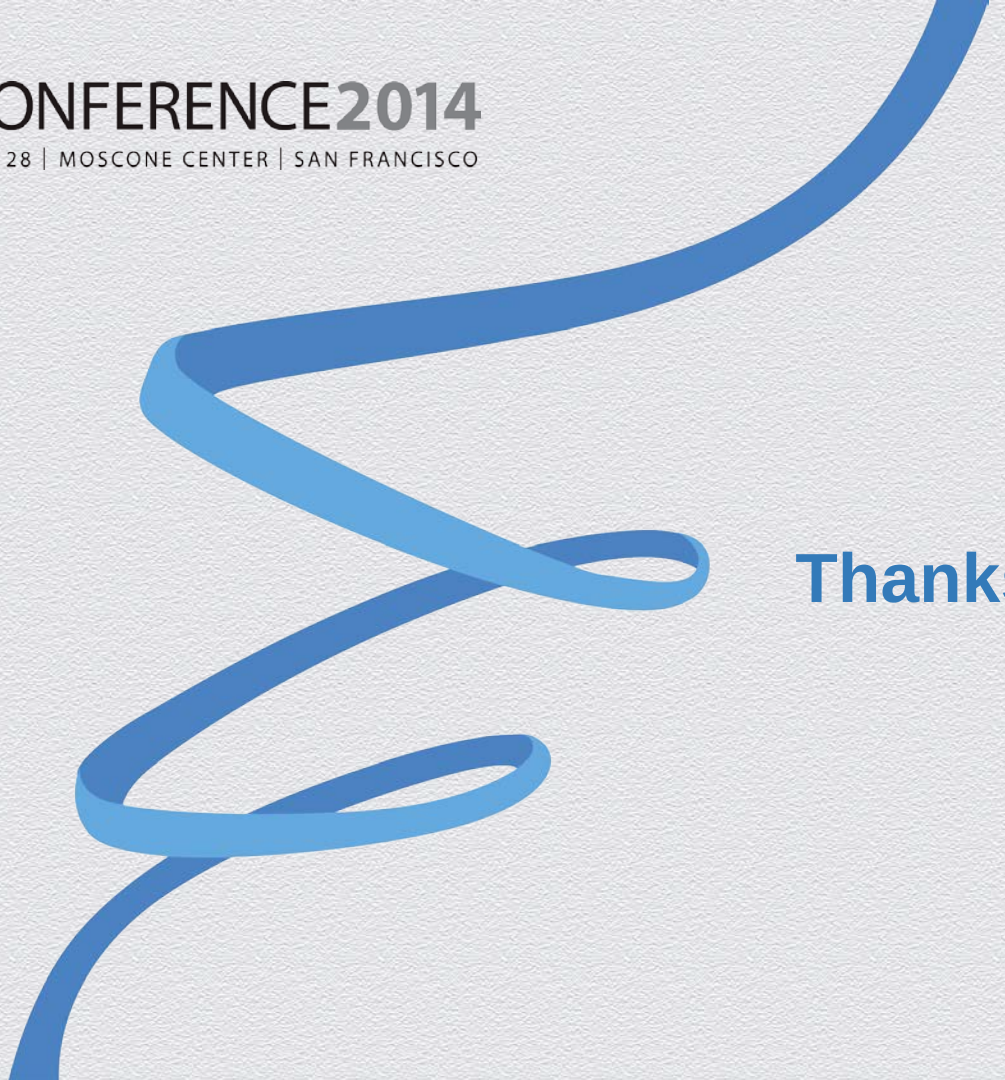
- Training and awareness
- Enhanced termination procedures

Future of BYOD

- What if organizations require employees to use their own devices like carpenters use their own tools?
- Younger work force will demand to use their own devices.
- SaaS will migrate to Apps if they haven't already. Platform agnostic apps will rule.
- Growth of non-traditional employees will foster BYOD



Any Questions?



Thanks for listening.