iProblem: Making BYOD Policies Work

Compliance Week Annual Conference

May 21, 2013

Joseph V. DeMarco

Washington, D.C.

DeVORE & DeMARCO LLP

Attorneys and Counselors at Law

My Background

- Partner, DeVore & DeMarco LLP
  - Boutique law firm in New York City
- Cyberlaw Practice
- Previously, Assistant U.S. Attorney, Southern District of New York, 1997-2007
  - Founder and Chief, Computer Hacking and Intellectual Property Unit (CHIPS)

BYOD – AN OPPORTUNITY

- *Forces you* to address compliance with laws governing data privacy and security
- *Forces you* to deal with the fact that "perimeter defense" is an obsolete concept

BYOD – KEY LEGAL DRIVERS

- Data Privacy and Security law: Encryption, virtualization, defense in depth and ring fencing may help -- but each have limits and drawbacks
- Surveillance and geolocation tracking: Wiretap laws vary among jurisdictions
- eDiscovery, records retention, litigation hold and cloud computing issues rarely considered in advance
- Miscellaneous legal issues: Devices as (work tools; overtime pay for after-hours work; "equal rights" issues; no retaliation for lawful conduct.

Thank you!

Joseph V. DeMarco, Esq.
DeVore & DeMarco LLP
99 Park Avenue
Suite 330
New York, NY 10016
T: 212.922.9499
F: 212.922.1799
jvd@devoredemarco.com
www.devoredemarco.com

The iProblem: Making BYOD Policies Work

Jane A. Levine

Worldwide Director of Compliance, SVP

Sotheby's

COMPLIANCE WEEK 2013

POWERFUL INSIGHTS, PRACTICAL IDEAS, REAL SOLUTIONS

#CW2013

The iProblem: Making BYOD Policies Work

Some Background on Sotheby's

- Sotheby's began as a small book auction house in England in 1744.
- As early as 1754, Sotheby's became involved in selling paintings and decorative works of art, the facets of our business that now dominate our auction activities.
- Sotheby's has been publicly traded since 1988.
- Today, Sotheby's maintains 90 locations in 40 countries and conducts 250 auctions each year in over 70 categories.
- In 2012, net auction sales were $3.8 billion, with revenues of $717 million.

The iProblem: Making BYOD Policies Work

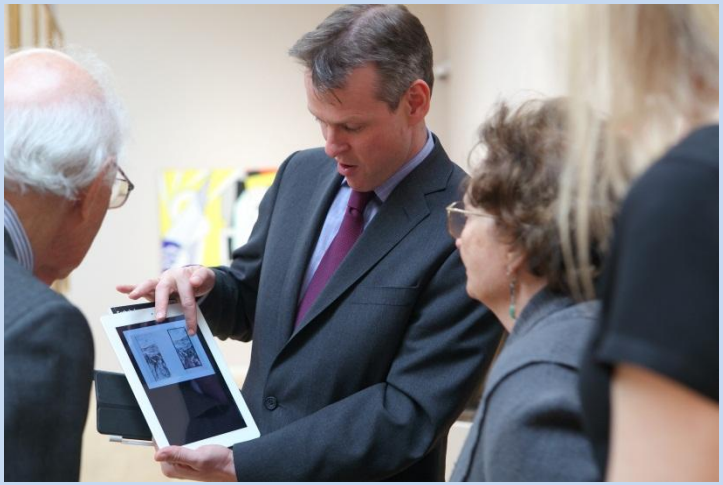
Sotheby's Business

- In its role as **auctioneer**, Sotheby's functions as an agent accepting property on consignment from its selling clients. Sotheby's bills the buyer for property purchased, receives payment from the buyer and remits to the consignor the consignor's portion of the buyer's payment after deducting Sotheby's commissions, expenses and applicable taxes.
- Sotheby's also brokers **private sales** of fine art, jewelry and collectibles.
- Additionally, Sotheby's has a **financial services** segment that provides loans to collectors and dealers secured by works of art.

The iProblem: Making BYOD Policies Work

Mobile Devices Greatly Enhance our Business

- Image-intensive nature of our work
- Global business, but client-centered
- Sourcing globally, selling at auction in five locations
- Increased staff use of POD's; business desire to encourage use **but retain control**



The iProblem: Making BYOD Policies Work

Overview

- Initial impetus from IT based in NY - one page “consent form”
- Collaboration with Compliance and Ethics Team – 7 page single spaced form and policy

Cultural Clash

- Adverse reaction of European colleagues
- Differences in expectation of privacy

The iProblem: Making BYOD Policies Work

Crafting a Global Consent Form and Policy for PODs and CODs

Legal Issues

- Stricter privacy laws in UK/Europe
- Works counsel approvals
- ICO Data Protection Act Guidance on BYOD – personal data includes corporate, employee/family member data.
- "Blanket" or general consent not permitted; specific purposes for which tracking, monitoring, erasing will be used must be enumerated.
- Harmonizing policy vs. number of employees in location

Areas of Tension

- Shared use – family members (spouses and children using PODs)
- Use of Cloud storage, iCloud, Dropbox, Google Docs, etc. – unauthorized access issues, security, erasing

The iProblem: Making BYOD Policies Work

Consent Form

- Online process
- Consent to terms of use and to policy governing use
- “Don’t agree” triggers disabling of active sync

COD’s

- Afaria (SAP-related product)
- Inventory control – remote functions
  ie. Erase, location, app pushing
- Password standards
- Restrictions on certain functions
  - ie. iCloud and camera




The iProblem: Making BYOD Policies Work

Technology Does Not Replace Training or Mitigate Human Error or Bad Judgment

- Backup ability *will* exist for COP + POD
- Family member access cannot be prevented
- Reporting lost devices is manual
- In the end, success or failure, from a data protection, security perspective depends on effective use of technology AND traditional compliance program effectiveness – training, monitoring, culture.

Making BYOD Work

Richard Martin, CIA, CISA, CISSP

Texas State Technical College

Director of Information Security and Compliance

Making BYOD Work

What were the objectives of governing BYOD?

- Protect data that by regulation is considered confidential.
- You mean PII?

Making BYOD Work

What data if released could be harmful to the organization and/or individual?

- Name?
- SSN?
- Financial Accounts?
- Addresses?

Making BYOD Work

We figured out it was data in combinations!!

Yay!!

Now what the hell do we do?

Making BYOD Work

Risk Analysis

- What could happen?
- Probability
- Impact
- Cleanup

Making BYOD Work

What is the solution?

- Mobility device management policy
- Preventive controls (logical access)
- Detective mechanisms (data in combinations)
- Loads of training

Making BYOD Work

Conclusion:

It's hard. No solution will mitigate every risk.

Understand the risk appetite of your organization.

80/20 rule will fit most organizations.