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

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

BYOD – An Interpretive Dance

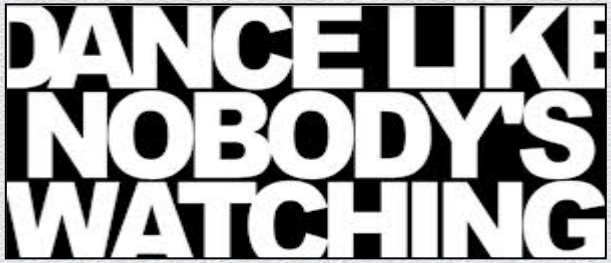
SESSION ID: **DSP-F02**

Constantine Karbaliotis
Americas Privacy Leader
Mercer

Ellen Marie Giblin
Privacy and Data Protection Group Leader
Ashcroft Law Firm

MERCER

ASHCROFT LAW FIRM



BYOD – An Interpretive Dance

- Security and Privacy engage in a dance with the Users…
- Whose toes will get stepped on?

BYOD – An Interpretive Dance!

Agenda

- BYOD – A New Interpretation
- BYOD – Redefined - A New Dance
- BYOD – Privacy vs. Security Risks
- BYOD – Mechanisms to Address Risk

BYOD – A New Interpretation!

- It is a no longer about keeping executives with iPads or Generation X/Y/Z happy…that is so….. 2010
- It is about the “Company Two-Step” – Expect to “Bring It”
  - The company laptop will go the way of the “Company Car”
  - Promised cost savings to companies will be staggering
  - Choice and flexibility – “Your choice and we can be flexible!”
  - Costs/Benefits/Risks – Shifting the risk to the user, then shifts the cost as well, and that is the benefit
  - Or, is there an encore to this dance…

BYOD – Redefined – A New Dance!

- Employee-owned mobile devices in the workplace paid by the end user, the organization, or through shared payment
- Explicitly requires the relaxation of the standard that only organizational devices can be used for work-related purposes
- However, your dance moves and your partner's (your device) will be defined and monitored by the enterprise
- Risk Assessment vs. Cost Benefit Analysis

Security Risks v. Privacy Risks

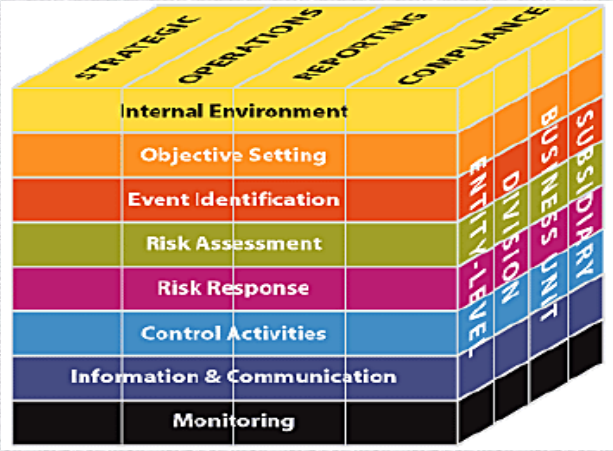
Security Risks	Privacy Risks
Exposure of organizational infrastructure, data	Regulatory exposure for data lost from BYOD
Ownership risks	Commingling of personal data belonging to the end user and organizational data
Undisciplined use – apps, usage, malware	Exposure of end user information to the organization
Management of multiple O/S, carriers, configurations, proliferation	Management of end user and organizational data

BYOD – An Interpretive Dance – Address the Risk

- BYOD – Mechanisms to Address Risks
  - Basic Elements of a Compliance Program
  - Policies & Procedures
  - Technology Solutions
  - Privacy Risk Assessment
  - Security Risk Assessment
  - Data Minimization through Data Mapping

Mechanisms to Address Risk:
Basic Elements of a Compliance Program

*COSO Risk Model



Risk Assessment:

- Know what data you have through data mapping
- Know where your data resides

Risk Response (Risk Appetite)

- Understand internal company policy toward Privacy risk

Control Activities:

- Know your “System of Internal Controls”

Information & Communication

- Define mechanisms to identify, inform and communicate requirements and performance against those requirements

Monitoring:

- Measure compliance

MERCER

ASHCROFT LAW FIRM

#RSAC

RSACONFERENCE2014

Mechanisms to Address Risk: Policies & Procedures

- Privacy Policy
  - Who gets to BYOD – Employees, contractors, interns?
- Acceptable Use
  - Requires explicit recognition of what uses are prohibited
- Information Classification
  - What class of data and level of sensitivity is permitted on devices
- Information Security
  - Examples: role-based requirements; camera usage; security requirements for Android devices; location use

Mechanisms to Address Risk: Technology Solutions

- Selection of acceptable devices
  - Avoid proliferation while offering choice
  - “Last year’s model” challenge
- Requirements include:
  - Compartmentalization of data
  - Encryption
  - Remote wipe of organization data
  - Records management

Mechanisms to Address Risk: Privacy Risk Assessment

- Development of appropriate policies and technology choices follows an understanding of risks for your organization
- The purposes of a privacy risk assessment are:
  - To identify and weigh privacy risks for an initiative or project
  - To mitigate the risks as far as reasonably possible
  - To ensure there is an accountable person taking responsibility for accepting the residual risks
  - And to document that you have done all these things!
- With a privacy risk assessment, organizations consciously accept risk.

Mechanisms to Address Risk: Security Risk Assessment

- Conduct a Security Risk Assessment along with your Privacy Risk Assessment
- Consideration needs to be given to what is/needs to be different:
  - Asset & identity management
  - Network access levels and permissions
  - Corporate versus personal apps
  - Protection of end-user data
  - Monitoring & surveillance
  - Ensuring appropriate security controls on end-user devices
  - Theft/loss handling/protocols

Mechanisms to Address Risk: : Data Minimization & Data Mapping

- Data minimization means minimizing *opportunities* to collect personal data about others, minimizing the *amount* of personal data being collected, and minimizing *how long* personal data is retained
- Data mapping is an effective way to chart the flow of information into and out of an organization – through entities, systems and jurisdictions - and identify key risks, guiding risk mitigation strategies

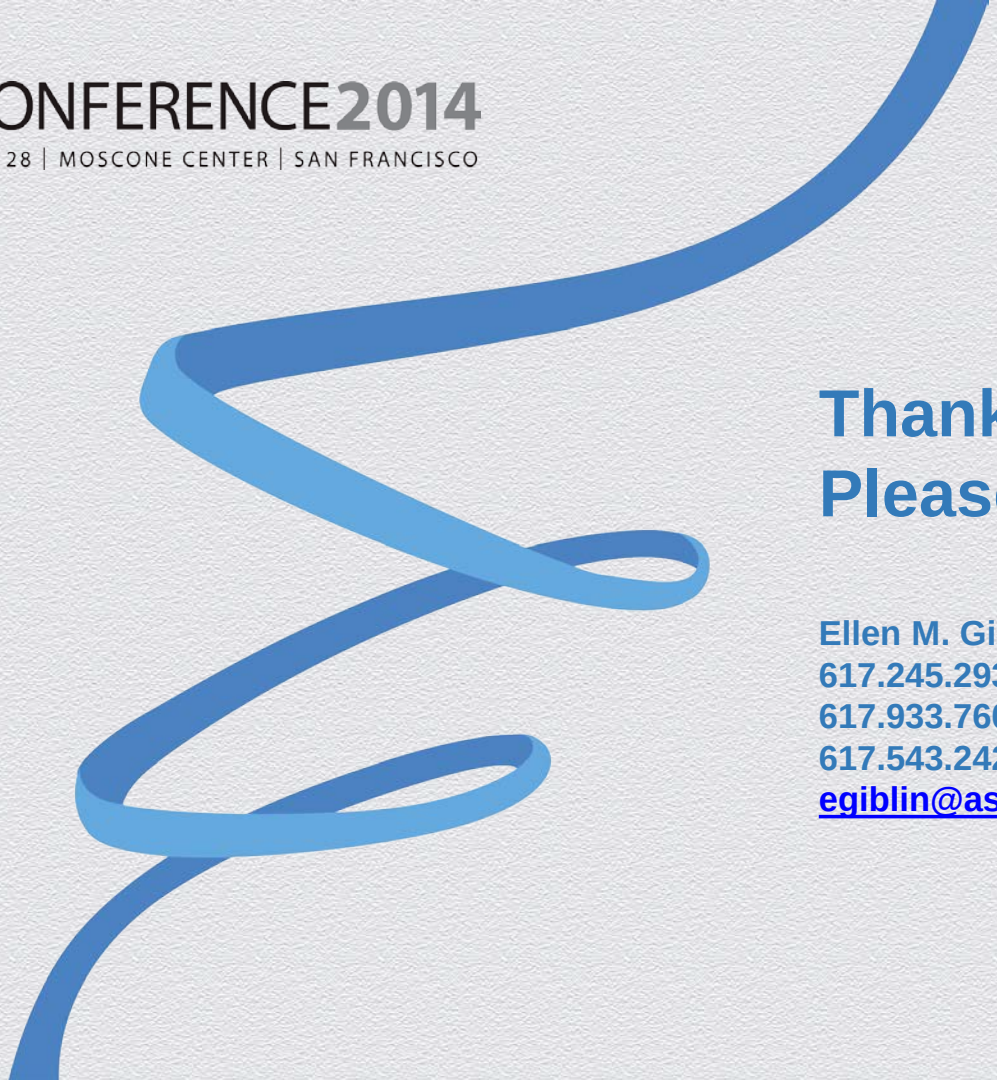
Let’s Dance

MERCER

ASHCROFT LAW FIRM™

#RSAC

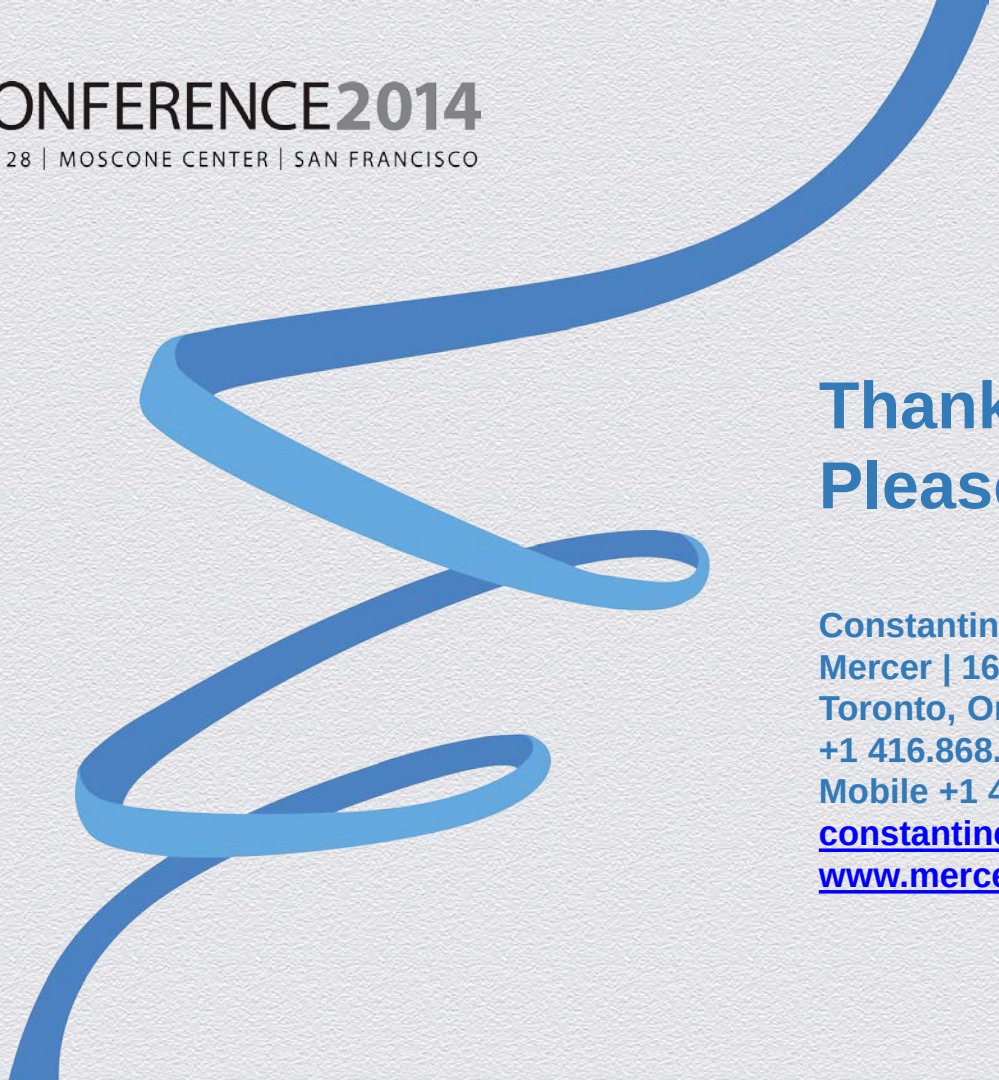
RSACONFERENCE2014



Thank You!
Please contact:

Ellen M. Giblin, Privacy Counsel, CIPP/C/G
617.245.2939 |Phone
617.933.7607 |Fax
617.543.2421 |Mobile
egiblin@ashcroftlawfirm.com |Email

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



Thank You!
Please contact:

Constantine Karbaliotis
Mercer | 161 Bay St., PO Box 501 |
Toronto, Ontario M5J 2S5, Canada
+1 416.868.2215 | Fax +1 416 868 7555 |
Mobile +1 416 402 9873 |
constantine.karbaliotis@mercer.com
www.mercer.com | Mercer