Bridging the Trust Gap for Mobile BYOD Deployments

Ojas Rege, *VP Strategy*, MobileIron

Professional Techniques – D12

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

Privacy in a BYOD World

This presentation should not be used as a substitute for competent legal advice from a licensed professional attorney in your geography.

Today's session

Objectives

- Understand the privacy expectations of the employee base
- … any how they differ by demographic and geography
- Identify BYOD best practices for your organization

Agenda

- Trust Gap results
- BYOD best practices
- Evolving approaches to privacy

Privacy in a BYOD World

Today

From the employee
- Perception
- Requirements

From the organization
- Strategy
- Best practices

Trust Gap survey

~3000 employed adults from three countries

- Germany (1,000)
- United Kingdom (1,004)
- United States (993)

Randomly selected and balanced using age and gender

Online survey from June 14-18, 2013

Conducted by Vision Critical – 3rd party

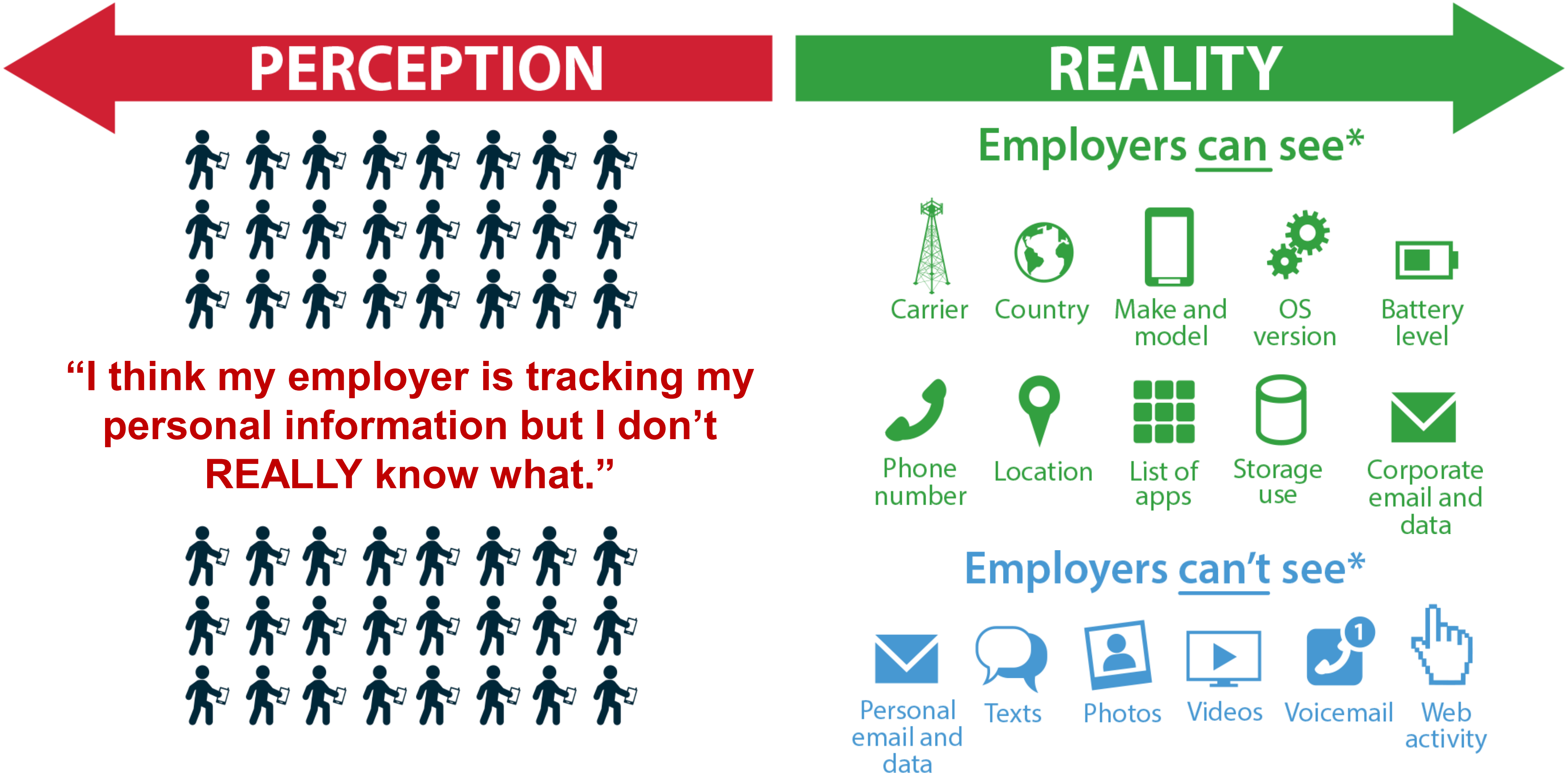
over
80%
of consumers are now using personal phones and tablets for work.

this is a
TRUST GAP
between employees and the companies they work for.

only
30%
"completely trust" their employer to keep personal information private.

why?

Employees are confused about what employers can and can't see on their mobile devices:



PERCEPTION

"I think my employer is tracking my personal information but I don't REALLY know what."

REALITY

Employers can see*

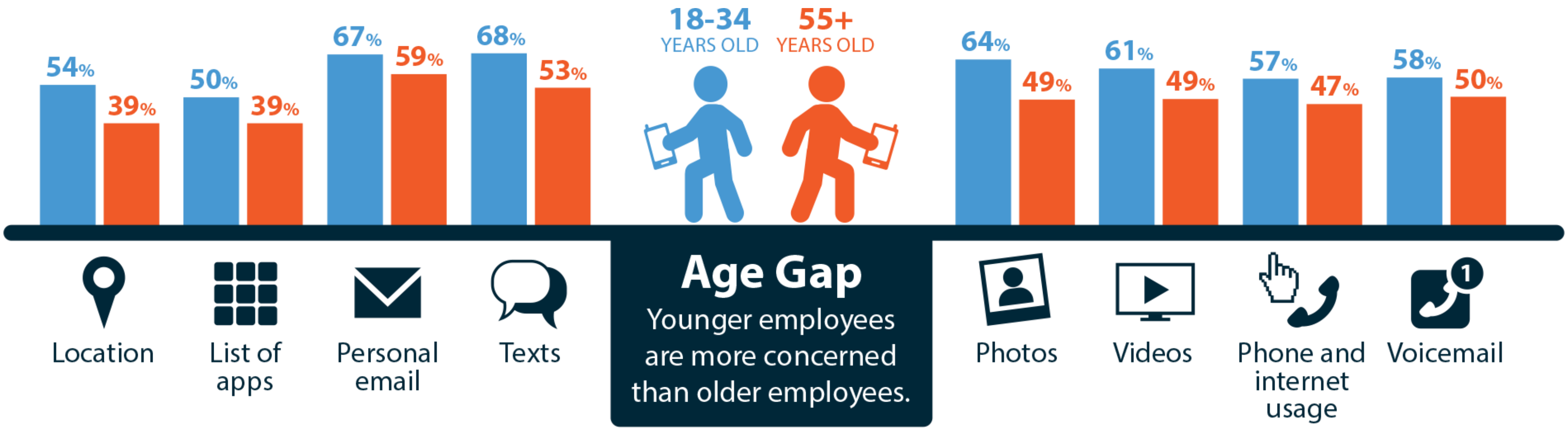
- Carrier
- Country
- Make and model
- OS version
- Battery level
- Phone number
- Location
- List of apps
- Storage use
- Corporate email and data

Employers can't see*

- Personal email and data
- Texts
- Photos
- Videos
- Voicemail
- Web activity

* Represents visibility on iOS, but will vary by mobile operating system and employer policy.

Employees are **not comfortable** with employers seeing:

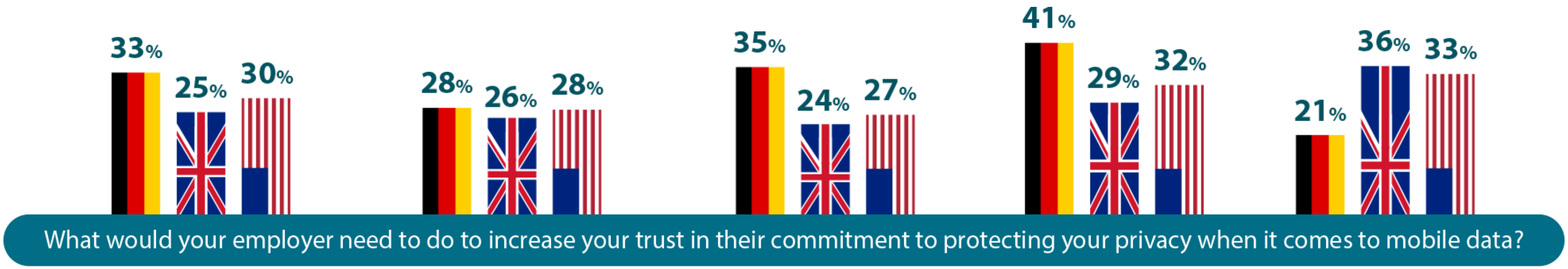


Age Gap

Younger employees are more concerned than older employees.

Communication is the way to bridge the Trust Gap

…and German employees are the most receptive:



Give me **written notification** about what they can see and what they cannot

Ask my permission in writing before accessing anything on my device

Promise in writing that they will only look at company information

Explain in detail **the purpose** of seeing certain information on my device

There is nothing they can do to increase my trust

Deploying BYOD programs

Understanding employee concerns

Managing fragmented policy ownership

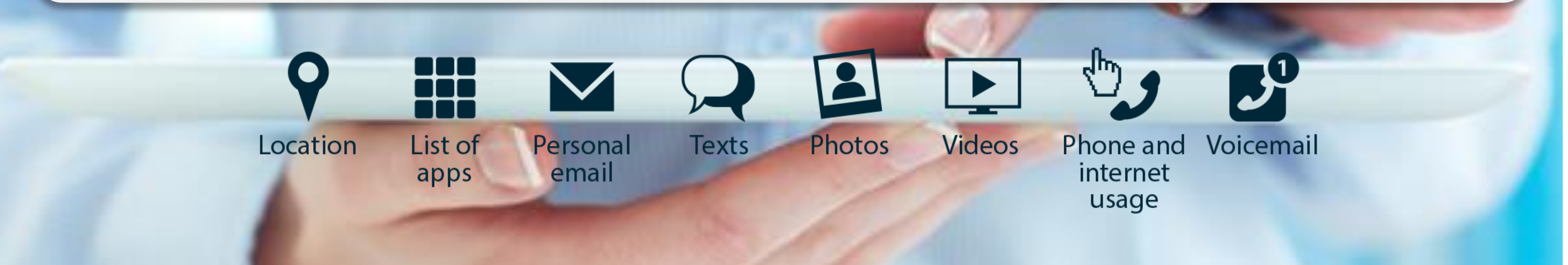
Going global – working with Works Councils

Scaling operations

Understanding employee concerns

"To what data do you have access on my mobile device?"

- List of current apps – **yes**
- Location tracking – ***available but not used***
- Personal email – **no**
- Photos – **no**
- Text messages – **no**
- Voicemails – **no**
- Device wipe – ***selective (standard) or full (exception)***



Managing fragmented policy ownership

Situation

- No clear ownership on mobile policies
- Lack of policy enforcement
- Out of date information
- Inconsistencies across mobile policies

Mobile Policy Advisory Council (MPAC)

- Cross-functional team representing HR, Legal/Compliance, Ops, Information Security, Messaging, Finance, and Telecom
- Bi-weekly cadence with agenda topics and decision timelines
- Policy alignment and ownership assignment

Going global – Works Councils

Situation

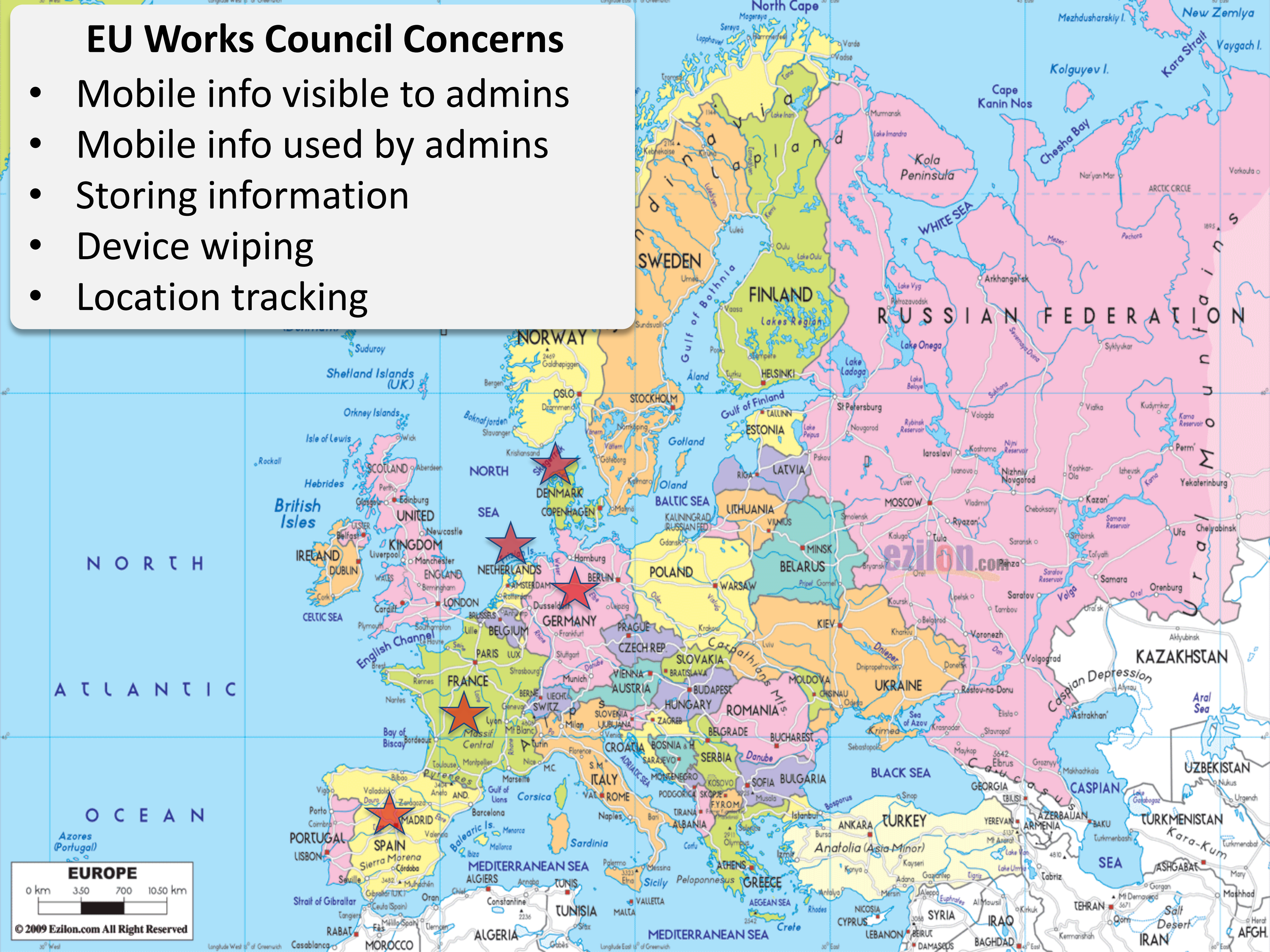
- No idea on what to expect; new area for legal dept
- Varying standards and timelines per country
- Privacy is the “hot” topic

Recommendations

- Start **early!!!** … the process can take over a year per country
- Create a template … provide outline of product/service with fairly detailed description of the information requested
- Respond quickly

EU Works Council Concerns

- Mobile info visible to admins
- Mobile info used by admins
- Storing information
- Device wiping
- Location tracking



Scaling operations

Set overall program objectives

Understand customer (i.e. employee) demographics

Make getting started REALLY easy – e.g. reg approval

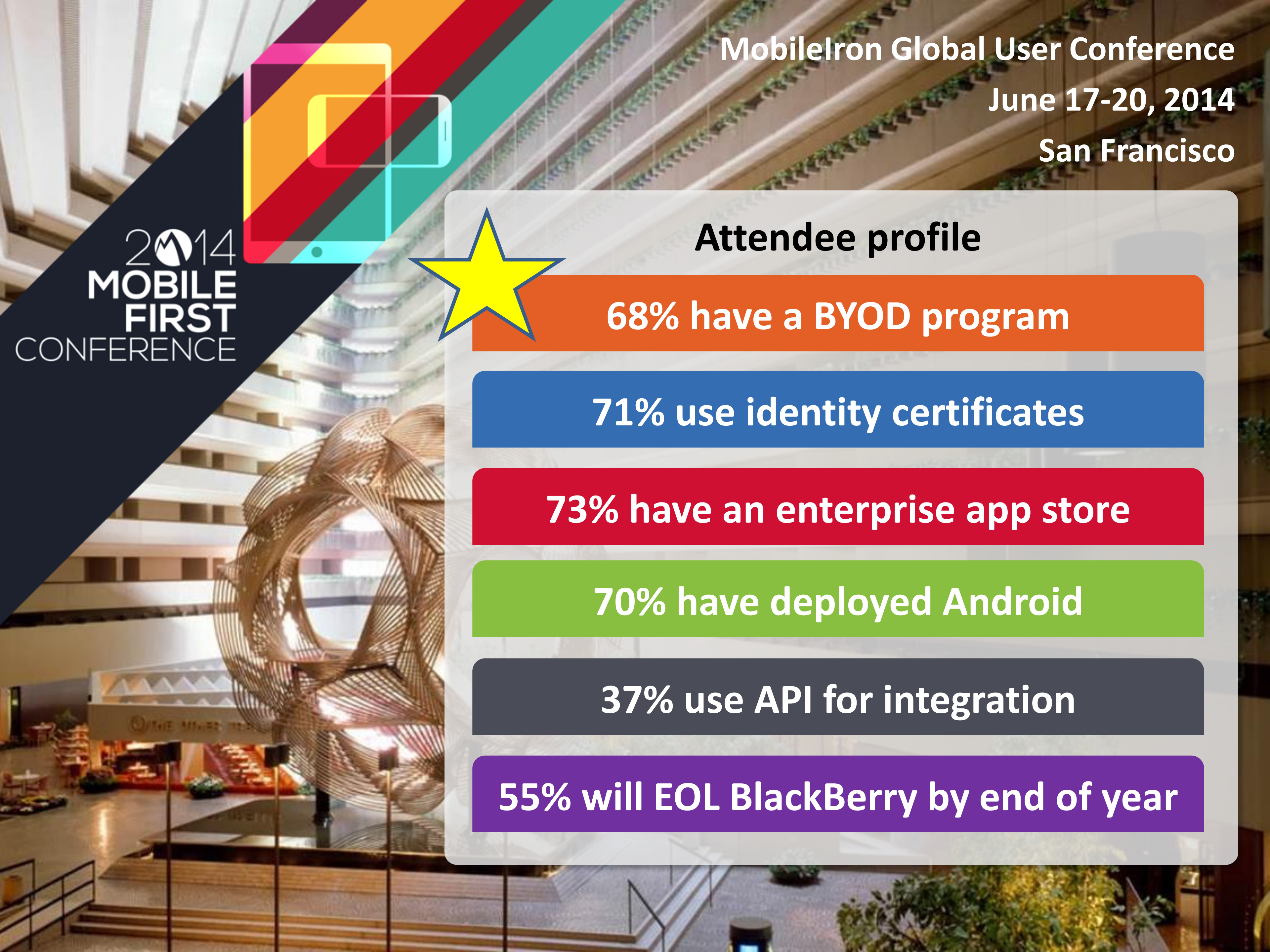
Consider early white glove treatment – learn / scale

Brand IT – show IT being user-responsive

Provide "carrot" – services of REAL end-user value

Evolving approaches to privacy

- “Reasonable expectation of privacy”
- No bright line for access
- Aligned communications
- Risk mitigation vs. adoption
- Clear process of record
- Training for edge cases
- Legitimate purpose, scope, exposure
- Public awareness: APPS act, NSA PRISM



2014
MOBILE
FIRST
CONFERENCE

MobileIron Global User Conference
June 17-20, 2014
San Francisco

Attendee profile

- 68% have a BYOD program
- 71% use identity certificates
- 73% have an enterprise app store
- 70% have deployed Android
- 37% use API for integration
- 55% will EOL BlackBerry by end of year

Major technology and business transition

1960+

Mainframe
Era

1980+

PC
Era

1995+

Internet
Era

2010+

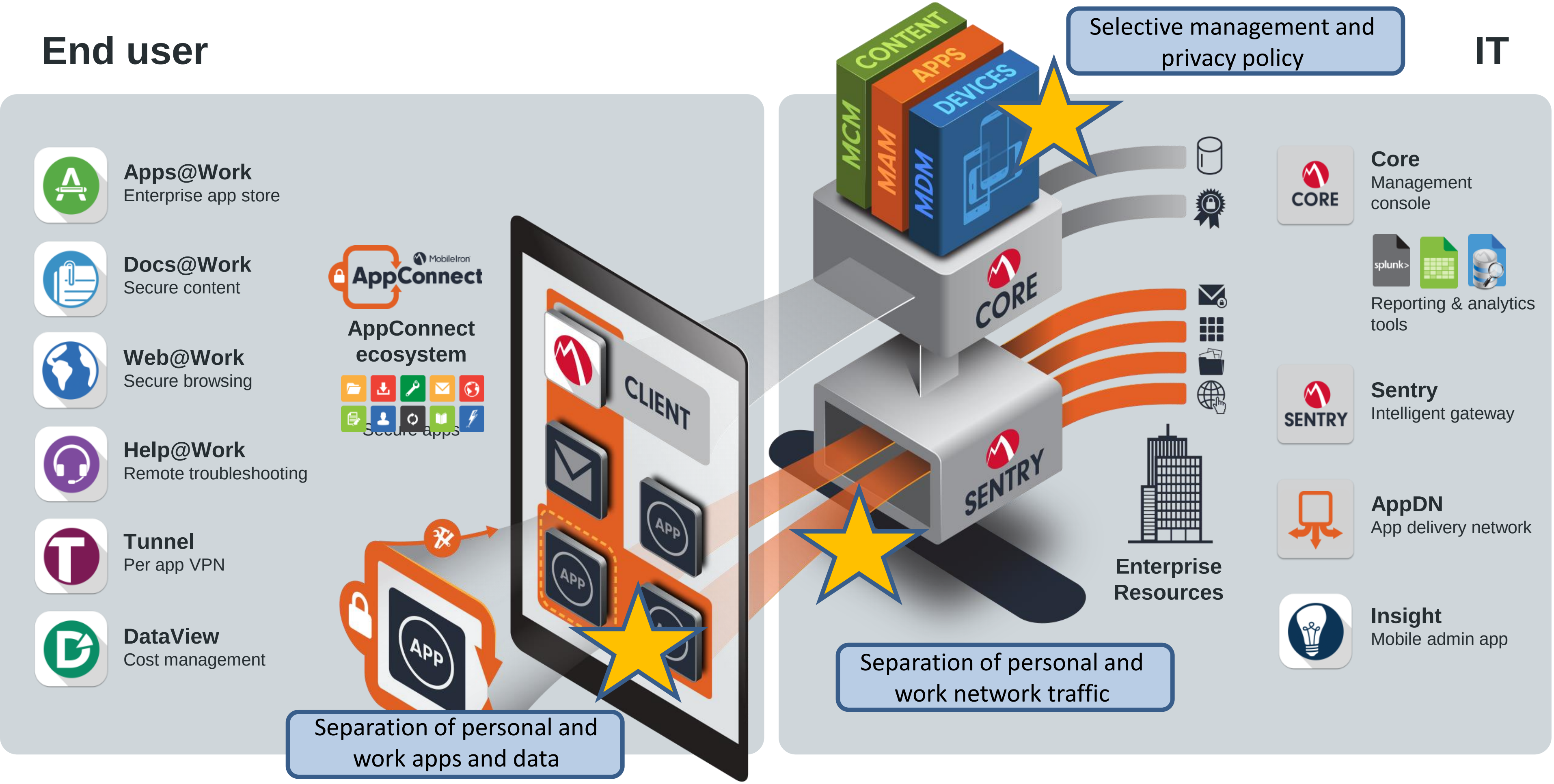
Mobile First
Era

MobileIron

Past technology transitions

- Change the way people work
- Disrupt enterprise architectures
- Create opportunities for innovation

MobileIron: Purpose-built architecture for enterprise security and management



End user

IT

Apps@Work
Enterprise app store

Docs@Work
Secure content

Web@Work
Secure browsing

Help@Work
Remote troubleshooting

Tunnel
Per app VPN

DataView
Cost management

MobileIron AppConnect

AppConnect ecosystem

Secure apps

Selective management and privacy policy

Core
Management console

Reporting & analytics tools

Sentry
Intelligent gateway

AppDN
App delivery network

Insight
Mobile admin app

Enterprise Resources

Separation of personal and work network traffic

Separation of personal and work apps and data

Mobility unlocks human potential in the workplace

Thank you!

Ojas Rege
ojas@mobileiron.com
@orege (twitter)

MobileIron®