Data Privacy Event

Bring your own device (BYOD)

Roselyn Sands  
EY Société d’Avocats France  
EMEIA Labor & Employment Law Leader

Karlheinz Mohr  
IBM  
Director IT Risk & Privacy in the Chief Information Security Office

13 February 2014  
Brussels
New technology brings more ways to access data in the “Post-PC era”, creating a shift towards BYOD.

Benefits of BYOD
- Greater job satisfaction
- Improved employee productivity
- Access of corporate information anywhere
- Reduce IT costs
- Improve user efficiency
- Avoidance of multiple devices

Economic uncertainty/Enterprise IT budget cut
Ubiquity of smartphone platforms and media tablets
Cloud computing
Social applications
3G/4G LTE
Extensive wireless network
High-level executive support

Data Privacy Event
BYODs are already a day-to-day reality in companies like IBM

IBM in a snapshot

435,000 employees (+ contractors)
50% of employees are "mobile"
600,000 managed laptops/desktops (5% personally owned)
100,000 managed mobile devices (80% personally owned)

BYOD = Bring Your Own Device
(IAPD = IBM Authorized Personal Device)
IBM has been supporting “BYOD” for many years
Mobile and consumerization of IT is simply accelerating
Key lesson: today’s employees simply expect it
…you can not stop it
…if you don’t enable it, employees will self enable
Access to BYODs may depend on employees’ positions subject to objective justification

Mobile Never
- Voice only
- User never uses mobile devices for IBM data

Mobile Optional
- Core Collaboration Apps: Email/Calendar/Contacts, Connections, Sametime

Mobile Enhanced
- Mobile Optional
  + File Sync/Backup
  + Core Enterprise Apps (w3 Intranet, Mgr tools, Expense & Time Reporting, etc)

Mobile Primary
- Mobile enhanced
  + Productivity Apps & Print
  + Role Enablement Apps (e.g., Sales = CRM, FMS, Forecasting tool, etc)

User funded (BYOD)
IBM or User funded
IBM funded
BYOD raises data security risks

Based on Gartner, Mobile Security Risks, interviews with members of ISS xForce, and Corporate Executive Board. e.g. Industry (not IBM only) view

Control Category I: Focus on risks for all mobile devices used by IBMers for IBM business purposes
Control Category II: Focus on risks for targeted populations of IBMers (ex. SVPs)
## New challenges to control the use of BYODs

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Tablet and Mac](image) | With the latest trends in technology and Tablets and Macs being everywhere and being even status symbols of executives, it is nearly impossible to keep BYOD out of your business.  
- As a result, the company is faced with SYOD (Smuggle Your Own Device). So you have a risk of losing control without any official BYOD program. |
| ![Facebook and Twitter](image) | The strategy to avoid privacy related separation of personal vs. corporate data by not allowing BYOD, does not fly as even on corporate owned devices where personal use is allowed (or even only tolerated) the same issues exist and need to be addressed by policies and procedures. |
| ![LinkedIn and YouTube](image) | Today's policies and security concepts need to be adjusted any way as we go to mobile first, always online, social/cloud computing, work life integration,...., so when we do this we have to already keep the BYOD as a phenomena in mind, even if we modify it to a rich CYOD (choose your own device) corporate program, that then still has to allow some personal/private use. |
Legal challenges as well....
Potential legal risks

- **Risk 1: Working time management**
  - Increased difficulties to monitor working time

- **Risk 2: Confidentiality issue/Access & security of company data**
  - Maintaining company data confidential
  - Risk of employee lending, losing BYOD

- **Risk 3: Private/Professional life**
  - Increased psychological risks related to the continuous access & use of information and communications

- **Risk 4: Discrimination/equality of treatment issues**
  - Who can use a BYOD?
Potential legal risks (contd)

► Risk 5: Violations of software editor licenses
  ► Who bears the responsibility? Can BYODs reduce the risk for employers? Or increase it?

► Risk 6: Who is legally responsible for the inappropriate use of BYOD?
  ► Who is liable for the use of BYOD at work for illicit purposes? (illegal downloading, hacking)
  ► Is the employer liable if it can access an application downloaded by the employee in his/her own device with automatic geo-localization?

► Risk 7: BYOD: is it a benefit in kind?
  ► Employers have the duty to provide employees with necessary means to perform their duties
  ► How does one account for BYOD? Compensation of the employee? subject to social security contributions?
Is the law keeping up with technology and practices? Unchartered waters: BYOD – related legislation/case-law?

No specific legislation in Europe:
- **European Union**: Proposition European Regulation 2012 (should be enforced in May 2014) aiming to reinforce the rules on data protection in the employment relationships.
- **Countries: France, Spain, Netherland, Germany or Italy**: No specific legislation, existing legislation may apply but does not directly address BYOD

Guidance in the UK on the protection of data:
- Information Commissioner’s Office (ICO) has released guidance
- Issues raises, e.g.: how will the device be controlled, if lost, or employment terminated?
- Recommendations given, e.g.: register devices with a remote locate and wipe facility

Case-law in European Countries:
- No direct cases at the European level
- France, Germany, Italy, Spain and Netherlands: no case-law directly linked to BYODs
- In France and Germany, Courts have ruled on “smuggled” BYOD

**Conclusion**: as always, reality is ahead of the law and the law catches up!
Is the law keeping up with technology and practices? Insights from French Courts…

1) The Dictaphone case: French Supreme Court May 23, 2012:

► Facts:
  ► An employee brought her personal Dictaphone to work, recorded conversations with her co-workers, without their knowledge or consent.
  ► The employer discovered the Dictaphone on “record mode” in the offices and immediately listened to its content, while its owner was absent. The employee was consequently dismissed for gross misconduct.

► Decision: The French Supreme Court ruled that the dismissal was unfair since:
  ► The employer should not have listened to the recording without the presence of the employee or at least with prior warning;
  ► The employer destroyed the recording, no respect of the adversarial procedure!
Is the law keeping up with technology and practices? Insights from French Courts…. (contd)

2) USB key case: French Supreme Court February 12, 2013:

► Facts:
  ► An employee copied confidential and personal files of her employer and co-workers on her personal USB key, plugged into her company computer.
  ► While the employee was away from the office, the employer took and read the information on the USB key, and discovered the copied files. She was dismissed for gross misconduct.

► Decision: The French Supreme Court ruled that:
  ► As the USB key was plugged into the company’s computer provided to the employee, the USB key was presumed to be used for professional purposes.
  ► Therefore, the employer was entitled to access files which were not identified as “personal” contained in the USB key, without needing the employee’s presence, or prior warning.
BYODs must be regulated by several tools

**Education**
- Formal
- Casual
- Social
- Developer

**Strategy**
- Acceptance
- Personas
- “Day In The Life”
- Funding Models

**Technology**
- Endpoint
- Management
- Anti-Malware
- Network Access Control
- Application Security
- Containerization/Virtualization

**Policy**
- Legal
- General controls
- Technical controls
- Support
Examples of agreements on BYODs

► Terms & conditions for personal devices should include topics such as:

**Employee will:**
- Understand use of the device is governed by enterprise rules
- Allow installation of enterprise management agents
- Understand enterprise can wipe all *work* data/property off device
- Ensure all software on device is fully licensed
- If device is lost/stolen, call in as enterprise security incident
- Not share the device with non employees
- Must understand enterprise can revoke right to use device

**Company will:**
- Honor data privacy laws and employee’s private life
- Not wipe full device without asking permission
- Not track users geo-location without permission
- Provide for a compensation of the professional use (under French law)
- Do not remove the use of BYOD suddenly
Examples of an implementation check-list

- **Legal tools:**
  - **Internal rules:**
    - Reminder to employees of their responsibilities when using BYODs
    - Reminder to employees of potential disciplinary measures in case of violation of protection rules (e.g.: breach of the confidentiality obligation)
  - **IT Charters:**
    - Provide for “good practices” and rules when using BYODs
    - Provide for data protection rules (antivirus, software, password…)
  - **Employment contract:**
    - A clause agreeing on BYODs use and employee’s obligations
    - And agreeing on the financial compensation for the use of BYODs
  - **Legal Action:** final option
    - Prevent employee’s breach of rules on confidentiality
    - French specific legal action: obtain proof of non-compliance with the adversarial principle at the beginning of the legal procedure
Examples of an implementation check-list (contd)

HR tools:
- **Internal audit** of the company: determine existing BYODs and needs
- Determine **objective categories of employees** and type of devices concerned
- Involve staff representatives and employees in the **creation of a policy**.
- Develop a **participative management** to encourage employees’ involvement: mobilize staff, create and organize a dialogue in order to listen and share information and knowledge.
- Make sure your employees are **aware of the benefits and issues** of BYOD: meetings, training, information displayed within the company.

IT tools:
- Provide the employee with company anti-virus
- Access control and frequent change of password
- Prohibition to download certain applications
- Audit and control of material
- Locking system
- Mobile Device Management (MDM): conditioning the network connection
Summary of issues to consider

- Data Privacy Event
- Internal rules
- IT Charters
- Employment Contracts
- Daily Monitoring
- Legal Action
- Security rules
- Network monitoring
- Software restrictions
- Working time compliance
- Proportionate disciplinary measures
- Rules on internet use
- Private life preservation
- Confidentiality

- Rules on internet use
BYOD definitely a challenge!

The various legal tools, such as **Employment contracts, IT Charts/Code** of conducts or internal rules, are at heart of the BYOD issue:

- They will allow employers to manage risk, and if necessary, monitor and sanction employees;
- They also give employees a sense of responsibility by giving them rights and obligations.

Whilst IT and Human resources issues also need to be addressed, BYODs necessarily require trust in employees. Therefore, good management and a trusting culture are a “must”!
Questions?
Thank you
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 EYGM Limited.
All Rights Reserved.
EYG no. ED 524899
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com