Employee Data Privacy in a Globalized Workforce

Barbara Hoey, Partner and Chair, Kelley Drye Labor and Employment Practice

Mark Konkel, Partner, Kelley Drye Labor and Employment Practice

Minjoo Lee, Assistant General Counsel, Employment Law Regulatory, JP Morgan Chase & Co.

July 22, 2015
Part One

Computers Don’t Compromise Security, People Do:
Real World Examples of How Employees Factor into Legal Privacy and Security Risk
# Real World Hypothetical # 1

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>SSN</th>
<th>DOB</th>
<th>Employment Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smith, Jane</td>
<td>170 Centre Street, Fairfield, CT</td>
<td>548-85-6415</td>
<td>05/08/1975</td>
<td>Employed</td>
</tr>
<tr>
<td>Smith, John</td>
<td>101 Park Avenue, New York, NY</td>
<td>105-54-5412</td>
<td>11/21/1981</td>
<td>Terminated</td>
</tr>
</tbody>
</table>
Issue-Spotting: What Could Possibly Go Wrong?

- State data breach notification laws
- Internal management
- Equal Employment Opportunity issues
Real World Hypothetical # 2
Issue-Spotting: What Could Possibly Go Wrong?

• What could/should the company have done prior to the employee’s departure?
  • Take additional steps to protect valuable data
  • Implement a pre-departure inspection
  • Set parameters for the non-retention of company data post-employment
  • Establish a litigation strategy
Real World Hypothetical # 3

[Image of a cell phone displaying a Gmail inbox with various messages]
Issue-Spotting: What Could Possibly Go Wrong?

- Employee consent
- Employee handbook disclaimer
- How should the employer have acted?
Real World Hypothetical # 4
Issue-Spotting: What Could Possibly Go Wrong?

- What is the potential exposure?
  - Federal law
  - State law
  - NLRA

- What questions should employers be asking?

- The fact is, most employers have access to this information
  - Challenge: Will you use it and how?
Contributing Factors to Employer Data Dilemmas

• Data no longer “live” in one place

• Too many companies still use the concept of paper-copy “files” as an analogue for electronic data

• Mobile devices, cloud computing, and remote access to work systems blur the line between the company’s workspace and the employee’s private space

• How can a company monitor, protect, use, and disclose data appropriately and legally?
Contributing Factors to Employer Data Dilemmas

BYOD Policies in Place By Company Size And Industry

- Finance / Insurance
- Healthcare
- Professional Services
- Manufacturing
- Transportation / Logistics
- Legal
- Communications
- Government (Federal)
- Software
- Entertainment / Media
- Retail / Wholesale
- Life Sciences
- Government (Local)
Hackers or Employees?

2015 Verizon Data Breach Investigations Report

- MISCELLANEOUS ERRORS: 29.4%
- CRIMEWARE: 25.1%
- INSIDER MISUSE: 20.6%
- PHYSICAL THEFT/LOSS: 15.3%
- WEB APP ATTACKS: 4.1%
- DENIAL OF SERVICE: 3.9%
- CYBER-ESPIONAGE: 0.8%
- POS INTRUSIONS: 0.7%
- PAYMENT CARD SKIMMERS: 0.1%
Hackers or Employees? Drilling Down…

INSIDER MISUSE

2015 Verizon Data Breach Investigations Report
The Aftermath: Breaches are Costly

- Average U.S. data breach cost (2015) = $6.5 million per incident
  - Includes detection, escalation, notification, remediation, lost business
- Also invites:
  - Lawsuits and/or government investigations (increasing $$$ exposure)
  - Employee morale takes a hit
  - Negative media coverage
- But do these factors motivate proactive compliance and dedicated security resources?

Ponemon Institute, 2015 Cost of Data Breach Study: United States
Part Two

Privacy Rights in the Workplace:
Challenges for Multinationals
What Is “Personal Data” in the U.S.?

No single definition, but generally non-public personal information, such as:

- Social Security number
- Date of birth
- Protected class information
- Medical records
- Communications of an entirely personal nature?
- “Employees” often construed as “consumers” under consumer protection laws, bringing within scope broad “personally identifiable information” definitions as well
What is “Personal Data” in the EU?

- **Personal data** are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[.]" 

- Translation: **broader definition of personal data than in the U.S.**
Expanding Borders: Tackling International Issues
Data Breaches in the EU

- Volume of Records Breached (Millions)
- Number of Breach Incidents

Graph showing the volume of records breached and number of breach incidents from 2005 to 2014.
EUROPE: One Set of Rules

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free
movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF
THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in
Article 189b of the Treaty (3),

Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured
require not only that personal data should be able
flow freely (4) across Member States and

Google

Notice of removal from Google Search

We regret to inform you that we are no longer able to show the following pages from your website in response to certain searches on European versions of Google:


For more information, see
https://www.google.com/policies/faq/?hl=en
Europe: One Set of Rules

- The European Commission plans to unify data protection within the EU with a single law, the General Data Protection Regulation (GDPR).

Europe: One Set of Rules

Still lots of controversy, but GDPR is expected to:

- Apply a single set of rules
- Broad definition of “personal data”
- Apply to all “organizations” of any kind that gather or maintain personal data
- Apply extra-territorially
- Require multinationals to appoint cross-border Data Protection Officers (more than 250 employees)
- More stringent breach reporting obligations
- Allow employees a “right to be forgotten” – i.e., companies would have to erase personal data where the interest of the company are “overridden by the interests or fundamental rights and freedoms of the data subject”
In Contrast: A Patchwork of U.S. Privacy Laws

Employee Privacy

State Law
- Statutes

Federal Law
- Common law
- Regulatory Authority (NLRB)
In Contrast: Patchwork of U.S. Data Security Laws

- Federal Law:
  - FTC Act
  - HIPAA
  - COPPA

- State Law:
  - GLBA
  - FCRA
  - Information Disclosure
  - Information Security
  - SSN Protection
Employee Emails in the UK

Gosden v. Lifeline Project Ltd.
Facebook in Italy

- Dismissed employee insulted former manager on Facebook
- Messages contained vulgar and explicit language ("Pezzi di merda")
- Former employee is accused of defamation

*Tribunale Livorno*
What Would Have Happened in the U.S.?

- In heated union organizing campaign at a restaurant, a food server took to his Facebook page and posted, rather mildly, that his boss was:
  
  Such a NASTY MOTHER F*****R
  
  F**k his mother and his entire f*****g family!!! . . . Vote YES for the UNION!!!!!

- Shockingly, the server was fired

- The former employee filed an unfair labor practice with the NRLB

- The NLRB found that the server’s speech was protected under Section 7 of the NLRA

*Pier Sixty LLC, 362 NLRB No. 59 (March 31, 2015)*
Employee Data Protection & Privacy Approach for Multinationals

1. Global/Regional Data Privacy Legal Review
   - Review of the data privacy laws for the region or the country.
   - There may be corporate policies or other forms that will need to be implemented in order to properly store or transfer employee data.

2. Regional/Local Employment & Labor Law Review
   - Works councils or other organized labor organization may have the right to review/comment on employee data related practices or policies.
   - There may be consent requirements.

3. Regional Data Privacy Compliance Review
   - Review/cooperation with regulators in the country or regions, e.g. the CNPD in Luxembourg, may be required.

4. Local Regulatory & Technology Compliance Review
   - There may be technical requirements that do not relate specifically to employee data, but rather to the technical requirements applicable generally to your company.

Common Information Requirements

- **What** data is being collected
- **Why** is the data being collected
- **Where** is the data being stored
- **How** will the data be used
- **Who** will have access to the data
- Will the data be transferred, and if so, how/where
Part Three

Avoiding the Landmines:
Top 7 Strategies for Striking the Right Balance
1) Develop a Data Security/HR Partnership

Information Technology

Human Resources
2) **Ensure Basic Security**

1. Written and implemented information security program

2. Avoid the low hanging fruit…
   1. Train employees on basic privacy/security obligations relevant to their roles
   2. Have a data breach plan in place
   3. Require registration of personal devices
   4. Ensure a “remote wipe” capability
   5. Use inactivity timers
   6. Require meaningful password protection
3) Obtain Employee Consent

Obtain employee consent to:

1. Install, modify, and remove security controls
2. Remotely wipe a device and **everything** on it
3. Monitor the device when it accesses a corporate network
4. Inspect the device for legitimate business purposes, even if the device is personal
5. Image the device to implement a litigation hold
6. Access company information stored in the employee’s cloud account
7. Perform background/credit checks and provide appropriate notice afterwards if there is an adverse decision
4) Think About Onboarding

- Advise each new employee of the company’s expectations regarding the protection of confidential information and critical infrastructure
- Offer in-depth explanations of any policies
- Establish employee accountability
Get the Right Agreements in Place

- Carefully define “company property”
- Reserve broad rights to examine employee personal devices
- Require the employee’s signed acknowledgment of compliance upon separation
- Define the company’s entitlement to immediate injunctive relief to compel compliance
6) Be Careful with Departures

- Insider threats typically occur within 30 days of announcement of departure

- Limit or prevent access:
  - Institute a protocol to remove or limit access to confidential information
  - Audit the employee’s previous access to ensure the employee did not harvest any confidential information

- For terminated employees, ensure reduction of access **before** you tell them
7) Be Careful When You Monitor
Questions?