Presenters

Moderator

Michael Porter, Partner, Miller Nash LLP, Portland, Oregon, USA
mike.porter@millernash.com
Presenters

Speakers

**Sonia Cortes**, Partner, Cuatrecasas, Gonçalves Pereira, Barcelona, Spain
sonia.cortes@cuatrecasas.com

**Olle Jansson**, Partner, Kilpatrick Townsend & Stockton LLP, Stockholm, Sweden
ojansson@kilpatricktownsend.com
Presenters

Speakers

michael.leftley@addleshawgoddard.com

Jan Tibor Lelley, Partner, Buse Heberer Fromm, Essen Germany
lelley@buse.de
Angelo Zambelli, Partner, Grimaldi Studio Legale, Milan, Italy
azambelli@grimaldilex.com
Workplace privacy and employee monitoring: the do’s and don’ts
Workplace Privacy: Spain

- Conflict between employees’ fundamental right to privacy and employers’ right to business
Workplace Privacy: Spain

Sustaining employee rights: the Do’s

• Implement company policy, i.e., inform employees:
  – They should expect no privacy of IT use
  – Random controls may be carried out

• Forbid or limit employees’ private use of IT
Workplace Privacy: Spain

• Video surveillance:
  – Prior information: works council & notice
  – Proportionality & reasonability tests:
    • Limit to business needs
    • Limitations to storage term
    • Choose the least interference procedure
Workplace Privacy: Spain

Sustaining employee rights: the Don’ts

• Unjustified controls / surveillance
• Excessive or inappropriate controls/surveillance
  ⇒ conform to the specific justifying purpose or business needs
Workplace Privacy: Spain

- Avoid tolerance of private use of IT by employees
- In Europe, avoid infringement of Data Protection Directive: data base registration, prior information, limit to purpose, comply with law for personal data transfers to the U.S., etc.
Workplace Privacy: Sweden

- Employers’ right to lead and delegate work
- Control employees’ e-mails?
- Monitor employees’ internet activities?
- Video surveillance?
- Biometric identifiers?
Workplace Privacy: Germany

- Video surveillance
- Monitoring of internet and email use
- Global Positioning System (GPS)
- Electronic and bio-metric access surveillance to office buildings and/or workplace
Workplace Privacy: Germany

- Let your employees consent!
- Have a legal basis at hand for monitoring with technical devices!
- Obey data privacy laws [e.g. Federal Data Protection Act – BDSG]!
- Involve your works council before you start!
- Involve your data privacy officer!
Workplace Privacy: England & Wales

- Monitoring employee use of email and internet involves processing personal data and must be in line with the Data Protection Act 1998.
- Any monitoring must be for lawful purposes and must be proportionate.
Workplace Privacy: England & Wales

- Potentially lawful purposes include: investigating serious misconduct, health and safety and service standards.
- Obligation to inform employees.
- Impact assessments
Workplace Privacy: Italy

General principle:
Ban on distance monitoring devices directly aimed at controlling the employees' work activities/performance (keystroke pattern analysis, systematic scanning and recording of e-mail messages, systematic storage of web pages visited, etc).
Workplace Privacy: Italy

Exceptions:

• Unintentional controls (with prior works’ council agreement or labour office authorization)

• Defensive monitoring (always allowed)
Holding applicants and employees responsible for tweeting, blogging, and using social media
Tweeting, Blogging, etc.: Germany

• Differentiate between communication at work and …
• Communication elsewhere
• Freedom of speech as constitutional right - even at work
• German labor courts are reluctant with accountability for use of social media
Tweeting, Blogging, etc.: Germany

• Make a social media guideline mandatory:
  – Prohibit private use of social media at work
  – Create rules for private use – if allowed
  – Make compliance with laws an express duty
  – Prohibit sharing of trade secrets and company‘s intern information
  – Make clear the consequences for violations (e.g., warning, termination of employment)
Tweeting, Blogging, etc.: Italy

- Guidelines issued by the Data Protection Authority in March 2007
- Internal policies on the use of the Internet, e-mail accounts, etc. from company devices
- Use of social networks and the Internet during working hours: performance of activities other than work during work time and disciplinary consequences
Tweeting, Blogging, etc.: Italy

- Cases of dismissal based on social media information: they mainly relate to the misuse (or use against the company policies) of the Internet – including Facebook – during work hours
Tweeting, Blogging, etc.: England & Wales

- Clear policies and procedures
- Acceptable use
- Bullying and harassment
- Employer reputation
Tweeting, Blogging, etc.: Spain

• Ensure implementation of appropriate company policy to:
  – Allow obtaining lawful evidence to use in trial
  – Avoid tolerance
• Court decisions assess severe loss of working time as breach of duty
• Importance of the test of proportionality and reasonability
“Tweeting, Blogging, etc.: Sweden

- Duty of loyalty
- Freedom of speech
- Employees working in private vs. public sector
- “The high school principal”
Differentiating between personal and work-related communication
Communication: England & Wales

- Employer reputation paramount
- Can there be a legitimate expectation of privacy when using social media?
- During work vs. outside of work?
- Can an employer take account of private activities?
Employment reputation

- In the UK, employer reputation is a key theme running through cases involving misuse of social media.
- Dismissals have been found to be fair where:
  - Email is sent to client from home computer
  - Derogatory comments made on Facebook
  - Employee involved in BDSM activities on web-unrelated to work
Communication: England & Wales

Expectation of privacy when using social media

• Comments posted on social media sites by their nature are public

• Potential readership will be relevant to the reasonableness of the sanction imposed
Communication: England & Wales

During work vs. outside of work

• During work
  – Issues around unreasonable usage

• Outside of work
  – Inappropriate private behaviour
  – Criticising the employer
  – Bullying and harassment
Private activities

• An employer can take account of private activities but only in limited circumstances

• Where private matters interfere with ability to carry out duties
Communication: Sweden

- Work equipment
- Guidelines
- Private vs. work-related e-mails
• Major distinction: is personal use of employer’s communication tools (internet, email, smartphone etc.) allowed?

• Telecommunication privacy privilege (Telekommunikationgesetz) applicable to all personal communication

• Generally no monitoring permissible if telecommunication privacy privilege is applicable
Communication: Germany

- All work-related communication can be legally monitored
- Telecommunication privacy privilege applicable only during transfer of data
- Telecommunication privacy privilege applicable only if information is classified as “private”
Communication: Germany

- Unauthorised monitoring of private communication can be considered a criminal offense (Section 206 Criminal Code, Section 202 a Criminal Code – StGB)
Communication: Italy

- Monitoring allowed if:
  - Employee uses employer-owned and controlled equipment or networks;
  - Employer has a clear computer use policy;
  - Prior agreement with works council or labour office authorization.
Communication: Italy

• Disclosure of company’s confidential information: balance between employee’s privacy rights and employer’s right to protect its interests. The latter prevails.

• Monitoring of unlawful activity carried out by the employee – including the one perpetrated through social networks – is legitimate (defensive monitoring).
Communication: Italy

- Negative statements about the company: individual freedom to express one’s opinion(s).
- Limit: damage of the company’s reputation (libel - defamation).
Communication: Spain

• **At work:** Unreasonable usage or inappropriate behaviour

• **Out of work:** Protected by privacy and right to freedom of speech. Employer can interfere only if it has a relevant impact:
  – Interference with other employees’ fundamental rights, e.g., discrimination (race, gender, etc.)
  – Inappropriate behaviour having a relevant impact on employer’s business
When and how background checks can include obtaining information on the Web
Background Checks & the Web: Italy

Ban to process information regarding the candidate that is not relevant to assess his/her professional attitude, irrespective of any written consent given:

- Politics
- Religion
- Trade union affiliation
- Any other data irrelevant for performing working activities
Exception:
Organization with specific tendencies (such as religious schools or political parties), provided that the role to be assigned to the candidate is not “neutral”
Background Checks & the Web: Italy

- Examples of forbidden background checks:
  - Kinship with other employees;
  - Criminal records (except for specific types of activities);
  - Pregnancy;
  - Sexual orientation
  - Candidate's health conditions (unless relevant for performing the job functions)
Background Checks & the Web: Italy

• Examples of permitted background checks:
  • Identity of the candidate;
  • Previous work experience;
  • School/training/professional qualification;
  • Attitude/psychological tests
The law permits employers to access and rely on information about an employee that is publicly available unless it relates to a protected characteristic, such as race or disability, or a protected activity, such as a union affiliation.

The same rules apply to job applicants.

Employers may not use coercion or fraudulent means to access a candidate’s social network posts or contents where the candidate has taken steps to secure the information or otherwise keep it private.
Background Checks & the Web: Spain

- Required justification to access private websites, particularly where access has been limited

- Justification related to nature of job, particularly where health and safety are involved
Background Checks & the Web: Sweden

- *Obtaining* of information is always allowed
- If the information is *being kept* in automated/organised files, the Personal Data Act requires the following:
Background Checks & the Web: Sweden

1. Only authorities are generally allowed to keep data concerning legal offences.

2. The employee has the right to be informed of the information registered through the background check.
Background Checks & the Web: Sweden

3. Consent is required for: (i) sensitive personal data and (ii) financial information that is not obtained before hiring for an executive position or a position with great financial responsibility. A weighing is always being done when there is no consent.

4. The personal data can not be kept for longer than necessary with regards to the purpose of the treatment of the data.
Background Checks & the Web: England & Wales

- Do employers vet online?
- Risks? - discrimination
- Approach, when to vet in the process, consistency, verification.
Background Checks & the Web: Germany

- Background check offline and online
- Legal and illegal information
- No transparent applicant or employee
- Co-determination of works council
- Review by data privacy officer
Background Checks & the Web: Germany

- Legal information from background checks on the web:
  - Any information that is work related; and
  - Is directly connected to the employee’s position or for which an applicant is hired
Background Checks & the Web: Germany

- Illegal information from background checks on the web:
  - Any information that is not work-related or related to the position to which the applicant has applied
  - Any facts that could be used as basis to discriminate against the applicant
Data protection and privacy issues
Data Protection & Privacy: Sweden

- The Personal Data Act
- General rule: the employee’s consent is required
- Weighing of interests
- Sensitive personal data
- Transfer of personal data within the EU/EES
- Transfer of personal data to a third country
- The Safe Harbour Principles
Data Protection & Privacy: Spain

- Restrictions to body search and search of employee’s lockers
- Whistleblowing
  - No anonymous whistleblowing
  - Limited storage of data
- Employee representatives’ right to certain employee information
Data Protection & Privacy: Italy

- Personal data: processing only with the express consent of the employee, documented in writing.

- Consent not required if the processing is necessary either to comply with an obligation imposed by the law, regulations, and EU legislation or for performing obligations resulting from a contract (example: pre-contractual use of personal data for recruitment purposes).
Data Protection & Privacy: Italy

• Sensitive data: processing without consent provided that the Data Protection Authority allows it (general authorization no. 1/2011).
Data Protection & Privacy: Germany

• Federal data protection act (Bundesdatenschutzgesetz – BDSG) applicable to collecting, using, and monitoring personal data.

• General rule: collecting, using and monitoring personal data is prohibited unless:
  – Employee consents expressly in writing
  – Law expressly allows it.
32 BDSG provides for legal basis to collect, use, and monitor data legally at work.

Company’s data privacy officer has to review and confirm.

Works council can claim co-determination.
Data Protection & Privacy: England & Wales

- Data Protection Act 1998
- The Employment Practices Code
Please Complete Our Survey

Please take a few minutes to complete the survey that should appear on your computer screen immediately following the webinar.

To listen to this webinar again or to any past ELA webinars, please visit our website at: www.employmentlawalliance.com.

The ELA is not authorized to give Continuing Education credit for its webinars; however, a Certificate of Attendance and supporting materials are now posted on the ELA website (click this webinar’s title; the link is on the landing page). Attendees seeking HRCI or SHRM credit should submit the materials directly to HRCI at www.hrci.org or to SHRM at www.shrm.org.