



EUROPÄISCHE AKADEMIE

zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH

Direktor: Professor Dr. Dr. h. c. Carl Friedrich Gethmann

“Big brother on my desk” –

Can office surveillance systems be compatible with privacy protection at the workplace?

A question of legal clarity and corporate responsibility

Katja Stoppenbrink, LL.M., M.A., Maître en Droit

*(Europäische Akademie zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen,
Bad Neuenahr-Ahrweiler, Germany)*

PRISE Final Conference – AGENDA

**Towards privacy enhancing security technologies – the next steps
28th and 29th of April 2008, Austrian Academy of Sciences, Vienna**

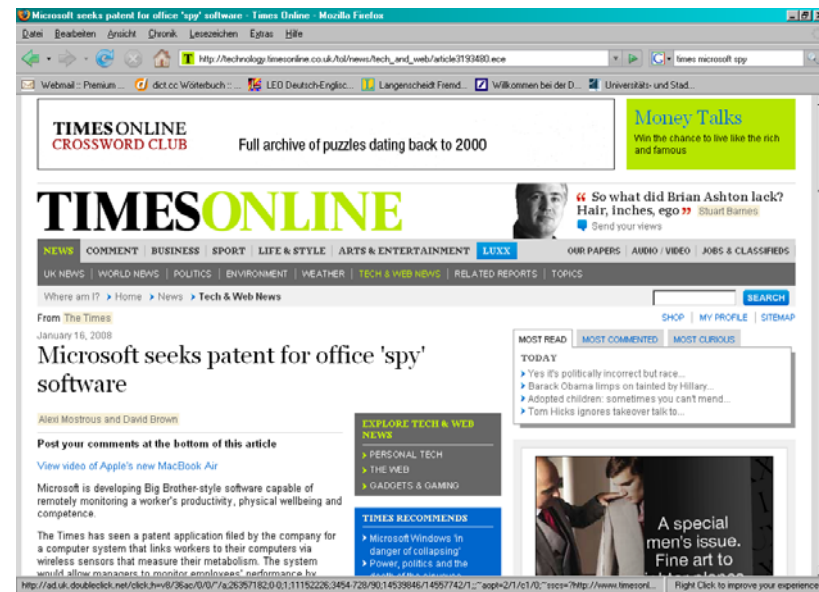
Introduction: Challenges to Workplace Privacy posed by (future) office surveillance systems

Patent application pending in the US:

- Microsoft Corp. developing “a unique activity monitoring system” [27.06.06]
- Thought experiment or future threat to privacy?

Recent cases from Germany:

- Covert video surveillance in supermarkets and slaughterhouses directed at customers **and** workers
- Illegal but *normal* application?



http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193480.ece [16.01.2008]

No. 17, 17.04.2008

<http://www.stern.de/magazin/heft/617346.html>

Workplace Privacy Protection: **Six Theses**

1. Security vs. privacy dilemma in private contexts
2. Problems of intra-corporate law enforcement and compliance
3. New quality of privacy invasions through office surveillance systems
4. Complex and "pointillist" legal landscape
5. Employee data protection agenda
6. CR as a worldwide approach to privacy protection

Workplace Privacy Protection: Objectives

These **six hypotheses** capture the distinctive features of the **security vs. privacy dilemma in private contexts** (as opposed to problems related to policing and/or the public sphere).

Their objective is an attempt to strike a **balance between conflicting** privacy and security **interests in employer-employee relationships** based on an adequate understanding of legal requirements, business ethics and corporate responsibility.

 The aim: an affirmative answer to the **compatibility question**.

Workplace Privacy Protection: **Overview**

- 1. Security vs. privacy dilemma in private contexts**
2. Problems of intra-corporate law enforcement and compliance
3. New quality of privacy invasions through office surveillance systems
4. Complex and "pointillist" legal landscape
5. Employee data protection agenda
6. CR as a worldwide approach to privacy protection

1st Thesis: **Security vs. Privacy Dilemma** **In Private Contexts**

- The standard explication of the **security vs. privacy dilemma** does not adequately account for the peculiarities of private sphere phenomena such as **employer-employee relations** and has to be adjusted accordingly.

Security vs. Privacy: **Public Sphere**

- **Traditional interpretation:**
 - Subordination
 - Citizens subject to public authority, control & sanction
- **Rights-based view:**
 - Privacy as a "negative right"
 - Public invasions permissible if justified: legitimate/proportionate
- **Privacy:**
 - Based on human/constitutional/fundamental rights
 - More comprehensive right than mere data protection
- **Security:**
 - Equally legitimate claim of citizens vis-à-vis state
 - Security even in favour of privacy rights
(e.g. public protectionary measures in e-government applications)
- **Dilemma: More security = lower level of privacy?**

Security vs. Privacy: **Private Sphere**

- **Peculiarities of employment relation:**
 - Consensual agreement and co-ordination of individuals
 - Entry and exit on voluntary basis (as opposed to citizenship)
- **Traditional liberal interpretation:**
 - Subordination of worker under authority & control of employer
 - Cf. German labour law: employer's right of "direction"
- **Modern interpretation:**
 - Preservation of employee's rights during contract
 - Case to case balance between conflicting rights: tensions & ignorance of respective rights
- **Dilemma: Employer's security vs. employee's privacy rights?**

Private Contexts: **Individuals & Their Interests**

Employer's

- **Freedom to conduct a business (art. 16)**
- **Right to property (art. 17) ...**
[cf. EU Charter of Fundamental Rights]
- **Monitor employee activity & breaks**
- **Assess performance / output**
- **Control attitude / behaviour / health**
- **Control work flow**
- **Prevent unlawful activities, industrial espionage & inappropriate conduct**
- **Acquire knowledge base for entrepreneurial decisions...**

Employee's

- **Human dignity (art. 1)**
- **Right to respect for private life & protection of personal data (art. 7 & 8)**
- **Integrity of person (art. 3)**
- **Freedom of expression, assembly & association (art. 11, 12)**
- **Non-discrimination (art. 21)**
- **Fair & just working conditions (art. 31) ...**
- **Restricted personal file access etc.**
- **Consent to communication control...**
- **Committee & trade union membership**
- **Healthy work environment ...**

Workplace Privacy Protection: **Overview**

1. Security vs. privacy dilemma in private contexts
 - 2. Intra-corporate law enforcement and compliance**
 3. New quality of privacy invasions through office surveillance systems
 4. Complex and "pointillist" legal landscape
 5. Employee data protection agenda
 6. CR as a worldwide approach to privacy protection
- 

2nd Thesis: Problems of Intra-Corporate Law Enforcement

- **Intra-corporate law enforcement and compliance** are distinct from and in some respects **more difficult to achieve** than extra-corporate, public abidance by the law (e.g. traffic surveillance through CCTV):
lack of enforcement powers; only "soft" incentives & sanctions
- This **applies to both** security and privacy concerns:
lack of intra-corporate "judicial review of rights" etc.
- Proposed solutions have to be in line with **other intra-corporate compliance schemes** (cf. implementation of accounting standards & **anti-bribery, anti-fraud, anti-discrimination schemes** etc.)

Workplace Privacy Protection: **Overview**

1. Security vs. privacy dilemma in private contexts
 2. Intra-corporate law enforcement and compliance
 - 3. New quality of privacy invasions through office surveillance systems**
 4. Complex and "pointillist" legal landscape
 5. Employee data protection agenda
 6. CR as a worldwide approach to privacy protection
- 

3rd Thesis: **New Quality of Privacy Invasions**

- The **potential for privacy invasions** of a new generation of activity-centric office surveillance systems **transgresses** both a **quantitative and a qualitative threshold**.
- The **development** of such systems is **industry-driven** and irrespective of concerns for privacy and data protection management.

'Activity-Centric' Office Surveillance Systems: Workflow & Productivity Monitoring

Microsoft proposes (US Patent Application 20070300174, Dec 27, 2007, Claim 1, p. 1):

"An **activity monitoring system** that facilitates managing and optimizing **user activity automatically** to improve overall user **productivity** and **efficiency** comprising:

- a monitoring component that can monitor user activity conducted **on one or more computing devices** [desktop, handheld, laptop, pocket PC, PDA, phone ...]
- an activity management component which can **process** and **evaluate user activity data** to **assess user performance** on their respective activities and the current **allocation of system and human resources**. (...)
- Rather than monitoring only one document in isolation (...) the subject systems and methods monitor and manage the activity in its entirety."

➔ 'activity-centric' as opposed to application-/device-/document-centric
➔ purpose = workflow management; security interests???

Combining Sensor & Communication Technologies: **A Private "Panopticum"?**

The proposed activity monitoring system includes:

- **Real time** monitoring of user activity,
- **data storage**,
- **automatic** analysis & decision making,
- a physiological **sensor detection component** measuring ("at least one of") **heart rate, galvanic skin response, brain signals [?], respiration rate, body temperature, movement, facial expressions, blood pressure (...)**

= a new quality of personal & bodily invasiveness

New Surveillance Options: Old & New Concerns

COMPONENT	CONCERNS	PRIVACY PRINCIPLES [cf. Directive 1995/46/EC]
Communication (eavesdropping)	Covert (?) data collection Consent?	Transparency, purpose-binding, data security, ...
Physiological sensors	Free informed consent? Sensitive data	Legitimacy, purpose-binding, transparency, personal/bodily integrity
Data storage ("historical information")	Retention period? Deletion? Access?	Legitimacy, access/data security, minimization,...
Data aggregation & analysis ("system can infer user intent ... [&] identify lower performers")	Linking of (sensitive) data Access? Control?	Legitimacy, purpose-binding, transparency, proportionality, minimization, ...
Automated decision-making ("triggering help request")	Linking of (sensitive) data Access? Control? [Cf. art. 15 Directive 95/46/EC!]	Legitimacy, purpose-binding, transparency, proportionality, ...

Workplace Privacy Protection: **Overview**

1. Security vs. privacy dilemma in private contexts
2. Intra-corporate law enforcement and compliance
3. New quality of privacy invasions through office surveillance systems
- 4. Complex and "pointillist" legal landscape**
5. Employee data protection agenda
6. CR as a worldwide approach to privacy protection

4th Thesis: **Complex & "Pointillist" Legal Landscape**

- The legal landscape of **privacy rights**, **data protection regulation** and **jurisprudence** with respect to the workplace is **fairly complex** and **detailed** in some **substantial** (e.g. eavesdropping, video surveillance) and **geographical** areas (EU vs. US & rest of world) and shows great blanks and **lacunas** in other areas.
- This **lack of legal clarity** favours **ignorance** of the respective legal framework by both employers and employees (cf. clarity as a **principle of justice**; non-compliance due to **complexity**?)

Workplace Privacy Protection: **Overview**

1. Security vs. privacy dilemma in private contexts
2. Intra-corporate law enforcement and compliance
3. New quality of privacy invasions through office surveillance systems
4. Complex and "pointillist" legal landscape
- 5. Employee data protection agenda**
6. CR as a worldwide approach to privacy protection

5th Thesis: Employee Data Protection Agenda

- Legislation is required to decide on **criteria for workplace surveillance** such as the permitted **degree of intrusiveness** of novel techniques.
- Current debates (e.g. on an “**Employee Data Protection Act**” in Germany) focus on the **standard repertoire of criteria** such as purpose-binding, transparency and voluntariness, restrictions to the collection, storage, combination and disclosure of data gathered.
- **Clarification** is needed as to where the **bottom-line** is [health data?].
- **Data protection management schemes** have to become an **integral** and **legally required part** of the implementation of office surveillance systems (monitoring of **product and processes/checks**).

Workplace Privacy Protection: **Overview**

1. Security vs. privacy dilemma in private contexts
2. Intra-corporate law enforcement and compliance
3. New quality of privacy invasions through office surveillance systems
4. Complex and "pointillist" legal landscape
5. Employee data protection agenda
- 6. CR as a worldwide approach to privacy protection**

6th Thesis: **Corporate responsibility ...**

- Data protection and privacy legislation are substantiations of **general legal and ethical principles** (human rights, justice).
- Intra-corporate **employer-employee relations** have so far been **neglected in** theory and practice of **corporate responsibility**.
- **Privacy rights impact tests** should thus become part of **corporate self-regulation** and be included in **compliance schemes** and **certification processes**
(e.g.: privacy seals for products; ISO 26000 on social responsibility).

... as a worldwide approach to privacy protection

- Whereas legislation is primarily of national origin, **technology** and growing **awareness for corporate responsibility** are – at least in the paradigm case of multinational corporations – **worldwide phenomena**.
- **Global business ethical principles** and **corporate cultures** may and should **bridge the divide** between national legislations.



Thank you for your attention. - Questions?

Europäische Akademie

zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen

Bad Neuenahr-Ahrweiler GmbH

Katja Stoppenbrink, LL.M., M.A.

Wilhelmstr. 56

53474 Bad Neuenahr-Ahrweiler

Germany

Tel. +49 (0) 2641 973-323

Fax +49 (0) 2641 973-320

katja.stoppenbrink@ea-aw.de

www.ea-aw.de

