Workplace surveillance: examining current instruments, limitations and legal background issues

Vigilância no local de trabalho: examinando os actuais instrumentos, limitações, problemas e enquadramento jurídico

Ulrike Hugl
School of Management, University of Innsbruck, Austria; ulrike.hugl@uibk.ac.at

ABSTRACT

Working life is increasingly characterized by strong tendencies towards control and surveillance of employees. To control and monitor employees, employers may use diverse surveillance instruments into consideration: examples may be time-tracking and access control systems, e-supported systems like chip cards, RFID (radio-frequency identification) chips, human implants, various biometric systems, computer surveillance, network monitoring software, GPS tracking, telecommunication, visual and Internet monitoring, as well as surveillance of detective agencies. Reasons for employers to monitor employees’ behavior are manifold: from an avoidance of malicious insider threats, the prevention of image damage, increased productivity, and through to reduced costs. This work starts with a fictive story of an employee, followed by a short presentation of surrounding viewpoints of organizational control and surveillance. The main part of the paper focuses on an analysis of currently used monitoring instruments and the Austrian legal framework of employee surveillance and related privacy issues.

Keywords: Surveillance, control, monitoring instruments, employee privacy, legal framework (Austria).

1. Preface

Peter works for a very innovative medium-sized Austrian software development company with enormous increase in turnover in its market segment. His work as regional sales manager involves work in the field (service and customers’ acquisition) and other places of work like the corporate head office in Tyrol and diverse branch offices. To enter the head office, every employee has to use a contract-free RFID-based key tag which simultaneously monitors his specific working time. In his office, Peter tries to get manifold jobs done: phone calls, e-mails, researches on the Internet, meetings with colleagues, preparation of a sales presentation regarding a new product development for a meeting with a key customer. During his work he listens to some music videos on youtube.com. Although the company’s guidelines prohibit to make private phone calls and to write e-mails etc., from time to time Peter contacts some family members and friends. In his opinion, the related security guidelines have been announced to deter employees from doing ‘really malicious acts’ and not such ‘harmless acting’. Furthermore, he is convinced that his company does not monitor his computer, Internet and phone activities. During the afternoon, he also calls his best friend Toni by using his fixed phone; chance brought it about that he is working for a competing company since a few months. During the afternoon, Peter also sends an e-mail to his bank asking for an increased credit line as well as a specific change of his credit card conditions. At 5 PM, Peter finishes his work in the head office, does some screenshots of some product development versions, serves the screenshots and the finished sales presentation on his USB flash drive and leaves the building. On the following day, Brain has to drive with his company car to Zurich for a meeting with an important customer. At his return trip he makes a stop at Bregenz and giving him an USB flash drive. - All attempts to explain fail and Peter gets his termination with immediate effect. Furthermore, he is threatened with legal steps against him. About two weeks after his termination Brain gets an invoice of an investigation agency – he is required to bear the full costs for the company’s surveillance activities.

2. Surveillance: reasons and surrounding issues

The story outlined above is fictive. Nevertheless, it shows a tendency in modern business, namely increased surveillance activities of quite a few companies. During the last years, mainly the Internet is largely responsible for an increase in employee surveillance (Ball, 2010). Nevertheless, workplace surveillance is nothing new since the early era of industrialization, but nowadays especially technological opportunities have increased and facilitate all related

the house making pictures etc. For the moment, Peter does not mean any harm... At the end of the month, Peter has to find out 17 hours undercharged on his time sheet respectively his pay slip. Upon request, his colleague in the personal management department informs him that the undercharged hours are seen as compensation for private activities during his working time. In addition, the company has docked off about 100 Euros for the private drive to his best friend on the way back from his meeting in Zurich. Furthermore, Peter gets a disciplinary warning letter because of his security guidelines’ disregard. A few days after the next surprise: Peter has to keep an appointment with the firm’s executive board as he is confronted with the allegation of corporate espionage, especially regarding the disclosure of crucial recent product developments to a person from a competing company. The members of the executive board make clear that they know from his financial problems as well as from all private activities during his working hours. In addition, they deliver documents like his detailed e-mail and phone call lists, visited Internet-sites, as well as a picture showing him with Toni in Bregenz and giving him an USB flash drive. - All attempts to explain fail and Peter gets his termination with immediate effect. Furthermore, he is threatened with legal steps against him. About two weeks after his termination Brain gets an invoice of an investigation agency – he is required to bear the full costs for the company’s surveillance activities.
activities. Further reasons for this trend are manifold, for example (1) malicious insiders and scandals of companies and its announcement in well known media (Hugl, 2010a) as well as (2) the prevention of related image damage, (3) the defense of corporate espionage, (4) the discovery of specific causes for dismissal on grounds of conduct, (5) a general intended protection of corporate assets, (6) the detection of illegal software and missing data, (7) the increase of productivity, (8) the detection of reasons for a disciplinary warning letter or a termination, and finally (9) significantly reduced costs and increased availability of surveillance technologies. A further observable tendency concerns an increased public awareness of privacy violations. For several years, (9) the data protection regulation and (8) the awareness of employees' surveillance was increased. (technological) pervasion of the overall working environment, employees successfully generate so-called ‘data shadows’. Or as the German Federal Commissioner for Data Protection and Freedom of Information states: “In recent years, a close meshed ‘net of surveillance’ in business life has been built up. […] In addition, more and more availability of data involves and increases the risk of data abuse and claim for revised activities in the field of (also legal-based) employees' data protection” (Schaar, 2008, p. 398).

Increased surveillance activities – for example the implementation of the European Data Retention Directive (concerning data generated or processed in connection with the provision of publicly available electronic communications services or networks) (EU, 15 March 2006) and related resistance of citizens, broadly communicated claims of politicians for increased activities in the field of video control (CCTV), as well as discussions and resistance against Google Street View (see e.g. Albert, May 1, 2012, Grill & Schaal, 2012). In 2008, Lidl (a German discounter) systematically searched of employees' car trunks, employees' financial and family situation, kind and background of tattoos, screening of online social networks (Hugl, 2011), movement profiles of employees inside the company's buildings based on access control systems (e.g. biometric systems like hand geometry, iris or retina scans, electronic fingerprinting, alcohol and drug testing), in some countries also human implants (e.g. Mexico, USA) are in use (for further examples of employee surveillance see Hugl, 2010b). Based on an increased resistance, (technological) pervasion of the overall working environment, employees successfully generate so-called ‘data shadows’.

3. Panopticism and surveillance instruments

Manifold studies have investigated the writings of Michel Foucault and his metaphors of surveillance and control and panopticism (mainly referring to a disciplinary state examining direct surveillance) across society. The master metaphor of Panopticism refers to Jeremy Bentham, an English author, philosopher and social and legal reformer who developed a design for a prison building, the so-called panopticon. Bentham’s ideas was universal transparency to “[…] keep the prisoners on their best behavior” (Moore, 2011, p. 697). In a panopticon, a prisoner never knows whether or not he/she is under surveillance and therefore tends to modify his/her behavior as if the monitoring is constant. A permanent feeling of potential monitoring generates in turn leads to a higher level of disciplining and behavior compliant – individuals completely are assured that they are being monitored and probably punished. This compliance to rules can also be called moral code of good behaviour – hence, surveillance as a strategic power “[…] is used to control and discipline” and also benefits (intended or unintended) social inclusion (Lipartito, March 2010, p. 6). However, the panopticon does not exclusively refer to an architectonic concept, to a greater degree it also covers all organizational concepts, technologies and instruments focusing on comprehensive and efficient surveillance activities or enabling surveillance. In this regard, the panopticon seems to be a metaphor for the power of surveillance.

Foucault (1977) argues that “[…] that panopticism implies omnipotence over the mind” (Briviot & Gendron, 2011, p. 138). In such a sense, surveillance activities may give “[…] power of mind over mind” (Foucault, 1977, p. 206). Moreover, some scholars focus on hierarchical issues – for example, Townley (1994) observes that “[p]anopticism operates through hierarchical observation […]” (p. 139) – or on issues of disciplinary power of employees (Covaleski, Dirsmith, Heian, & Samuel, 1996) and individuals as manageable, measurable and transformable objects based on such disciplinary power (Briviot & Gendron, 2011, p. 138, referring to Covaleski et al. 1998). The concept of panopticism is still a dominant
metaphor, but Foucault “[...] failed to notice that late 20th-century technological and infrastructural developments were qualitatively different from the earlier examples he studied” (Graham & Wood, 2003, p. 230). Therefore, Poster (1990) argues that new technological developments force a re-evaluation of Foucault’s concept, because “[...] today’s circuits of communication and the databases they generate constitute a Superpanopticon, a system of surveillance without walls, windows, towers or guards. The quantitative advances in the technologies of surveillance result in a qualitative change in the microphysics of Power” (p. 93). Hence, the main differences between analogue and digital surveillance are quantitative. Quantitative advances, digital data storage devices can store enormous data volumes and much faster than in times of analogue systems. But the main point seems to be the question: What can be done with the information gathered and stored? Digital surveillance increases the opportunities of interconnection of different surveillance systems and instruments, also in combination with so-called algorithmic surveillance based on automated processes (set of automatically done instructions based on specific software) (see e.g. Graham & Wood, 2003). Technology development seems to be a door opener enabling new forms of analyses.

Workplace monitoring as a powerful tool for employers to ensure that individuals are performing their work has been in use since the early days of industrialization. In the game of surveillance, critical scholars may argue that, in most cases, new technological opportunities may provide crucial forms of (Neo-)Taylorism, “measuring keystrokes and delivering anti-theft tactics” (Miller, 2010, p. 11). Surveillance may constitute a “whip in a new digital Taylorism” (Schmitz 2005, p. 728) or “surveillance transcends traditional Taylorism” (Lyon, 1994, p. 126). From a sociological point of view, the labor process is competing for “who determines the nature and form of work” and becoming a “frontier of control” (Sewell, 1998, p. 399).

3.1. Techniques of attendance and time monitoring

The most common form of employee surveillance is the monitoring of employees’ working time. In comparison to previously mainly used simple attendance recorders, the latest systems are computer-operated and provide much more functions than mechanical ones: among a time monitoring of working times and breaks, they also include features in terms of user administration and evaluation as well as interfaces for pay stub. Furthermore, some systems also provide entry control opportunities. Whereas conventional physical systems via a time clock keep the potential of surveillance within limits, electronic entry control systems (via in/out-surveillance software) generate much more data. The main objective of attendance control systems is to allow authorized employees entrance to for example rooms, departments and buildings in a secured way. Modern attendance control systems work with the rules who-when-where-to, determining who is allowed to entrance what area at a specific moment in time. In comparison to conventional offline systems with low complexity of installation, online systems match the key codes with a central data base and generate protocols of all relevant activities.

So-called smart card, chip cards or integrated circuit cards can be seen as a further development of magnetic cards and require specific card-reader units. Advantages of (process) chip cards are its storage facility and encryption opportunity of stored data (of importance regarding potential manipulation). The German Federal Office for Information Security (BSI) states: “In general, an organisation can choose between the technologies of contact cards and contactless cards. Contact cards – as their name already implies – need to be inserted in a card reader device whereas contactless cards need to be bypassed in a specified distance to a card reader device respectively an electronic terminal” (BSI, 2010, p. 13). An RFID chip normally contains a micro processor, is memory-equipped and an antenna allows contactless data transfer. At present, RFID chips are available in manifold types, for example with different frequency ranges, power supply, size or form, and (physical) range (Finkenzeller, 2008, p. 11-24). Most common are RFID-chips in the size of credit cards, key tags, clocks or bracelets – least common as human (chip) implants (Hugl, 2008). Typically, with the exception of human implants, “[...] attendance monitoring is not invasive and is to be expected by employees” (Ciocchetti, 2011, p. 306).

In comparison to the above presented systems, biometric techniques do not require a key medium (e.g. a bracelet, a keychain etc.) which has to be carried along: based on an employee’s individual bodily characteristics, the human itself is the key medium. Biometrics – bios (live) and metron (measure), also called the ‘science of measurement of human beings’ – and related techniques still have disadvantages: relatively high costs, low acceptance rate of employees and error-proneness (error-acceptance and error-rejection). Biometrics may be use in combination with an electronic employee ID card (attendance and identification card), in this case data can be stored either in a reference data base or (for a later data transfer) directly on the card (BSI, 2010, p. 16).

What are the major problems of diverse attendance and time monitoring systems? First, in comparison to online systems, offline systems are typically exclusively limited to physical access control. Subsequent analyses, for example to generate movement profiles, would involve major effort, for example regarding the readout of all readers and the consolidation of all relevant data. Second, contact-based biometric access systems do have limits if groups enter a specific area: in such a case, only one person would have to use the key medium, others not. Hence, both access information as well as the movement profile of only one person, the person using the key medium, is correctly performed; the problem for the employer lies in the fact that stored data do not allow an evaluation if data are correct or not. RFID systems with a larger operating range (several meters), via an automatically read-out when a person passes the reader solve this problem. Third, electronic-based access control systems (except biometric systems) do not have a direct identification – in fact, the key medium verifies identification for a specific area, but not the person her/himself: therefore, unauthorized passing on or fraudulent falsification of the key medium may pose a threat to the organization. For years, also secured chip cards or RFID chips can be copied or faked without considerable expenditure (Langheinrich, 2007, p. 256). Fourth, biometric systems cover at least the same surveillance potential than all other electronic-supported access control systems. Nevertheless, a human itself is key medium for verification and (despite already mentioned limitations of groups) therefore the reliability and increased force of data expression as well as person-based relevant data (movement profiles etc.) makes the difference.

3.2. Local and central computer surveillance

Computer work has the highest penetration in the employees’ working life. A German study of the Federal Association for Information Technology, Telecommunications and New Media (BITKOM, 2010) highlights that in 2009 52% of all Austrian and German employees at least use once a week their computers at work (44% in 2003). Four main forms of local computer surveillance can be differentiated: 1) hardware keylogger (or system monitor or keystroke logger) as a software device (USB keylogger or keystroke imprints an employee types on a his/her computer’s keyboard (no software necessary; data analyses via master password or de-installation), 2) cookies as local stored small text files with
specific information about visited websites, browser cache (also local stored information for a reduced loading time of already visited pages) and browser history (see in your browser e.g. progress or chronic), 3) remote control software to control other computers or their users at a distance (e.g. applications for use within an Intranet as a private network), and 4) computer monitoring software as low-cost and common used so-called spyware - partially as all-in-one solutions with extensive monitoring functions and qualitative enhancement of protocol data with the help of graphical analyses - and of course with very high invasion of employees' privacy (e.g. Spector Pro 2012, MemorySpy including social networking dangers etc., lambdabrother, Orwell Monitoring 2012, Spytech Spy Agent/Spy Suite/Realtime-Spy, Winston Monitoring 3.8 etc.).

Local computer surveillance builds a very easy form of surveillance, also possible without specific soft- and hardware: operating systems, browsers and all day used programs comply with basic surveillance requirements. Specific activities are stored in protocols and local hard disks and can be used for surveillance purposes. On a more upper level, specific surveillance software with a different range of functions and intensity can be employed to monitor diverse computer activities. Further possibilities of local computer surveillance are for example remote access software or specific surveillance hardware.

Central or server-based computer surveillance opportunities involve 1) gateways (router, firewall, or proxy server), 2) network surveillance software, and 3) groupware software (e.g. Microsoft Exchange, AhrePoint Workspace, OpenXchange, with shared day planners, task lists, e-mails, documents etc.). As a main difference to the techniques of local computer surveillance the installation is central: diverse workplace computers built a local network (LAN) which is connected via a central gateway with the Internet. At the gateway (hub) all sent and received data packages are monitored (protocols), for example e-mails, FTP, Instant Messaging (audio/phone and chat), web requests, etc. In addition, the installations make it possible to determine what software is being used (in an unattended computer environment). The main reason for its usage at the workplace may be manifold: as (further) attendance or access control, to ensure safety, surveillance of technical operations, employee's control and supervision etc. Surveillance software re-active and pro-active surveillance opportunities can be installed (e.g. security software of websense.com including Web 2.0 and Facebook security etc.).

3.3. Monitoring of telecommunication and social media

Telecommunication surveillance comprises monitoring of fixed phones and mobile phones. Modern fixed phone systems are quasi computer systems and involve several functions like the differentiation of private and work calls, data storage of incoming and outgoing calls, the length of calls, listening and recording functions. Much more surveillance opportunities exist for smart phones and enable comprehensive monitoring of employees' activities (e.g. software like Mobile Spy 4.1 or FlexiSPY). - Another aspect of surveillance related to online social network sites (OSNs) and other social media with respect to a potentially reputational risk stemming from employees' negative comments on the Web. In Germany, Facebook (80% with an active account) and Youtube (37%) are dominating users' online presence (PwC, 2012). Therefore, especially larger companies formulate specific policies or rules for employees' behavior on such sites and also establish control mechanisms to ensure that staff acts in the organization’s interest. Nevertheless, such regulations are always a balancing act between employer interests and employees’ privacy.

3.4. Mobile and video surveillance

This form of surveillance efforts works with 1) GSM (Global System for Mobile Communications) location respectively (radio) cell triangulation for mobile phones, 2) GPS surveillance, 3) digital tachographs, and 4) fleet management systems (e.g. with specific software like easyfleet; 3) and 4) are mainly used in the logistics sector). In general, these techniques cover all kinds of position and movement data focusing on activities outside the organization (e.g. sales representatives, service employees, professional drivers). Typically, employees with tasks outside the company are also equipped with a laptop or similar devices – this allows the same surveillance opportunities than for office computers. Software-based opportunities of these surveillance technologies are very similar to previously presented techniques.

By now, from the viewpoint of each citizen, video surveillance seems to be one of the most common (visible or hidden) surveillance techniques inside and outside of companies. According to Müller (2008), reasons for its usage at the workplace may be manifold: as (further) attendance or access control, to ensure safety, surveillance of technical operations, employee's control and supervision etc. Surveillance opportunities can be available in different kinds, sizes (very large to pin-sized), picture qualities, with various recording features and based on diverse technologies (digital or analog). Furthermore, in this field, software-based and intelligent image and face recognition opportunities are on the way.

3.5. Detective agencies and architectural issues

In the introduction we already mentioned occurrences regarding employees' surveillance of detective agencies built a further form of monitoring. An online research of such agencies in German speaking countries shows that most of them are also working in the field of surveillance for employers, both in the employee's private as well as the company-related environment. The main reasons may be a control of potential misconduct, to produce evidence as preliminaries for potential disciplinary warning letters or terminations, and in some cases also used for intimidation.

Based on Bentham's panopticon, architecture can also be used for control and surveillance. For example glass walls and open space offices (for an efficient control by supervisors). The windowed offices allow surveillance of every facial expression or movement. In the worst case, a moment of thought may be interpreted as idleness, a discussion with colleagues as a conflict situation - employees are working in the knowledge of continuously being controlled and probably adapt their behaviors (compatible or incompatible with the organization’s interest).

4. Legal background in Austria

In general, an employer has the right to control his employees, nevertheless, an employer has to ensure duty of care to choose exclusively select the most gentle surveillance instruments (principle of proportionality). Furthermore, the statutory rules of the Austrian data protection act (DSG, 2000) have to be mandatory observed. Further issues to consider are the intensity of control as well as the weighing of interests (protection-related interests of an employee). As the kind and scope (intensity) of surveillance activities may occur in very different ways, the legal meaning and legitimacy has to be evaluated on a case-by-case basis.

Austrian employers are legally bound to ensure records of employees' working time. Legitimacy is based on the question of the intensity and opportunities of analysis of a used system: purely checks on attendance (recording of entry and exit) are not subject to approval; a system's possibility to generate further analyses like movement profiles would affect or violate the employees' human dignity and requires an agreement between the works committee and the management or an approval of all employees (e.g. recordings of restroom breaks are in no case allowed). Biometric time attendance systems
are also subject to approval (Austrian Supreme Court (OGH, Dec. 20, 2006)).

Employees’ computer surveillance has to be reviewed depending on the applied techniques: in any case, key logging and the generation of screenshots is legally not allowed (even if on visible installations and informed about it). In the case of merely statistical data collection an installation of computer surveillance software may be legal – anyhow, an agreement between the works committee and the management is needed. As routers, firewalls and proxy servers are necessary to maintain the basic requirements and functionality of an organization’s computerized information system, a deactivation is not necessary. Hence, from a legal point of view, it has to be evaluated if an Internet usage for employees’ private purposes is allowed or not; if it is forbidden no problem regarding a review of protocol data occurs. If a private Internet usage is explicitly allowed or not forbidden and only abstract data (and not personal data) are generated (e.g. access statistics), data protection issues are not concerned; in the case of an individual-oriented data storage of web accesses and e-mails an authorization requirement and mandatory agreement between the works committee and the management is needed. The just mentioned regulations apply (in a very similar way) also for e-mails: in any case allowed and not subject to approval is a collection of anonymized usage statistics, the block and filtering of specific e-mail addresses, as well as spot checks and audit in a case of reasonable suspicion.

The range and surveillance intensity of fixed phone systems is determining the legal-oriented appraisal. Modern systems with installed listening and recording functions are not allowed. In the case of a systematically allocation and control of called phone numbers corresponding with specific extension numbers an agreement between the works committee and the management is needed. In any case illegal would be eavesdropping and listening of employees’ phone calls without foreknowledge of those affected - in addition, body checks or the installation of a video camera in rest rooms (e.g. threat to the human dignity, data of employment issues are not concerned; in the case of an individual-oriented data storage of web accesses and e-mails an authorization requirement and mandatory agreement between the works committee and the management is needed. The just mentioned regulations apply (in a very similar way) also for e-mails: in any case allowed and not subject to approval is a collection of anonymized usage statistics, the block and filtering of specific e-mail addresses, as well as spot checks and audit in a case of reasonable suspicion.

A legal evaluation of a gathering of position and movement data on the one hand has to consider a weighing of interests, on the other hand it has to be considered if the intended surveillance objective also can be reached with other and more gently tools (principle of proportionality). This means that in most cases a collection of movement data is not permitted. In any cases of GPS surveillance software in use (e.g. in the logistics sector), such systems require worker participation or a special agreement.

Since 2010, based on an amendment of the Austrian data protection act, before an installation of a video camera a notification at the so-called Data Processing Register (Austrian Data Protection Commission) is needed; in the case of digital data storage of audio and picture recording a prior vetting of the Austrian Protection Commission is needed. Exceptions are only analog systems or systems with only live-monitoring. For sensitive sectors like banking houses, jewelers or petrol stations and others, the data protection act considers a so-called standard application (§19 DSG 2000) with simplified regulations for equal data applications. A surveillance of objects (e.g. machines, cashier’s offices) at the working place is allowed. Based on the Austrian Labour Constitution Act (ArbVG, 1974, §69a) and the Austrian Labour Constitution Act (2009) and the Austrian Supreme Court (§§96 and 96a ArbVG). A last critical point refers to a missing exclusion of evidence (improperly obtained): a spy out of corporate secrets, a violation regarding the telecommunication secret and an infiltration of computer networks are judicially relevant, but not a usage of stolen data. Hence, illegal gained or collected means of evidence are adjudged (for example to stake reasons for a termination) and illegal behavior (regarding the submission of means of evidence) is approved by a court.

5. Conclusion

Nowadays, a company has manifold opportunities to control and monitor its employees. Based on an increased technical development, it is difficult to predict further opportunities and their implications on employees’ behavior, satisfaction as well as on employees’ privacy and human dignity. An example in the future could be the usage of human implants for security reasons (crossing the mainly still existing frontier of the human body) or tendencies towards patent pending regarding invasive (biometric) privacy issues or cross of the mainly still existing frontier of the human body) or tendencies towards patent pending regarding invasive (biometric) privacy issues or dependencies on implications on employees’ behavior most notably in times of economic crisis. – Surveillance technologies are on the way, the question seems to be: what kind of future should we want?