

SURVEILLANCE IN MODERN ORGANIZATIONS1

Topic: Security, Cybersecurity

Paper Title: Surveillance in modern organizations

Word Count: 2165

Pages: 11

Referencing: Harvard

Education Level Masters

Surveillance in modern organizations

[Name of Student]

[Name of Institution]

[Course]

SURVEILLANCE IN MODERN ORGANIZATIONS2

Introduction

In several works (Gilliom, 2010; Lyon, 2007), the concept of surveillance is limited to the collection of various information (data, images, sounds). According to Lyon (2007) surveillance is the acquisition, temporary, permanent or variable duration, information. This information can be visual, auditory, or other; it is often the product of our senses or technologies designed to support, but the meaning-monitoring link is not conclusive. Many forms of information do not match the human sense (for example, the structure of the DNA of an individual). In short, the meaning of surveillance relationship is primarily cultural and scientific (Gilliom, 2010). The information collected may relate to a particular individual, a type of person, a place previously unidentified persons were detected on computerized traces of various transactions on the Internet and in the physical world (traces consumption, for example) (Garfinkel, 2011). All this information can be stored separately or pooled to detect patterns or extrapolate missing elements from what is known using a toolbox of sociological theories, psychological, demographic and economic.

In this paper surveillance and different ways of surveillance operated in modern organizations is discussed

Purpose of Surveillance in Organizations

Almost all monitoring activities, whether aided or not a technology has the ability to gather information on a host of different objects (Gilliom, 2010). According to Allmer

SURVEILLANCE IN MODERN ORGANIZATIONS³

(2012) Surveillance is an outside goal at the mere collection of information, which can be summarized by the intervention or obtaining a benefit outside pure knowledge. The question of the purpose of monitoring activity is unfortunately less simple than it seems. Often the explicit goal is the expression of an ideal that is never realized practice (Matteralt, 2010).

Electronic Surveillance in organizations

Several authors (Allmer, 2012; Harris, 2011; Matteralt, 2010) have provided definitions of surveillance technology and management models proposed to debate. Matteralt (2010) defines information surveillance as the process that involves the observation and analysis of scientific, technological and economic impacts present and future environment, to identify threats and opportunities for development focusing interest in the present and highlighting its highly valuable strategic guidance and prevention of potential conflicts of predictive nature of the organization. According to Hier & Greenberg (2009) the technological monitoring is the process of collection, analysis, validation and dissemination of strategic value information which is responsible for the identification of the problem to be analysed. Prescott & Gibbons (2003) propose the adoption of a geocentric view of the practices of competitive intelligence.

It is difficult to find the right balance between the respect due to the employee's private life in the workplace and the need to control the use of the tools that the employer makes available to him (Laidler, 2008). In order to respect this balance that the law and the jurisprudence formulate a set of rules and procedures enabling the employer to exercise what is called cyber surveillance of the employees (Ball, 2005). This surveillance may be carried out either on the computer stations of certain employees or may constitute a veritable internal monitoring device applicable to all. The possibility for an employer to access his employee's

SURVEILLANCE IN MODERN ORGANIZATIONS⁴

computer to control its use has evolved considerably in a few years, allowing an increased control by the employer of computers used in a professional setting.

In principle, access to the Internet at work must be used for the performance of professional tasks and not be used for personal purposes by the employee. If, in practice, the use of the computer tool for private purposes is generally tolerated as long as it is not abusive, the employer may nevertheless put in place a computer charter within the company in order to regulate this practice. In all cases, the employer has an extended right of access to the computer equipment used in the workplace. Its powers are often misunderstood by employees (D'Urso, 2006). The employer can control the employee's Internet connections even in his absence, since these are presumed to be of a professional nature. The employer can also consult the list of favourites (Norris & Armstrong, 2009).

The employer may access the files on his employee's computer hard disk, except where the employee has identified these documents as personal. But he considers that the appointment of a hard disk "Personal data" does not prevent the employer from accessing it nevertheless. The employer can access emails from the employee under certain conditions. If these e-mails are not identified as personal, the employer may consult them.

Many employees have free access to the telephone as part of their work. This freedom can sometimes lead to abuse when the employee uses the telephone line of his company to make long calls unrelated to the performance of his work. The jurisprudence has thus established certain rules regarding the telephone monitoring of employees (D'Urso, 2006).

Many companies also make mobile phones available to their employees for the purpose of their professional activity. Law considers that the employer may consult the SMS received on

SURVEILLANCE IN MODERN ORGANIZATIONS5

these telephones even in the absence of the person concerned, since these messages are presumed to have a professional nature. However, messages received on these phones cannot be consulted by the employer once a "personal" mention is identified in the subject of the SMS (Ball, 2005).

Documents in the workplace of an employee are presumed to be of a professional nature. In principle, the employer can therefore consult them freely. In this capacity, it may in particular access documents in the cabinets or drawers of the employee's office. On the other hand, the case law considers that such consultation is restricted when the employee has identified the documents as personal. In this case, the employer can only access it in the presence of the employee, or after having asked the judge to appoint a bailiff to do so. In the same sense, when an employee receives letters at his place of work, the contents of these letters are protected by the secret of correspondence if their personal character is specified.

The employer can use different means of control to supervise its employees. In principle, this practice is permitted provided that the means employed do not have a disproportionate character with regard to the freedoms of employees. Before setting up these processes, the company must at least inform its employees and the works council. The latter must in particular be consulted on the arrangements for implementing the proposed scheme (D'Urso, 2006).

The most frequently used means of control in practice are the electronic badges allowing to check the schedules of entry and exit of the employee in the company and to control its activity and Video surveillance devices, the implementation of which is conditional upon compliance with certain conditions.

The employer cannot set up a spinning mill against an employee. This process infringes his privacy. It is therefore a mode of unlawful proof that will not be retained by the courts in the

event of a dispute. This rule is valid both when the employer uses a private detective and when he or she (or one of his subordinates) exercises the spinning suit (D'Urso, 2006).

The case of video surveillance of employees employed at home (maternal assistant, cleaning lady, nurse etc.) is a bit special. Although he is at home, the particular employer who wishes to film his employee is subject to the rules of labor law. This implies informing the employees concerned about the installation of the cameras and their purpose. In addition, employees must not be filmed permanently.

How Surveillance affect work performance

At a time when all our tools of work are becoming digital, measurement, control and surveillance continue to extend their grip on productive relationships and beyond, on all our human relationships. All tools now seem to be used to count, to calculate the productivity of each. Productivity is now under the control of machines and the feedback loop they produce (i.e. information that machines are returning that serves as an indicator to reinforce measured behavior) is increasingly looking for maximize.

Take DeskTime for example, a software that monitors employees' on-screen activity, depending on which applications they are launching and actively using. For each software and for each employee, the manager who uses DeskTime must determine if the software in question is a productive, non-productive or neutral application (Coker, 2011). For example, this means monitoring a graphic designer's work time by looking at his time spent on Photoshop, to qualify its use of the internet as neutral, or to listen to music as unproductive. Under its apparent neutrality, is it a reflection of a reality other than that of the preconceived ideas of the manager? Does the work of a graphic designer need to be measured only by the time spent on Photoshop?

SURVEILLANCE IN MODERN ORGANIZATIONS7

Measuring the productivity of everyone raises a fundamental question: what is efficiency? Do our management and management systems have a good definition?

According to Newsome et al (2013), most manufacturers and supermarkets chains make the mistake of skimping on labour costs, whether by low wages or by under-investment in training. Low-paid, poorly trained jobs often cost companies a great deal in terms of performance. One of the reasons is that the workforce management software used to manage employees. Indeed, they encode all workers as a cost rather than as a resource. Optimisation therefore leads large companies to have employees to manage the goods, but little to answer customers' questions. If the workers are better trained, better paid, if they know better the tastes and the demands of the customers then they sell more.

A vast majority of studies(Coker, 2011; Salamon& Robinson, 2008; Gagné&Deci, 2005) show that surveillance has a negative impact on productivity. In most companies, employers keep a watchful eye on the activity of their employees to prevent them from doing "something wrong". Continuous or random checks, everywhere something or someone is watching what the employees are doing. Most managers are trained above all to control the others and 30% to 50% of their time is devoted to this monitoring activity. But if this control is supposed to prevent employees from doing "something wrong", do not they prevent them from doing "something good?"

If they are not supervised, workers use their methods of work which are always more efficient than the prescribed methods. Performance increased not so much because the workers were hidden from their supervisors, but because they were able to share ideas and practice them without remonstrance (Salamon& Robinson, 2008). At a time when surveillance through digital

SURVEILLANCE IN MODERN ORGANIZATIONS8

tools is becoming ubiquitous, the risk is that surveillance is discouraging and in the end, much less productive than its defenders hope.

When employees find out that they are being watched, employees thought that, for their boss, the quantity of work is more important than quality (Mayer& Gavin, 2005). Employees under supervision often perceive their work conditions as more stressful and are more subject to boredom, anxiety, depression, fatigue and anger than others. Monitoring reduces performance and feeling personal control.

We have seen the harms of supervision and management by coercion; how rules, rituals, processes, and surveillance have become our new forms of authority. Yet the challenge remains the same: finding more relevant indicators to better measure productive relations without always being aware of the impact that these new forms of surveillance will have on productive relations. To change indicators, the challenge is often to multiply them. As digital tools become more and more intimate, new metrics interfere with productive relationships.

Conclusion

As a matter of principle, the implementation of an IT monitoring system for employees requires the employer to comply with several prior consultation and information obligations. In the event of non-compliance with any of these requirements, the supervisory device cannot be opposed to employees and the resulting evidence is unlawful. Nevertheless, the case-law has been able to qualify these prior disclosure obligations in the light of the purpose of setting up the supervisory arrangements.

Thus, the device used may have as its object the overall supervision of the activity of the employees without, however, permitting the identification of the perpetrator of a particular act.

SURVEILLANCE IN MODERN ORGANIZATIONS⁹

For example, the device may allow the listing of the websites visited by all employees without being able to carry out identification by item. In addition, the employer must always declare the telephone monitoring software (PBX) or the Internet (devices for individual monitoring of connection times or sites consulted). Video surveillance recordings are also always considered to be personal data within the meaning of the law. It is only allowed if the aim of the system is precisely the supervision that the provision of information to employees is necessary.

However, it has also been noticed that employees consider surveillance and monitoring as lack of trust from employer's side which, instead of improving, decrease the quality of their performance. Hence, it seems a better option for employers that instead of continuous surveillance, try to create a relationship with employees which is based on trust. This will help to enhance the quality of performance as well as productivity of the employees.

References

- Allmer, Thomas, 2012. *Towards a Critical Theory of Surveillance in Informational Capitalism*.
Frankfurt Main: Peter Lang
- Ball, K., 2005. Organization, surveillance and the body: Towards a politics of
resistance. *Organization*, 12(1), pp.89-108.
- Coker, B.L., 2011. Freedom to surf: the positive effects of workplace Internet leisure
browsing. *New Technology, Work and Employment*, 26(3), pp.238-247.
- D'Urso, S.C., 2006. Who's watching us at work? Toward a structural-perceptual model of
electronic monitoring and surveillance in organizations. *Communication Theory*, 16(3),
pp.281-303.
- Gagné, M. and Deci, E.L., 2005. Self-determination theory and work motivation. *Journal of
Organizational behavior*, 26(4), pp.331-362.
- Garfinkel, Simson, 2011. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly
& Associates, Inc.
- Gilliom, John, 2010. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*.
University Of Chicago Press
- Harris, Shane, 2011. *The Watchers: The Rise of America's Surveillance State*. London, UK:
Penguin Books Ltd.
- Hier, Sean, P. and Greenberg, Joshua, 2009. *Surveillance: Power, Problems, and Politics*.
Vancouver, CA: UBC Press
- Laidler, Keith, 2008. *Surveillance Unlimited: How We've Become the Most Watched People on
Earth*. Cambridge, AU: Icon Books Ltd
- Lyon, David, 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press
- Matteralt, Armand, 2010. *The Globalization of Surveillance*. Cambridge, UK: Polity Press
- Mayer, R.C. and Gavin, M.B., 2005. Trust in management and performance: Who minds the
shop while the employees watch the boss? *Academy of management journal*, 48(5),
pp.874-888.
- Newsome, K., Thompson, P. and Commander, J., 2013. 'You monitor performance at every

hour': labour and the management of performance in the supermarket supply chain. *New Technology, Work and Employment*, 28(1), pp.1-15.

Norris, C. and Armstrong, G., 2009. *The Maximum Surveillance Society: The Rise of CCTV*.
Oxford, Berg Publishers

Prescott, J. E. and Gibbons, P. T., 2003. *Global Perspectives on Competitive Intelligence*.
Society for Competitive Intelligence Professionals, SCIP.

Salamon, S.D. and Robinson, S.L., 2008. Trust that binds: the impact of collective felt trust on
organizational performance. *Journal of Applied Psychology*, 93(3), p.593.