Dear clients and business friends,

In its recently published decision (BGE 139 II 7) the Federal Supreme Court for the first time took a stance on the question of whether surveillance of employees by means of so-called spyware is permitted.

The Federal Supreme court views the use of spyware that surreptitiously monitors the (online) activities of employees is clearly inadmissible as well as disproportionate, thereby confirming the prevailing doctrine. At the same time, it prohibited the use, as evidence before the court, of illegally obtained information (in the case in question, as justification for a dismissal). However, the ban on the so-called behavioural surveillance of employees does not apply without limits. In each individual case, the interests of the employer are to be weighed against the interests of the employee.

This issue of Legal News seeks to convey – from an employer’s perspective – the most important principles, the specific preconditions as well as the limitations of electronic surveillance at the workplace.

Daniel Bachmann
Attorney-at-law, Partner, Legal Services
daniel.bachmann@ch.ey.com

1. Introduction
In today's age of technology, there are many ways for employers to monitor their employees by electronic means. The reasons for such surveillance can be both manifold and justified. First and foremost, an employer must take care to ensure the economic viability and efficiency of his operations. In addition he must take an interest in exposing possible breaches by his employees. Finally, an employer is required to comply with those contractual and statutory obligations incumbent upon him in order to prevent damages claims or reputational damage caused by employees. Relevant in this regard is in particular the liability of the employer for his employees as auxiliaries or in his capacity as a principal, as well as product liability. The need for comprehensive surveillance over operations and personnel stands inherently juxtaposed to the interests of employees to have a pleasant work environment and sufficient privacy.

2. Principles
Pursuant to Art. 328 CO, employers are subject to a duty of care. In accordance therewith, employers must respect and safeguard the personal rights of employees. Depending on their design, however, electronic surveillance measures intervene to a significant extent in the personal sphere of employees. Particularly invasive and thus banned by law are measures, the sole purpose of which is to monitor employees' behaviour (see Art. 26 [1] of Ordinance 3 to the Employment Act, ArGV3). The targeted and permanent monitoring of employees at the workplace is thus deemed to be a prohibited act of behavioural surveillance. Electronic surveillance is only permitted to the extent it is necessary for other reasons (e.g. security, organization, or controlling production) as well as proportionate (see Art. 26 [2] ArGV3). Distinguishing between admissible and inadmissible surveillance can be difficult in individual cases. How the necessary weighing of interests might look in practice is elucidated on the basis of the three most common surveillance methods.

3. Video surveillance
Constant video surveillance is likely to severely affect the psychological well-being, mental health and performance of employees. In light of the severity of such action, video recordings are, as a rule, not properly suited for monitoring employees. In the interest of performance and quality control, it is possible, by way of an exception, to engage in surveillance for a limited period of time for training purposes. Primarily, however, only such monitoring is permissible as necessary for security reasons and thus must be targeted, not towards employees, but rather third parties, machines or certain production processes. Conceivable are thus video cameras placed in outside areas near access ways or parking lots, near dangerous machinery or equipment, at bank counters as well as in storage areas housing valuable items. The
employee must, however, have the option of withdrawing from the camera’s field of vision. As a rule, this requires that the employee is aware of the surveillance in question. Secret surveillance is only allowed in exceptionally rare cases, such as, e.g. in seldom used strong rooms or cashiers’ offices.

4. Telephone surveillance

Monitoring telephone traffic can take place by means of either analysing recorded telephone conversations or connection data and numbers dialled for such conversations. The latter is, as a rule, permitted, provided the employee is given prior notice as to the type and manner of both the monitoring and the uses to which it will be put (e.g. within rules of use). The recording and use of what is said is in the course of conversations, constitutes a severe act of intrusion into an employee's privacy. Recording is already subject to special statutory sanction, as long as not all persons participating in the discussion have given their consent (see Art. 179bis StGB). The use of recorded conversations is, moreover, only permitted, provided it is necessary for the purpose of monitoring the quality of services (namely in the case of call centres or hotlines), or for training or evidentiary purposes (i.e. in the case of telephone transactions such as orders, trading mandates and reservations).

5. Monitoring of internet use and email

For technical reasons any use of the internet and email inevitably leaves behind traces. Its analysis can, depending on the scope, constitute severe intrusion against the personal rights of employees. Prohibited by the highest court in the land is the permanent and individually targeted collection of personal information by means of spyware (see BGE 139II 7, as well as the comments contained in the foreword), which is comparable to constant video or telephone surveillance. Permitted on the other hand, is the general, anonymous collection of user information, provided employees have been informed with regard thereto. In addition, the monitoring of work-related correspondence must, in principle, be allowed for the purpose of performance and quality control. Decisive in this context is whether internet and email can also be used privately in a given place of work, or whether doing so has been banned by corresponding notices. In the case of a general ban, it is generally allowed that random, individualized spot checks be carried out (including) of private use. Otherwise, such checks may only be done in cases where a specific suspicion exists (e.g. in cases of reasonable suspicion of contract breach or criminal conduct). Reading the contents of private emails is clearly prohibited.

6. Conclusion

On the basis of the relevant applicable statutory protective provisions and the practice of the courts, employees are only allowed to monitor employees with cameras or listening devices in exceptional cases. Electronic surveillance of the (private) use of internet, email or telephone is only permitted to a limited extent. Moreover, prior to having recourse to electronic surveillance, all organizational options must first be exhausted. In any event, it is recommended that rules be enacted concerning the use of computerized methods, as well as to inform employees and obtain their cooperation. What is more, in order to do justice to the requirement of proportionality, all reasonable technical preventative measures should first be taken as a precaution. This would include, e.g. blocking certain phone numbers and internet websites, as well as including specific dialling codes to be used for private telephone calls, separating personal and business email, constantly updating security software, as well as rendering surveillance data anonymous. Failure to comply with the principles and recommendations set out above, can either result in claims for damages and satisfaction from affected employees, and/or criminal repercussions against the employer (see Art. 179quater StGB “breach of secrecy or privacy through the use of a recording device”, as well as Art. 179novissima StGB “obtaining personal data without authorisation”). As shown in the decision of the Federal Supreme Court cited above, unauthorised surveillance can also result in the inadmissibility of evidence in court proceedings.

Ernst & Young

Assurance | Tax | Legal | Transactions | Advisory

About the global Ernst & Young organization

The global Ernst & Young organization is a leader in assurance, tax, transaction and advisory services. It makes a difference by helping its people, its clients and its wider communities achieve their potential. Worldwide, 167,000 people are united by shared values and an unwavering commitment to quality.

The global Ernst & Young organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity’s acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

In Switzerland and Liechtenstein, Ernst & Young Ltd is a leading audit and advisory firm with some 2,100 people at 11 locations. The firm also provides tax, legal, transaction and accounting services. In this publication, “Ernst & Young” and “we” refer to the Ernst & Young Ltd, the Swiss member firm of Ernst & Young Global Limited.

For more information, please visit www.ey.com/ch

Imprint

Legal News
Electronic publication in German, French and English.

Designed and produced by Ernst & Young Ltd
Marketing and External Communications
P.O. Box 8022 Zurich

Subscriptions / address changes
www.ey.com/ch/newsletter

www.ey.com/ch/legal
© 2013 Ernst & Young AG
All Rights Reserved.

The Legal News provides an overview of new legal developments. The content does not represent any legal advice.