



Electronic Monitoring System Implementation Strategies

Companies now have access to a wide range of tools to monitor employee performance and streamline operations. While these tools have proven to significantly improve operations, they occasionally face resistance by employees.

GPS fleet tracking technology is one such tool that has the potential to cause an adverse reaction by some employees if not implemented properly. The primary concern voiced by some employees is the feeling that “big brother” will be watching their every move. This broad statement is typically based on a lack of knowledge of the technology and how it will be used by management.

We decided to research how such tools were implemented by best-in-class companies. We wanted to get a sense of which elements were included in their internal policies to minimize a negative reaction by employees.

In 2002, the U.S. General Accounting Office conducted a study of employee monitoring practices by 14 Fortune 1000 companies in the U.S. While this study was oriented toward computer usage monitoring, the results also apply to GPS vehicle tracking technology.

We found that the most important first step in implementation was creating a **policy** regarding the use of the electronic monitoring system.

Many of the items below were included in the policies of the surveyed companies:

- They provided a notice to all employees notifying them of the company’s electronic monitoring practices.
- They provided a general description of how the electronic monitoring system worked and what data is collected.
- The policies always affirmed the company’s right to review employee use of company assets.
- The policies state that employees have no expectation of privacy while utilizing company assets.
- They described the appropriate use of company assets.
- They described detailed penalties for misuse of company assets.
- They describe the goals & objectives for implementation of the system.

- They included restrictions on the disclosure of personal data to others outside of the company without the employee's consent.
- They explained that data should be collected and used lawfully and fairly.
- They explained that data is collected for the activities of all employees in a similar capacity to avoid the perception of discrimination.
- They described who has access to the data and what safeguards are in place to ensure that non-authorized people cannot access the data.
- They described the frequency of the data review or whether data will only be reviewed as part of an internal investigation.
- They described which managers can access the data to complete internal investigations.

Table 1: Key Elements of an Electronic Monitoring Policy

| Policy element | Type of statement |
|---|--|
| Monitoring use of proprietary assets | Statements that company assets are provided as tools for the business and all activities related to the use of these assets are to subject to monitoring, auditing, or review. |
| Establishing no expectation of privacy | Statements about the extent or limitations of privacy protections for employees while utilizing company assets. |
| Improper employee use | Statements that some uses of company assets are inappropriate including specific notices banning specific activities (e.g., use of assets for personal benefit, travelling with non-insured passengers, excessive speeding, idling, etc.). |
| Allowable employee uses | Statements explaining proper or acceptable uses of the company assets, including whether or not personal use is permitted. |
| Disciplinary action | Statements that there are penalties and disciplinary actions for violations of the company usage policy. |
| Employee acknowledgement of policy | A statement requiring that employees demonstrate they understand the company policy and acknowledge their responsibility to adhere to the policy. |

Other practices by some of the surveyed companies:

- Some created employee groups to participate in the formulation and review of the monitoring policies.
- Some gave employees access to any information collected on their electronic transmissions.

- Some precluded the employers' review of employee electronic transmissions except when they had a reasonable independent indication of inappropriate use.
- Some gave employees the right to dispute and delete inaccurate data.

Our research gave us interesting insight into the proper implementation of a GPS fleet tracking system. The first and most important step taken by these companies was to create a policy regarding the usage of electronic employee monitoring systems. They then included items within the policy based on their desired levels of transparency, accountability and data security. Each organization is unique, so they included or excluded the necessary items based on their judgment of the proper fit within their companies. Finally, they ensured that the policy was properly communicated to all impacted employees.

Sources:

U.S. General Accounting Office; "EMPLOYEE PRIVACY Computer-Use Monitoring Practices and Policies of Selected Companies"; 2002; <http://www.gao.gov/new.items/d02717.pdf>

International Labour Office Geneva; "Protection of Workers' Personal Data"; 1997; <http://www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf>

ACLU; "Privacy in America: Electronic Monitoring"; 12/31/2007; <http://www.aclu.org/technology-and-liberty/privacy-america-electronic-monitoring>