

2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY

Executive Summary

From e-mail monitoring and Website blocking to phone tapping and GPS tracking, employers increasingly combine technology with policy to manage productivity and minimize litigation, security, and other risks. To motivate compliance with rules and policies, more than one fourth of employers have fired workers for misusing e-mail and nearly one third have fired employees for misusing the Internet, according to **the 2007 Electronic Monitoring & Surveillance Survey from American Management Association (AMA) and The ePolicy Institute.**

Firing Employees for E-Mail and Internet Misuse:

The 28% of employers who have fired workers for e-mail misuse the following reasons: violation of any company policy (64%); inappropriate or offensive language (62%); excessive personal use (26%); breach of confidentiality rules (22%); other (12%).

The 30% of bosses who have fired workers for Internet misuse cite the following reasons: viewing, downloading, or uploading inappropriate/offensive content (84%); violation of any company policy (48%); excessive personal use (34%); other (9%).

Monitoring Internet, Blogs and Social Networking Sites:

Employers are primarily concerned about inappropriate Web surfing, with 66% monitoring Internet connections. Fully 65% of companies use software to block connections to inappropriate Websites—a 27% increase since 2001 when AMA/ePolicy Institute first surveyed electronic monitoring and surveillance policies and procedures.

Employers who block access to the Web are concerned about employees visiting adult sites with sexual, romantic, or pornographic content (96%); game sites (61%); social networking sites (50%); entertainment sites (40%); shopping/auction sites (27%); and sports sites (21%). In addition, companies use URL blocks to stop employees from visiting external blogs (18%).

Computer monitoring takes many forms, with 45% of employers tracking content, keystrokes, and time spent at the keyboard. Another 43% store and review computer files. In addition, 12% monitor the blogosphere to see what is being written about the company, and another 10% monitor social networking sites.

Monitoring Employee E-Mail:

Of the 43% of companies that monitor e-mail, 96% track external (incoming and outgoing messages), while only 58% monitor internal messages that are sent among employees. The failure to monitor internal e-mail is a potentially costly oversight, as employees tend to play

it fast and loose with internal e-mail, transmitting jokes, gossip, disparaging remarks, pornography, and other content that triggers workplace lawsuits.

When it comes to monitoring methods, 73% of organizations use technology tools to automatically monitor e-mail, and 40% of employers assign an individual to manually read and review e-mail. Employees assigned to read and review employee e-mail are employed by the following departments: IT (73%), HR (34%), legal (18%), compliance (17%), outside third-party (4%), other (17%).

How Employers Notify Users About Monitoring:

While only two states, Delaware and Connecticut, require employers to notify employees of monitoring, the majority are in fact alerting employees when they are being watched. Fully 83% inform workers that the company is monitoring content, keystrokes and time spent at the keyboard; another 84% let employees know the company reviews computer files; and an additional 71% of employer's alert employees to e-mail monitoring.

Unfortunately, the methods employers use to alert employees to e-mail and Internet monitoring are not necessarily the most effective: 70% of organizations in 2007 relied on an employee handbook to inform users about computer monitoring; 40% relied on e-mail notices; 35% used written notices; and 32% relied on intranet postings. Only 27% of employers addressed monitoring policies and practices as part of formal, on-site employee training—the recommended way to maximize compliance.

You cannot expect an uninformed workforce to comply with policy. And you cannot trust employees on their own to access the company intranet system or retrieve a copy of the employee handbook in order to educate themselves about monitoring or other electronic rules and policies. Best practices call for formal employee training, which grants employees the opportunity to ask questions and gain a thorough understanding of electronic rules, policies, and procedures.

Reasons for Monitoring Computer Activity:

Concern over litigation and the role electronic evidence plays in lawsuits and regulatory investigations has spurred more employers to monitor online activity. Data security and employee productivity concerns also motivate employers to monitor Web and e-mail use and content. Workers' e-mail and other electronically stored information create written business records that are the electronic equivalent of DNA evidence. As a result, 24% of employers have had e-mail subpoenaed by courts and regulators and another 15% have battled workplace lawsuits triggered by employee e-mail, according to 2006 AMA/ ePolicy research. To help control the risk of litigation, security breaches and other electronic disasters, employers are taking advantage of monitoring and blocking technology to battle people problems—including the accidental and intentional misuse of computer systems and other electronic resources.

Telephone Taping and Voice Mail Monitoring:

Concerned about inappropriate telephone use, 6% of employers have fired employees for misuse or private use of office phones. Fully 45% monitor time spent and numbers called, up from 9% in 2001. Another 16% record phone conversations, versus 9% six years ago. An additional 9% monitor employees' voicemail messages. Most employers notify employees of phone (84%) and voicemail (73%) monitoring.

Video Surveillance:

Almost half (48%) of the companies surveyed use video monitoring to counter theft, violence and sabotage, versus 33% in 2001. Only 7% use video surveillance to track employees' on-the-job performance, a slight increase over the 4% reported in 2001. Most employers notify employees of anti-theft video surveillance (78%) and performance-related video monitoring (89%).

Global Satellite Positioning and Emerging Surveillance Technology:

Employers have been slow to adopt emerging monitoring/surveillance technologies to help track employee productivity and movement. Employers who use Assisted Global Positioning or Global Positioning Systems satellite technology are in the minority, with only 8% using GPS to track company vehicles; 3% using GPS to monitor cell phones; and less than 1% using GPS to monitor employee ID/Smartcards.

The majority (52%) of companies employ Smartcard technology to control physical security and access to buildings and data centers. Trailing far behind is the use of technology that enables fingerprint scans (2%), facial recognition (0.4%) and iris scans (0.4%).

Findings

INTERNET, E-MAIL, BLOG & SOCIAL NETWORKING SITE MONITORING AND URL BLOCKING

Q. Computer Use: Does your organization monitor time spent, matter/content, or keystrokes entered?

All employees	28%
Selected job categories	17%
Not practiced	55%

Q. If monitoring of time spent, matter/content, or keystrokes is practiced, how would you categorize the monitoring?

Ongoing	32%
Routine	28%
Occasional	27%
Specified	13%

Q. Are employees informed of the organization's policy of monitoring time spent, matter/content, or keystrokes?

Yes	83%
No	17%

Q. Computer Surveillance: Does your organization store and review employees' computer files?

All employees	25%
Selected job categories	18%
Not practiced	57%

Q. If monitoring of files is practiced, how would you categorize the monitoring?

Ongoing	17%
Routine	29%
Occasional	33%
Specified	21%

Q. Are employees informed of the organization's policy of monitoring computer activity?

Yes	84%
No	6%
Don't know	10%

Q. If yes, how are employees informed about monitoring?(Check all that apply.)

On-site training	27%
Intranet postings	32%
E-mail notices	40%
Written notices	35%
Employee handbook	70%
Other	11%

Q. E-Mail: Does the organization monitor and review employees' e-mail messages?

All employees	26%
Selected job categories	17%
Not practiced	57%

Q. What type of e-mail does the organization monitor? (Check all that apply.)

External e-mail (incoming and outgoing)	96%
Internal e-mail (sent among employees)	58%

Q. If e-mail monitoring is practiced, how is it accomplished?

Use of technology tools (software, hardware, outside managed service)	73%
Individuals read/review	40%

***Q. If individuals review/read e-mail, in what department are the reviewers employed?
(Check all that apply.)***

IT	73%
HR	34%
Legal	18%
Compliance	17%
Outside Third-Party	4%
Other	17%

Q. Are employees informed of the organization's policy of monitoring e-mail?

Yes	71%
No	11%
Don't Know	18%

Q. Internet Usage: Does your organization monitor and review Website connections?

All employees	52%
Selected job categories	14%
Not practiced	34%

Q. If monitoring of Websites is practiced, how would you categorize the monitoring?

Ongoing	39%
Routine	24%
Occasional	23%
Specified	14%

***Q. Does your organization use blocking software to prevent Internet connections to
unauthorized/inappropriate Websites?***

Yes	65%
No	26%
Don't Know	9%

***Q. When it comes to blocking Web access, what type of sites is your company most
concerned about? (Check all that apply.)***

“Adult” sites with sexual, romantic, pornographic content 96%

Game sites	61%
Social Networking Sites	50%
Entertainment sites	40%
Shopping/Auction sites	27%
Sports sites	21%
Other	23%

Q. Does your organization regularly monitor the blogosphere to see what is being written about it?

Yes	12%
No	50%
Don't know	38%

Q. Does your organization use technology to block access to external blogs?

Yes	18%
No	56%
Don't Know	26%

Q. Does your organization regularly monitor social networking site (MySpace, Facebook, etc.) to see what is being said or posted about it?

Yes	10%
No	55%
Don't Know	35%

TELEPHONE, VOICE MONITORING AND TAPING

Q. Telephone Use: Does your organization monitor time spent and numbers called?

All employees	25%
Selected job categories	20%
Not practiced	55%

Q. If monitoring of time spent and numbers called is practiced, how would you categorize the monitoring?

Ongoing	27%
Routine	32%
Occasional	25%
Specified	16%

Q. Are employees informed of the organization's policy of monitoring telephone use: time spent and numbers called?

Yes	84%
-----	-----

No 16%

Q. Telephone Use: Does your organization record employees' phone conversations?

All employees 2%
Selected job categories 14%
Not practiced 84%

Q. If phone conversations are recorded, how would you categorize the monitoring?

Ongoing 29%
Routine 33%
Occasional 13%
Specified 25%

Q. Are employees informed of the organization's policy of recording telephone conversations?

Yes 82%
No 18%

Q. Does the organization record and review employees' voice mail messages?

All employees 4%
Selected job categories 6%
Not practiced 90%

Q. If voice mail is recorded and reviewed, how would you categorize the monitoring?

Ongoing 15%
Routine 23%
Occasional 39%
Specified 23%

Q. Are employees informed of the organization's policy of recording and reviewing voice mail?

Yes 73%
No 27%

VIDEO SURVEILLANCE

Q. Does your organization use video surveillance to counter theft, violence or sabotage?

All employees 25%
Selected job categories 22%

Not practiced	53%
---------------	-----

Q. If video surveillance is used as a deterrent to counter theft, violence or sabotage, how would you categorize the monitoring?

Ongoing	47%
Routine	29%
Occasional	10%
Specified	14%

Q. Are employees informed of the organization's video surveillance practices to counter theft, violence or sabotage?

Yes	78%
No	22%

Q. Does your organization use video surveillance to monitor employee performance?

All employees	0%
Selected job categories	7%
Not practiced	93%

Q. If video surveillance is used to monitor employee performance, how would you categorize the monitoring?

Ongoing	22%
Routine	28%
Occasional	39%
Specified	11%

Q. Are employees informed of the organization's practice of monitoring performance with video?

Yes	89%
No	11%

POLICY COMPLIANCE AND DISCIPLINE

Q. Has your organization ever fired an employee for e-mail misuse?

Yes	28%
No	38%
Don't know	34%

Q. If yes, what did the violation involve? (Check all that apply.)

Violation of any company policy	64%
---------------------------------	-----

Inappropriate/offensive language/content	62%
Excessive personal use of the company system	26%
Breach of confidentiality	22%
Other	12%

Q. Has your organization ever fired an employee for Internet misuse?

Yes	30%
No	37%
Don't know	33%

Q. If so, what did the violation involve? (Check all that apply.)

Viewing/downloading/uploading inappropriate/offensive content	84%
Violation of any company Policy (Internet, ethics, etc.)	48%
Excessive personal use of the company system	38%
Other	8%

Q. Has your organization ever fired an employee for misuse or private use of the office telephone?

Yes	6%
No	48%
Don't know	46%

Q. Has your organization ever disciplined an employee for misuse or private use of the office telephone? If so, what form did that discipline take? (Check all that apply.)

Formal reprimand or warning	59%
Informal reprimand or warning	29%

Q. Has your organization ever fired an employee for content posted on the employee's home-based personal blog?

Yes	0.4%
No	57%
Don't Know	42.6%

Q. Has your organization ever fired an employee for posting business-related content or videos on a social networking site (YouTube, FaceTime, etc.)?

Yes	0.7%
-----	------

No	57.3%
Don't Know	42%

SATELLITE TECHNOLOGY

Q. Does your organization use Assisted Global Positioning or Global Positioning Systems satellite technology to monitor/track any of the following? (Check all that apply.)

Company vehicles	8%
Company cell phones	3%
Employee ID/Smartcard	0.7%
NA	89%

Q. Does your organization use any of the following technology to control physical security access to your buildings or data centers? (Check all that apply.)

Smartcard technology	52%
Fingerprint scan	2%
Facial recognition	0.4%
Iris scan	0.4%
NA	45%

DEMOGRAPHIC QUESTIONS

Number of survey respondents 304

Number of employees per company

100 or fewer	27%
101–500	27%
501–1000	12%
1001–2500	12%
2501–5000	10%
More than 5000	12%

Industry That Best Describes Your Organization

Business/Professional Services	21%
Financial Services	7%
General Services	2%
Manufacturing	19%
Public Administration	12%
Wholesale/Retail	4%
Other	35%

The **2007 Electronic Monitoring & Surveillance Survey** is co-sponsored by American Management Association (www.amanet.org) and The ePolicy Institute (www.epolicyinstitute.com). A total of 304 companies participated: 27% represent

companies employing 100 or fewer workers, 101–500 employees (27%), 501–1,000 (12%), 1,001–2,500 (12%), 2,501–5,000 (10%) and 5,001 or more (12%).

The **2007 Electronic Monitoring & Surveillance Survey** questionnaire was designed by American Management Association and The ePolicy Institute's Nancy Flynn, author of *The ePolicy Handbook*, 2nd Edition (AMACOM 2008), *Blog Rules* (AMACOM 2006), *Instant Messaging Rules* (AMACOM 2004), and *E-Mail Rules* (AMACOM 2003). Comparative numbers drawn from **2001 Electronic Policies & Practices Survey** from American Management Association, The ePolicy Institute and *US News & World Report*.

--- End ---