2001 AMA, US News, ePolicy Institute Survey

Electronic Policies and Practices
Summary of Key Findings

Who's Watching and Listening?

The American Management Association's (AMA's) 2001 survey on electronic monitoring and surveillance found that more than three-quarters of major U.S. firms record and review employee communications and activities on the job, including phone calls, e-mail, internet connections, and computer files. The figure has doubled since 1997, when AMA inaugurated its annual survey. Almost all of the increased activity since 1997 has involved storage and review of computer files and e-mail messages, and monitoring internet connections.

In April 2001, AMA went back to its 1,627 survey respondents with a follow-up questionnaire to gain further insights into organizational policies and practices in this area. We received 435 completed returns to comprise the sample for this report. The follow-up sample has a somewhat larger representation of smaller and mid-sized firms than the original sample, but closely matches the original in terms of business categories represented. The section headed ***About This Survey*** at the end of this summary gives more detail in this regard.

This table lists the forms of electronic monitoring and surveillance featured in the original AMA questionnaire and the responses from both the original 2001 sample of 1,627 and the follow-up sample of 435. Note that we combine responses to create a category of ***active monitoring*** and a more inclusive category for ***all forms*** of electronic monitoring and surveillance:

	Original Sample (1,627)	Follow-up Sample (435)
Recording & review of telephone conversations	**11.9%**	**8.5%**
Storage & review of voice mail messages	**7.8%**	**7.6%**
Storage & review of computer files	**36.1%**	**36.3%**
Storage & review of e-mail messages	**46.5%**	**46.9%**
Monitoring Internet connections	**62.8%**	**61.6%**
Video recording of employee job performance	**15.2%**	**11.7%**
Total, active monitoring of communications & performance:	**77.7%**	**73.6%**
Telephone use (time spent, numbers called)	**43.3%**	**41.6%**
Computer use (time logged on, keystroke counts, etc.)	**18.9%**	**20.5%**
Video surveillance for security purposes	**37.7%**	**33.3%**
Total, all forms of electronic monitoring and/or surveillance:	**82.2%**	**77.7%**

Why Monitor Employees?

The AMA follow-up questionnaire listed five rationales for electronic monitoring and surveillance, and asked respondents to rate them in importance on a seven-point scale. Legal liability and security concerns were the most highly rated reasons, performance review the lowest rated. Among those reporting that their firm has been involved in some legal action concerning employee use of e-mail and the internet (see ***Legal Issues*** on p. 5 below), the importance ratings soar where legal liability and especially legal compliance are concerned, while there is little difference in the ratings for the other listed rationales.

	Whole Sample			Report Legal Action			No Legal Action		
Rationale	Avg Importance Rating	Pct Rating High (7 or 6)	Pct Rating Low (2 or 1)	Avg Importance Rating	Pct Rating High (7 or 6)	Pct Rating Low (2 or 1)	Avg Importance Rating	Pct Rating High (7 or 6)	Pct Rating Low (2 or 1)
Legal Liability	**5.89**	**68.3%**	**4.8%**	**6.30**	**81.8%**	**1.5%**	**5.82**	**65.9%**	**5.4%**
Security Concerns	**5.65**	**60.0%**	**3.9%**	**5.56**	**60.6%**	**7.6%**	**5.67**	**59.9%**	**3.3%**
Productivity Measurement	**5.06**	**45.5%**	**8.7%**	**5.08**	**42.4%**	**46.1%**	**5.06**	**46.1%**	**8.7%**
Legal Compliance	**5.04**	**50.1%**	**15.4%**	**5.48**	**60.6%**	**12.1%**	**4.96**	**48.2%**	**16.0%**
Performance Review	**3.70**	**45.3%**	**30.6%**	**3.89**	**25.8%**	**27.3%**	**3.66**	**17.1%**	**31.2%**

Policy Notification

With or without formal written policies, companies do make their legal right to monitor e-mail and internet connections known to their employees:

Employee Notification of Company's Legal Right to Monitor E-Mail & INet	Whole Sample	Active Monitoring		Any Legal Action	
		Yes	No	Yes	No
Yes	**83.7%**	**90.9%**	**63.5%**	**89.4%**	**82.7%**
No, but plan to	**4.1%**	**3.1%**	**7.0%**	**3.0%**	**4.3%**
No, not at all	**10.3%**	**4.7%**	**26.1%**	**7.6%**	**10.8%**

There is a strong correlation between active monitoring practices and formal, written policies covering e-mail, internet, and/or software use. Eighty-one percent of companies with written policies actively monitor employee communications, compared with less than half (49%) of those lacking written policies. Put another way 95% of companies that actively monitor employees have written policies, compared with 75% of those that do no monitoring. Another correlative is legal action; companies that report legal action involving e-mail or internet communications are more likely more likely to have written policies and active monitoring.

Written Policy	Whole Sample	Active Monitoring		Any Legal Action	
		Yes	No	Yes	No
For e-mail use	**81.4%**	**86.9%**	**66.1%**	**89.4%**	**79.9%**
For internet use	**77.2%**	**83.1%**	**60.9%**	**81.8%**	**76.4%**
For software use	**62.3%**	**67.5%**	**47.8%**	**72.7%**	**60.4%**

An important element of e-mail policy has to do with retention and deletion of messages; "due diligence" demands good record keeping, and e-mail may be subject to legal subpoena (see below). Only one-third of companies have set such a policy, although they are far more likely to have done so if they have been subject to legal action involving electronic communications:

E-Mail Retention/Deletion Policy	Whole Sample	Active Monitoring		Any Legal Action	
		Yes	No	Yes	No
Current	**35.4%**	**41.6%**	**18.3%**	**51.5%**	**32.5%**
Planned	**12.2%**	**11.9%**	**13.0%**	**10.6%**	**12.5%**
None	**49.9%**	**44.7%**	**64.3%**	**34.8%**	**52.6%**

Although the correlation exists, there is no **necessary** connection between written policies and monitoring practices. Companies may have written policies outlining the proper use of various forms of communications technologies without actively monitoring that use. Conversely, companies may store and review e-mail messages and record or restrict internet connections without having a formal policy on the books. Also, having no **written** policy does not necessary mean having no policy at all – although policies **should** be written to assure consistency and avoid confusion.

Where written policies do exist companies are far more likely to offer training programs to employees, but such training is still relatively rare:

E-Policy Training Programs	Whole Sample	Any Written Policies		Active Monitoring	
		Yes	No	Yes	No
Current	**23.9%**	**26.4%**	**2.2%**	**27.8%**	**13.0%**
Planned	**10.3%**	**9.5%**	**17.8%**	**10.3%**	**10.4%**
None	**64.1%**	**63.8%**	**66.7%**	**60.6%**	**73.9%**

Companies that have experienced legal actions relating to e-policies are more thorough in informing employees about their policies **in writing**, either on paper or electronically, and also practice multiple ways of spreading such information.

How Employees are informed	Whole Sample	Active Monitoring		Any Legal Action	
		Yes	No	Yes	No
Written notification via memo	**68.4%**	**68.6%**	**53.9%**	**66.7%**	**64.5%**
Broadcast notification via e-mail/intranet	**48.3%**	**51.6%**	**39.1%**	**66.7%**	**45.0%**
Policy postings in office facilities	**29.2%**	**31.6%**	**22.6%**	**36.4%**	**27.9%**
Policy postings on organizational intranet	**25.3%**	**28.8%**	**15.7%**	**40.9%**	**22.5%**
Oral notification by supervisors	**40.7%**	**43.4%**	**33.0%**	**37.9%**	**41.2%**

Employees Acknowledge Notification:	Whole Sample	Active Monitoring		Any Legal Action	
		Yes	No	Yes	No
In writing, with signatures	**50.6%**	**56.9%**	**33.0%**	**43.9%**	**51.8%**
In other ways than signed	**5.1%**	**5.6%**	**3.5%**	**6.1%**	**4.9%**

How New Hires are Informed	Whole Sample	Active Monitoring		Any Legal Action	
		Yes	No	Yes	No
Special written notice	**22.3%**	**23.8%**	**18.3%**	**33.3%**	**20.3%**
Included in e-policy manuals	**52.6%**	**58.1%**	**37.4%**	**59.1%**	**51.5%**
Part of orientation program	**55.6%**	**58.4%**	**47.8%**	**62.1%**	**54.5%**

Personal Use of Office E-mail and Internet Connections

While four out of ten surveyed companies allow employees full and unrestricted use of office e-mail, only one in ten allow the same unrestricted access to the internet. As will be seen, companies are far more concerned with keeping explicit sexual content off their employees' screens than with any other content or matter. Justified or not, anxieties about charges of a hostile workplace environment in a sexual harassment lawsuit are guiding corporate policy in this area, and those anxieties are focused more on the worldwide web than on e-mail communications. Also, technology allows blocking connections to certain websites but not to specific e-mail addresses.

Personal Use of Office E-Mail	Whole Sample	Written E-Mail Policy Yes	Written E-Mail Policy No	Active Monitoring Yes	Active Monitoring No
Full and unrestricted personal use	**39.3%**	**35.3%**	**56.8%**	**35.9%**	**52.2%**
Full use with prior management approval	**21.1%**	**23.4%**	**11.1%**	**25.6%**	**13.0%**
Spousal/family communications only	**3.9%**	**4.5%**	**1.2%**	**5.0%**	**3.5%**
Emergency uses permitted	**6.7%**	**6.2%**	**8.6%**	**8.4%**	**4.3%**
No personal use whatsoever	**23.9%**	**27.1%**	**9.9%**	**25.6%**	**19.1%**

Twenty percent of respondent firms place some sort of time limitations on personal use of office e-mail connections – when employees may make such personal use, or for how long:

Time Restrictions on Personal E-Mail Use:	Whole Sample	Written E-Mail Policy Yes	Written E-Mail Policy No	Active Monitoring Yes	Active Monitoring No
Specific time duration limits	**7.4%**	**7.3%**	**7.4%**	**8.8%**	**3.5%**
Specific times during business hours	**2.3%**	**2.5%**	**1.2%**	**2.2%**	**2.6%**
Use during non-business hours only	**9.9%**	**11.3%**	**3.7%**	**10.6%**	**7.8%**

Notice how the rules change when the issue is internet connectivity rather than e-mail communication:

Personal Use of Office INet Connections:	Whole Sample	Written Internet Policy Yes	Written Internet Policy No	Active Monitoring Yes	Active Monitoring No
Full and unrestricted personal use	**11.7%**	**7.4%**	**26.3%**	**8.1%**	**23.5%**
Personal use allowed, websites restricted	**65.3%**	**70.8%**	**46.5%**	**69.1%**	**57.4%**
No personal use whatsoever	**19.5%**	**20.2%**	**17.2%**	**22.2%**	**12.2%**

Time Restrictions on Personal INet Use:	Whole Sample	Written Internet Policy Yes	Written Internet Policy No	Active Monitoring Yes	Active Monitoring No
Specific time duration limits	**7.8%**	**9.5%**	**2.0%**	**9.1%**	**4.3%**
Specific times during business hours	**3.9%**	**3.9%**	**4.0%**	**4.4%**	**2.6%**
Use during non-business hours only	**21.8%**	**24.7%**	**12.1%**	**22.5%**	**20.0%**

But more revealing are the restrictions set on connections to various types of websites. Bear in mind that only 38% of respondent firms use "blocking" software to prevent internet connections to unauthorized or inappropriate sites, so in many companies these restrictions must be enforced by monitoring:

Restricted Websites	Whole Sample	Written Internet Policy Yes	Written Internet Policy No	Active Monitoring Yes	Active Monitoring No
"Adult" sites with explicit sexual content	**76.6%**	**81.5%**	**59.6%**	**80.3%**	**66.1%**
Game sites	**26.4%**	**29.2%**	**17.2%**	**28.8%**	**20.0%**
Entertainment sites	**17.7%**	**19.6%**	**11.1%**	**19.4%**	**13.0%**
Sports sites	**14.7%**	**16.4%**	**9.1%**	**16.6%**	**9.6%**
Shopping sites	**13.1%**	**15.8%**	**4.0%**	**15.6%**	**6.1%**
Other sites	**11.5%**	**12.2%**	**9.1%**	**12.8%**	**7.8%**

This makes obvious what was stated above: management's primary concern is keeping sexually explicit materials off the screens of office pc's.

Legal Issues

The Microsoft antitrust case is the best known but by no means the only legal action where e-mail played an important evidentiary part. Concerning legal issues, the most frequent experience reported by respondent firms is receiving a subpoena for employee e-mail; subpoenas for records of internet connections are less common:

	Whole	Written Policy		Active Monitoring	
Received subpoena for:	**Sample**	**Yes**	**No**	**Yes**	**No**
Employee e-mail	**9.4%**	**10.5%**	**4.9%**	**9.4%**	**9.6%**
Record of internet connections	**2.5%**	**2.7%**	**2.0%**	**2.5%**	**2.6%**

Concerns over sexual harassment lawsuits are keyed to experience:

	Whole	Written Policy		Active Monitoring	
Defended Legal Claim(s) Based on Employee E-Mail and/or Internet Use	**Sample**	**Yes**	**No**	**Yes**	**No**
Sexual harassment/sexual discrimination	**8.3%**	**9.0%**	**2.2%**	**8.4%**	**7.8%**
Racial discrimination	**1.6%**	**1.8%**	**0.0%**	**1.9%**	**0.9%**

From these and previous tables presented here, we see a correlation between various policies and the experience of legal action. For example, those reporting legal action are more likely to have written policies; to have a policy on retaining and deleting e-mail; and to inform employees and new hires about their e-policies. Correlation is not causation, and no one would argue that having a policy invites legal action while the lack of a policy deters it. However, it is reasonable to assume the reverse: that legal action spurs the creation of formal, written policies that in turn determine other e-practices.

While liability issues may be as new as e-mail and the internet itself, software licensing and piracy are familiar concerns. The AMA questionnaire asked if respondent firms have notified employees that it is illegal to copy licensed software, and whether they have audited their computer systems to ensure against illegal or pirated software. We also asked if companies have been audited by such outside agencies as the Software and Information Industry Association (SIIA) or the Business Software Alliance (BSA). The results:

	Whole	Written Software Policy		Any Legal Action	
Software Issues	**Sample**	**Yes**	**No**	**Yes**	**No**
Employee notification	**91.0%**	**97.4%**	**80.5%**	**97.0%**	**90.0%**
Internal audit for illegal/pirated software	**66.9%**	**70.0%**	**40.0%**	**80.3%**	**64.5%**
External audit by SIIA, BSA, or others	**6.9%**	**7.0%**	**6.7%**	**6.1%**	**7.0%**

Disciplinary Actions

Under ***Legal Issues*** above, we put forward the argument that legal actions against a company prompt the creation of written policies. When we bring a history of disciplinary actions into the mix, both the "active monitoring" and "legal action" variables leap forward. No surprise that companies actively monitoring computer use report far more incidents of both termination and other discipline; monitoring is, after all, a primary tool in discovering misuse. Legal action, however, truly makes a difference: companies reporting legal action are far more likely to report terminations and other discipline for all of the reasons listed in the AMA questionnaire. The conclusion: being sued (or its prospect) is a mighty spur to disciplinary actions against those who misuse the technology.

Reasons/Disciplinary Actions	Whole Sample	Active Monitoring Yes	Active Monitoring No	Any Legal Action Yes	Any Legal Action No
Sending sexually suggestive or explicit material via office e-mail:					
Termination	**14.0%**	**15.6%**	**9.6%**	**36.4%**	**10.0%**
Other discipline	**29.7%**	**34.4%**	**16.5%**	**54.5%**	**25.2%**
Any discipline (total)	**46.3%**	**42.1%**	**19.9%**	**71.2%**	**30.1%**
Downloading, uploading, or viewing pornography via office internet connections					
Termination	**16.8%**	**18.8%**	**11.3%**	**33.3%**	**13.8%**
Other discipline	**26.9%**	**31.6%**	**13.9%**	**54.5%**	**22.0%**
Any discipline (total)	**36.3%**	**42.2%**	**20.0%**	**65.2%**	**28.5%**
Connecting to unauthorized, restricted, or non-business related websites:					
Termination	**9.4%**	**11.9%**	**2.6%**	**21.2%**	**7.3%**
Other discipline	**30.6%**	**35.0%**	**18.3%**	**53.0%**	**26.6%**
Any discipline (total)	**34.5%**	**40.0%**	**19.1%**	**65.6%**	**30.3%**
Sending a menacing, harassing, discriminatory, or otherwise objectionable e-mail:					
Termination	**7.4%**	**7.8%**	**6.1%**	**22.7%**	**4.6%**
Other discipline	**25.7%**	**30.9%**	**11.3%**	**43.9%**	**22.5%**
Any discipline (total)	**28.0%**	**33.4%**	**13.0%**	**65.5%**	**23.4%**
Illegally downloading or duplicating copyrighted software:					
Termination	**1.1%**	**0.9%**	**1.7%**	**1.5%**	**1.1%**
Other discipline	**13.6%**	**15.9%**	**7.0%**	**28.8%**	**10.8%**
Any discipline (total)	**14.3%**	**16.6%**	**7.8%**	**28.8%**	**11.7%**
Participating in 'adults-only" online chat-rooms via office internet connections					
Termination	**4.6%**	**5.0%**	**3.5%**	**10.6%**	**3.5%**
Other discipline	**9.9%**	**10.6%**	**7.8%**	**18.2%**	**8.4%**
Any discipline (total)	**12.6%**	**13.8%**	**9.6%**	**22.7%**	**10.8%**
Violating any e-policy:					
Termination	**17.2%**	**18.8%**	**13.0%**	**36.4%**	**13.8%**
Other discipline	**44.1%**	**50.6%**	**26.1%**	**71.2%**	**39.3%**
Any discipline (total)	**50.6%**	**56.9%**	**33.0%**	**79.7%**	**46.1%**

Technical Issues

Digital technology is at the heart of all this activity and is also central to the task of storing and reviewing content. Eyeball searches of written memoranda or analog review of recorded materials would be prohibitively expensive in both time and money; digitized search engines solve both problems. Nearly one respondent firm in four (23.9%) performs key word or key phrase searches of e-mail and/or computer files; this includes 21.7% of those providing **unrestricted** personal e-mail use. Let the user beware, then.

And what companies look for, far and away, are sexual and scatological phrases and language. Just as the greater share of discipline concerns sexually suggestive or explicit words and images, the greater share of search activity looks for the same category of words. Again we see how the fact or prospect of legal action, specifically in a sexual harassment suit charging a hostile workplace environment, is the main trigger to computer monitoring and surveillance.

		E-Mail Policy				
	Whole Sample	No Personal Use	Restricted Personal Use	Unrestricted Personal Use	Any Legal Action Yes	Any Legal Action No
Use Key Word/Phrase Searches	**23.9%**	**24.0%**	**28.5%**	**21.7%**	**36.4%**	**21.7%**
	(104)	**(25)**	**(41)**	**(38)**	**(24)**	**(80)**
Key Word/Phrase Search Categories	**[Pcts below are of firms that perform key word/phrase searches]**					
Explicit sexual or scatological phrases or language	**70.2%**	**80.0%**	**68.3%**	**71.1%**	**75.0%**	**68.8%**
Names of current employees	**18.3%**	**16.0%**	**26.8%**	**15.8%**	**20.8%**	**17.5%**
Names of clients, customers, accounts	**16.3%**	**8.0%**	**14.6%**	**23.7%**	**16.7%**	**16.3%**
Names of vendors and suppliers	**14.4%**	**12.0%**	**12.2%**	**21.1%**	**16.7%**	**13.8%**
Names of former employees	**13.5%**	**16.0%**	**17.1%**	**10.5%**	**8.3%**	**15.0%**
Brand names of products/services	**10.6%**	**4.0%**	**12.2%**	**10.5%**	**8.3%**	**11.3%**
Brand names of other orgs.' products/svcs	**9.6%**	**4.0%**	**12.2%**	**10.5%**	**4.2%**	**11.3%**
Names of prospective employees	**2.4%**	**0.0%**	**4.9%**	**2.6%**	**4.2%**	**2.5%**
Other	**15.4%**	**16.0%**	**14.6%**	**13.2%**	**8.3%**	**17.5%**

Employee misuse is one issue, employee sabotage another; the latter is far more rare. To the question "Has your organization's e-mail and/or internet system ever been attacked and/or sabotaged by a current or former employee?" only 17 surveyed firms, or 3.9% of the sample, answered yes.

But business interruptions are common, especially due to computer viruses:

Business interruptions due to:	**Yes**
Computer virus	**62.5%**
Mandatory software audit	**6.9%**
Denial of service attack	**4.6%**
Employee sabotage	**2.1%**

Not all viruses lead to business interruptions: in total more than three-quarters of respondent firms report viruses (77.5%), most often coming through as e-mail attachments. Those with written policies and those that monitor computer use are somewhat more likely to report viruses – again suggesting that the policies are written and implemented after the problems occur for the first time.

	Whole	Written Policy		Active Monitoring	
Virus Entered Through:	**Sample**	**Yes**	**No**	**Yes**	**No**
E-mail attachments	**75.4%**	**76.2%**	**68.9%**	**77.2%**	**70.4%**
Software download from the internet	**12.6%**	**12.8%**	**11.1%**	**13.1%**	**11.3%**
Illegally duplicated or pirated software	**6.2%**	**6.4%**	**4.4%**	**7.5%**	**2.6%**
Malicious hacker attack	**2.1%**	**2.3%**	**0.0%**	**2.2%**	**1.7%**

About This Survey

In April 2001 the AMA follow-up questionnaire on electronic monitoring and surveillance policies and practices was mailed to 1,627 participants in AMA's 2001 annual survey on workplace testing and monitoring. The earlier sample accurately mirrored AMA's corporate membership and client base, who together employ one-fourth of the U.S. workforce, but because such companies are largely drawn from the top five percent of U.S. businesses in terms of annual sales and total employees, that sample did not accurately reflect policies in the U.S. economy as a whole, where smaller firms predominate.

By July 1, 435 usable responses to the follow-up survey were in hand, forming the database for this report with a ±4.8% margin of error. The commonly used sub-groups for the tables in this summary have, of course, larger margins of error:

	Whole	Written Policy		Active Monitoring		Any Legal Action	
Sub-group	**Sample**	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**
Respondents in group	**435**	**390**	**45**	**320**	**115**	**66**	**369**
Margins of error	**±4.8%**	**±5.1%**	**±14.9%**	**±5.6%**	**±9.3%**	**±12.3%**	**±5.2%**

For the original survey sample of 1,627, the demographics were weighted against the respondent bases of the previous three years to give validity to comparisons with previous years' survey findings. Here are the demographic descriptors for the weighted original 2001 sample and for the sample for the follow-up survey, which is unweighted.

	Original	Follow-up		Original	Follow-up
Number of Employees (U.S.)			**Annual Sales (or budget)**		
Fewer than 100	3.3%	5.3%	Less than $10 million	9.8%	13.8%
100 to 499	16.2%	19.5%	$10 million to $49 million	18.3%	29.0%
500 to 999	10.8%	10.1%	$50 million to $249 million	27.7%	29.2%
1,000 to 2,499	11.4%	8.0%	$250 million to $499 million	12.1%	7.8%
2,500 to 9,999	12.0%	8.7%	$500 million to $999 million	7.8%	4.6%
10,000 or more	9.3%	6.7%	$1 billion or more	13.3%	8.5%
Not reported	36.9%	41.6%	Not reported	11.0%	**7.1%**
Business Category			**Geographical Region**		
Manufacturing	51.0%	48.3%	New England	5.5%	6.2%
General Services – nonprofit	12.0%	13.8%	Mid Atlantic	18.1%	13.3%
General Services – for profit	9.5%	9.4%	South	17.4%	17.7%
Business & Professional Services	8.6%	7.8%	Midwest	36.8%	39.3%
Wholesale & Retail	8.3%	9.0%	Southwest & West	10.9%	8.7%
Financial Services	7.7%	7.8%	Pacific	13.2%	13.8%
Public Administration	2.5%	3.2%	Not reported	1.3%	1.0%
Unclassified	0.4%	0.7%			

The follow-up questionnaire was designed with contributions from Nancy Flynn of the ePolicy Institute and author of ***The ePolicy Handbook***, and Dana Hawkins, Senior Editor at ***U.S. News & World Report***.

A complete printed datapack of all survey findings and the original raw data files (stripped of identifiers to protect the confidentiality of our respondents) may be purchased from AMA Research. For further information, visit our website (www.amanet.org/research) or contact Carol Canzoneri, Manager of Research Operations, at 212-903-7933 or ccansonzeri@amanet.org