

Employee E-mail and Internet Usage Monitoring



Issues and Concerns

[Introduction](#) 3

[Pros & Cons of Monitoring](#) 3

[Monitoring Pros \(Arguments for Monitoring\)](#) 3

[Facts](#) 6

[Formulating Appropriate Policies](#) 9

[Attributes of a Good E-mail, Internet Usage and Monitoring Policy](#) 10

[Steps for Evaluation and Deployment](#) 12

[Attributes of GOOD Monitoring Software](#) 12

[E-Mail Attributes](#) 12

[Internet Usage Attributes](#) 13

[Who can help?](#) 13

[Conclusion](#) 14

[TRG's Approach to Implementing Email and Internet Usage in the Workplace](#) 15

[Why Choose TRG](#) 18

[Philosophy](#) 18

[Technology Partners](#) 19

[Software Products](#) 19

[Hardware Products](#) 19

[Business Partners](#) 21

[TRG Qualifications](#) 22

[Technology Marketplace](#) 23

[Contact Information](#) 23

[More Information](#) 24

Introduction

Technical Resource Group (TRG) has created this document in order to provide information regarding the electronic monitoring of employee e-mail and Internet usage. Electronic monitoring of employee e-mail and Internet usage is more than just implementing a software application and turning it on. Companies are adopting workplace monitoring policies, procedures and systems at an increasing rate, as evidenced by the rapid growth of monitoring software offerings and surveys that have been done. According to the 2001 IDC survey on workplace monitoring the industry is expected to triple by 2004.

The choice to electronically monitor employee e-mails and Internet activities needs to be driven by upper management. There are delicate issues of trust and loyalty that need to be addressed in order to preserve the culture of the organization. Implementing monitoring requires planning, policies and procedures.

Opponents and proponents on monitoring agree that organizations need clear and definitive policies on electronic surveillance, and that these policies should be frequently and effectively communicated to employees. They also agree that employees should undergo formal training on e-mail and Internet policies, proper usage and conduct.

This paper presents the key issues surrounding workplace monitoring of employee e-mail and Internet usage. In addition, this paper provides guidelines for appropriate policy formation. This paper presents a summary of features that should be present in any e-mail and Internet monitoring application. Also included in this paper are resources where additional information can be found.

Pros & Cons of Monitoring

Monitoring Pros (Arguments for Monitoring)

Proponents for the monitoring of employee e-mail and Internet activity maintain that employers must take proactive steps to insure for the following:

- Assists in making the work environment free from hostile and harassing activity. This improved work environment lowers the exposure to employee lawsuits as monitoring assists in creating a safe and secure working environment.
- Employees maintain efficient and productive work habits. These improved work habits would boost efficiency, increase productivity and improve customer service.

- ⌋ Employees avoid misuse of the employer's equipment and resources. This misuse could clog up network bandwidth and computer disk space.
- ⌋ Sensitive information about trade secrets, intellectual property, customers, employees, and financial data is properly protected.

Employers are being held legally liable for the atmosphere in the workplace. They can be directly and indirectly liable for sexual harassment based on a hostile work environment. Employers have been found liable for failing to monitor and prevent inappropriate e-mail once put on notice by employees. The following case is an example of this:

- ⌋ (Blakey v. Continental Airlines June 2000 – NJ Supreme Court unanimously ruled that an employer had a duty to remedy electronic harassment because it had received notice that the employees were posting defamatory and harassing messages on the company's electronic bulletin board)

Employers have been found NOT liable when policies and procedures are in place and are followed. The following cases are examples of this:

- ⌋ Schwenn v. Anheuser-Busch, Inc. – Employee failed to establish a claim of a hostile work environment after receiving sexually harassing e-mail messages because the employer had an e-mail policy in place and promptly conducted meetings with employees involved to reiterate the company's sexual harassment policy.
- ⌋ Daniels v. WorldCom – Employer prevailed against employee claim of negligence for allowing "racially harassing e-mail on its computer system," greatly in part because it produced written policies that both included a comprehensive remedy procedure and was actively supported by management.

Other cases where employers prevailed against employee privacy suits:

- ⌋ Bourke v. Nissan Motor Corp. – 1993
- ⌋ McLaren v. Microsoft Corp – 1999
- ⌋ Simmons v. Southwestern Bell Telephone Co. – 1979
- ⌋ Bohach v. City of Reno – 1996

These legal issues are real and valid and monitoring could most likely be justified on the basis of curtailing sexual harassment in the workplace alone. However, monitoring is a two-edged sword. Currently, employers are not liable for harassment unless they are made aware that harassment is occurring. If an organization monitors employees then the organization assumes responsibility for the all content it monitors, whether an employee brings an issue

to the organization's attention or not. Employers are finding themselves between a rock and a hard place. Not monitoring could be seen as negligent while *monitoring but not acting on violations IS negligent*.

Monitoring Cons (Arguments for Not Monitoring)

Opponents of monitoring employees also make some valid arguments, many of which are around ethical, moral and cultural issues. Some of the arguments against monitoring are as follows:

- ┆ Loss of respect and trust for employer resulting in higher turnover, loss of productivity and decay of a positive work culture.
- ┆ People are paid to do a job, and so long as the job is done within the specified parameters, they should be allowed some personal freedoms at work.
- ┆ Monitoring costs the company more than it saves. It is a distraction to getting the business of the business done.
- ┆ Workplaces that are subject to high surveillance typically are culturally in trouble where trust is missing.
- ┆ Data collected during monitoring is subject to misuse in ways that could subject the organization to great liabilities.
- ┆ Disgruntled or disturbed employees can cause a company legal grief and liability in other ways by writing a letter, having a conversation, sending a FAX or making a phone call just as easily as by sending an e-mail.
- ┆ Without proper checks and balances, employers may take on a "Big Brother" role and abuse monitoring. Corporate governance needs to be explored in this area.

Facts

Two major surveys were completed in 2001. The American Management Association conducted the first of these surveys. The following is a partial list of key findings:

- ┆ 68% site Legal Liability
- ┆ 60% site Security Concerns
- ┆ 45% site Productivity Concerns
- ┆ 50% site Legal Compliance / Governance

IDC also compiled a survey in 2001. Following is a partial list of the survey's key findings:

- ┆ 57% of US companies are now monitoring employees
- ┆ 70% of firms with more than 1,000 employees monitor their employees
- ┆ 48% of employers site the need to protect against viruses and lost of information as the reason to monitor employees
- ┆ 21% site limiting legal liability as the driving reason to monitor employees

- i The Monitoring Software Market is growing about 36% a year
- i Industry revenue is expected to triple from 2001 to 2004

It is clear that these two surveys confirm that e-mail and Internet usage monitoring is becoming more and more commonplace.

In addition to these two surveys other organizations have been compiling statistics and notes about workplace monitoring. Consider the following:

- i 14 Million U.S. workers are currently having online access monitored (Privacy Foundation).
- i The primary complaint from employers is that employees do not distinguish between workplace and personal communications (The National Workrights Institute – Princeton NJ).
- i There was an ordered shutdown of employee tracking software in the Ninth Circuit Court of Appeals (Federal Appeals Court Judge Alex Kozinski). In an open letter to federal judges published in the Wall Street Journal, Kozinski wrote, “The proposed policy tells our 30,000 dedicated employees that we trust them so little we must monitor all their communications...how did we get to the point of even considering such a draconian policy?”
- i 1986 Electronic Communications Privacy Act, while prohibiting unauthorized interception of e-mail and other types of electronic communications, exempts service providers. This could include employers who provide e-mail and Internet access through their networks.
- i Employees have “No reasonable expectation of privacy at work” – Smyth v. Pillsbury (Smyth sent threatening e-mails to a supervisor, which were intercepted by the employer).
- i The New York Times fired 23 employees and disciplined 20 others for exchanging inappropriate e-mails with co-workers.
- i Dow Chemical fired 50 employees and 200 more faced suspension for transmitting offensive, pornographic, and explicitly violent materials.
- i Edward Jones & Company terminated 19 employees for failing to admit they sent pornography or off-color jokes over the company’s e-mail.
- i Philosophically and morally, employees are first and foremost people who are autonomous moral agents, where their moral status is defined by a set of rights. These rights include the right not to be used by others solely for the purpose of personal or organizational enrichment ... They are entitled to respect, which implies some right to privacy (Michael J. Meyer, SCU Professor of Philosophy).

With the move toward increased monitoring of employees, it may be just a matter of time

before companies begin to monitor other forms of communications such as phone calls, regular mail and faxes.

Formulating Appropriate Policies

The following should be considered when creating organizational policies related to e-mail and Internet usage:

Should the organization consider a BAN in outgoing e-mails of the following:

- i Racial language or images?
- i Sexist / sexual comments or images?
- i Jokes?
- i Operational results?
- i Negative tones about the company, customers, employees, vendors, etc.?

Should the company formalize the way all e-mails should be constructed:

- i Salutations?
- i Signed / ended?
- i Use of Emoticons?
- i Appropriate visual shorthand?

Should the company BAN access to inappropriate web sites that include:

- i Sexually explicit language or images?
- i Violent language or images?
- i Offensive language or images?

Should the company BAN use of e-mail and / or the Internet for personal use for the following:

- i Game playing?
- i Chat rooms?
- i Gambling?
- i Shopping?
- i Research?
- i Blogs?
- i Any activity not specific to their job and duties?

Should the company explicitly PROHIBIT posting or transmitting any material that could be

interpreted as being the following:

- i Obscene?
- i Hateful?
- i Malicious?

- i Threatening?
- i Hostile?
- i Abusive?
- i Vulgar?
- i Defamatory?
- i Profane?
- i Racial?
- i Sexual?
- i Ethnically objectionable?

While some of the answers are easy, others are subject to much debate and should be thoroughly explored before deploying policy, procedures and technology.

Attributes of a Good E-mail, Internet Usage and Monitoring Policy

The following is a list of guidelines that are important to consider when formulating e-mail, Internet usage and monitoring policy:

- i State the intent of the policy – why it is positive for the organization, employees, customers and other stakeholders.
- i State the guidelines and circumstances for policy enforcement.
- i Be specific as to how the company views an employee’s right to privacy while at work.
- i Be specific on the filtering and monitoring processes and procedures that will be conducted.
- i Be specific on the company’s position on employee accountability related to the content of e-mails, and the appropriateness of their communications with employees, customers, vendors and the community at large.
- i Be specific as to what constitutes “appropriate content.”
- i Be specific on the company’s position on the personal use of e-mail, the Internet or

other company assets.

- i Be VERY specific on the consequences and disciplinary actions that will result from violation of the policy.
- i Integrate the policy in context of the company's overall set of policies.
- i Require all employees to read and acknowledge their understanding of the policy via a signed affidavit that will reside in their personnel file.

Steps for Evaluation and Deployment

The process for evaluating and deploying the practice of monitoring e-mail and Internet usage in the workplace should be inclusive in its design.

The following is a list of recommended steps to follow:

1. Educate Executive Management on employee monitoring issues (Pro & Con).
2. Form a cross functional / Human Resource (HR) Department-led Task Force to coordinate the development of an overall deployment strategy including:
 - i Design of communications standards
 - i Design of employee orientation & training programs
 - i Design of workflows and procedures related to:
 - ◆ Monitoring and Detection
 - ◆ Ongoing and Issue Specific Communications to Employees
 - ◆ Disciplinary Notifications and Subsequent Actions
 - ◆ On-going Quality Reviews and Audits
3. Identify and acquire technologies to be used (Monitoring, Filtering, etc.).
4. Project plan for rollout.
5. Oversee the deployment process.
6. Conduct periodic post deployment quality and compliance audits.

Attributes of GOOD Monitoring Software

There are no standards around which e-mail and Internet monitoring software is written. As with most software applications, it is the buyer's responsibility to understand their requirements and to buy accordingly. Following is a list of attributes that should be considered when evaluating monitoring software:

E-Mail Attributes

- i Ability to search e-mails and attachments (inbound and outbound) for keywords and phrases.
- i Ability to quarantine e-mails for review prior to forwarding (inbound and out-

bound).

- i Ability to randomly select e-mails for review.
- i Ability to send employees a notification that their e-mail has been selected for review and the criteria used for selection.
- i Ability to track and report on all quarantined e-mails and their disposition.
- i Ability to create filters to block spam and to block specific e-mail addresses and domain extensions (@abc.com).

Internet Usage Attributes

- i Ability to block sites from access.
- i Ability to get regular vendor updates on URL's known to be offensive.
- i Ability to block URL sites based on specific words and phrases.
- i Ability to track all sites visited by each employee being monitored and the following information:
 - ◆ Time on site
 - ◆ Frequency of visit
 - ◆ Number of pages accessed
- i Ability to notify employees when they try to access a banned site.
- i Ability to produce monthly employee site visitation usage reports suitable for distribution to employee (via e-mail or hardcopy) after management review.
- i Ability to monitor and control instant messaging activity.

Who can help?

Not all organizations can implement employee monitoring on their own. In most cases, hiring a firm that is an expert in employee monitoring and can focus on the project is advisable. Selecting the best company for implementing monitoring is an important decision for your organization since it affects the employees.

The company selected should be the following:

- i Knowledgeable and experienced in Human Resources issues and understanding of the organization's culture.
- i Knowledgeable and experienced in technology issues, as technology will need to be implemented for monitoring to be successful.

- i Trustworthy, as they will be exposed to sensitive information in your organization.
- i Easy to do business with.

A good source to locate such firms would be local human resource organizations or your local Chamber of Commerce.

Conclusion

The monitoring of employees is a delicate issue that must be handled properly. Communication to the employees is critical as well as employee involvement in the implementation of any kind of monitoring technology. The policies and procedures must be clearly stated and followed for an organization to be properly protected. Hopefully, this document assisted in the decision as to whether monitoring should be done, and if so, how to implement it successfully into the organization.

TRG's Approach to implementing Email and Internet Usage in the Workplace

TRG has dedicated and experienced resources to work with an organization to define needs, costs, and options. TRG has a proven track record after years of innovation and achievement and, as a technology leader, can bring more overall understanding of data protection and the recovery technologies that are available to your organization. With TRG's unparalleled experts in business solutions and data protection, TRG can assure you a reliable plan.

You can also trust TRG to prepare your organization with a thorough business impact analysis, risk assessment, recovery plan development, and disaster recovery plan testing to enable you to respond to the unexpected. TRG can provide a complete evaluation of the consequences that would be experienced during an organization's interruption. This will enable your organization to be accountable to your customers, employees, and shareholders when your organization's very survival can be at risk.

TRG's approach to implementing Email and Internet Usage in the Workplace insures that the effort will be successful. The process consists of the following:

- ┆ Formal Assessment of the Your Company's Needs
 - ┆ During this phase of the effort TRG meets with top management and other key personnel to identify the issues and concerns related to monitoring email and Internet usage. Special care is taken to help employees to understand the rationales supporting monitoring.
- ┆ Creation of a Report & Plan Detailing
 - ◆ Current Areas of Risk,
 - ◆ Costs
 - ◆ Benefits
 - ◆ Technology Required
 - ◆ Software Required
 - ◆ Management Processes
 - ◆ Work Plan for Deployment
 - ◆ Training, and

- ◆ Ongoing Support

TRG works closely with the client to schedule and implement each step of the plan. Throughout the process TRG insures that the implementation goes smooth and without disruption of client's workforce.

TRG is a certified partner with SurfControl, the leading provider of e-mail content filtering and monitoring. Implementing an e-mail monitoring system is just as much a Human Resources issues as it is an Information Technology issue. TRG is sensitive to the employee's needs as well as the upper management's needs. TRG can tailor the proper e-mail and Internet guidelines for any organization

Appendix A: About TRG

Why Choose TRG

Technical Resource Group (TRG), headquartered in Santa Ana, California, was formed in 1995. TRG has a group of dedicated expert consultants who work together to align information technology with the business needs of its clients. TRG is highly respected in the business technology arena as well as being known for their service and support integration expertise. TRG has a long and successful proven track record. TRG's growing team of professional, high technology experts includes individuals that work together to solve business needs in today's ever-changing marketplace. TRG also has an outside team of nationally recognized experts in areas of strategic planning, business process improvement and key industry consultants that are available when their individual expertise and knowledge is required to assist the TRG team to solve client business challenges. Over the years, TRG has successfully partnered with its clients to deliver solutions in the areas of

- | Strategic IT Planning and Deployment
- | Business Process Improvement
- | Application Evaluation, Selection & Implementation
- | Custom Application Design and Development
- | Infrastructure and Network Planning, Implementation & Management
- | IT Facilities Management
- | IT Security Administration
- | Business Intelligence and Data Warehousing
- | Document & Workflow Management

TRG has over 400 clients throughout the United States with a majority in the Southern California area. The company's loyal client base ranges from single user installations to the Los Angeles Unified School District that has a 1000-user installation. Talent, variety, size and stability—TRG has all the qualities and expertise that create a successful IT service company.

Philosophy

TRG's philosophy is to give its clients a personal touch; however, still have a company structure and strength behind that personal touch.

Goal

TRG's goal is to be the company our clients and prospects call for all their information technology and computing needs. TRG wants leverage its client's growth and sustained prosperity. TRG's team strives to deliver the best services, products and information possible to their clients and to provide them with in-depth insight, technical knowledge and solutions for the success of the organization.

Technology Partners

TRG is proud to offer excellent powerful and high performance products and specialized services from these industry-leading technology companies:

Software Products

- ***Microsoft***—Windows Operating Systems: 2000/2003/XP and related products such as Office, Exchange, IIS, VB & SQL Server
- ***IBM***—Database Products & Tools such as UniVerse, UniData, wIntegrate & SB+
- ***SurfControl***—E-mail and Web Filtering
- ***Raining Data*** (formally Pick Systems)—Database Products & Tools such as D3, mv.BASE, mv. ENTERPRISE & FlashCONNECT
- ***jBASE***—Database Products & Tools
- ***MITS***—Business Intelligence Products
- ***Accusoft***—AccuTerm Terminal Emulator
- ***Esker Software***—DeliveryWare & VSI-FAX Fax Server
- ***Keynet***—Imaging Solutions
- ***Symantec***—pcAnywhere & Norton AntiVirus
- ***Veritas***—Backup Exec
- ***Via Systems***—Viaduct Terminal Emulator
- ***AcuPrint***—Secure Printing

Hardware Products

- Hewlett-Packard/Compaq—Intel-based Servers
- IBM—RS/6000 (pSeries) Servers
- Wyse—Wintermis/Thin Clients
- APC—Uninterruptible Power Supplies

- PF Micro— Intel-based Servers

Business Partners

- ***The Natural Intelligence Group (TNIG)***—Management Consultancy for business process improvement and reengineering
- ***Hartley & Associates***—Professional Services include Interim Management, Organization Building, Recruiting, Sales, Marketing & Advertising

TRG's account managers, technicians and consultants work closely with its partners to develop solutions for specific clients' needs and to assist with every challenge for all types and sizes of organizations.

TRG Qualifications

- **Windows Terminal Server professionals on staff.** At recent and upcoming trade shows, TRG is giving presentations on the benefits of Citrix, Windows Terminal Services and Thin Clients. Internally, TRG uses Thin Clients and Windows Terminal Services.
- **Microsoft Certified Partner** that has expertise in supporting Windows NT/2000/2003/XP, Exchange Server, Proxy Server, IIS and Excel. TRG has full-time Microsoft certified staff members (MCSE, MCP, MOUS).
- **Authorized IBM reseller** including UniVerse and UniData database products and tools and MITS business intelligence product and have on staff AIX operating system experts.
- **Over 175 years of experience in MultiValue/Pick** application design, programming and support.
- **Single Source for Hardware, Software and Services**, if client desires a single source. Or, if client chooses, TRG can provide one piece of the puzzle if the client has coverage in other areas.
- **Authorized Hewlett-Packard/Compaq Reseller (VAR)** with Certified professionals (ASE) on staff.
- **Value Added Reseller for all Raining Data** products and tools including D3, mv.BASE, mv.ENTERPRISE and FlashCONNECT.
- **Reseller of numerous supplementary products** such as APC uninterruptible power supplies (UPS), Esker VSI-FAX faxing software, Esker DeliveryWare, Keynet Imaging, AccuTerm terminal emulator, print servers, etc. that are important and necessary for TRG clients' IT requirements.
- **Windows application and Web development teams** that are knowledgeable in Visual Basic, SQL Server, FrontPage, HTML, etc.
- **Professional Service employee consulting staff**, in addition to specialized outside consultants to assist TRG employees when appropriate to solve the business needs of TRG's Clients.

TRG meets all the necessary qualifications for implementing a monitoring solution in an organization and has excellent references. In addition to referenceable clients such as Aloha Freight Forwarders and Pindler & Pindler, TRG has implemented monitoring technology internally for all the same reasons mentioned in this paper.

TRG has dedicated and experienced resources to work with an organization to define needs, costs, options, and possible cost savings. TRG has experts in solving interoperability issues between existing desktop hardware, operating system platforms and Windows NT/2000/2003-based applications. Additionally, TRG has a proven track record after years of innovation and achievement and, as a technology leader, can bring more overall market understanding to Thin Client technology. With TRG's unparalleled experts in business solutions, TRG can assure organizations an effective monitoring solution. For more information on monitoring, visit www.picktrg.com.

Technology Marketplace

Organizations can choose a large and expensive consulting company that may not take the time to know the organization or their current technology. Organizations can choose a one-man shop that does not have the technology expertise in all the areas the organization needs and cannot keep pace with the ever-changing technology. A single person cannot possibly be knowledgeable in all areas of Information Technology (IT). There is also the high probability that the one-man shop might be out of business tomorrow.

TRG's team specializes in emerging technology solutions. TRG's service offerings include advisory, consulting and assessment services. TRG's close-knit team can bridge the gap between complex non-Windows based IT infrastructures such as UNIX and Windows NT/2000-based environments. TRG has the expertise that can provide cost-effective solutions that are specific to organizations in all their IT needs and business-critical applications.

Contact Information

Technical Resource Group (TRG)
2850 Red Hill Ave. Suite 110
Santa Ana, CA 92705
949.296.8380— Fax 949.756.0029
E-mail: asktrg@picktrg.com
Web Site: www.picktrg.com

More Information

For the latest information about our products and services, please see the following:

www.picktrg.com

References/Additional Resources

- s Center for Democracy and Technology – www.cdt.org
- s Electronic Frontier Foundation – www.eff.org
- s Electronic Privacy Information Center – www.epic.org
- s Privacy Rights Clearinghouse – www.privacyrights.org
- s ACLU Freedom Network: Cyberliberties – www.aclu.org/issues/cyber/hmcl.html
- s Yahoo Privacy Resources – www.yahoo.com/law/privacy
- s Employee Monitoring: Is There Privacy in the Workplace? - <http://www.privacyrights.org/fs/fs7-work.htm>
- s AMA (American Management Association) – 2001 AMA Survey on Workplace Monitoring & Surveillance
- s IDC 2001 Survey on Workplace Monitoring
- s “Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age” by Mark S. Dichter and Michael S. Burkhardt
- s “The Right to Goof Off” By Joseph Garber; Forbes (Oct. 20, 1997 - p. 297)
- s “The Impact of Federal Legislation to Limit Electronic Monitoring” by Paul S. Greenlaw and Cornelia Prudeanu – Public Personnel Management #26, 2 (June 22 1997 – p. 227)
- s “Liberal and Communitarian Defenses of Workplace Privacy” by Rita C. Manning – Journal of Business Ethics, 6, 8 (June 1997 - p. 817)
- s “Privacy, Morality, and the Law” by W. A. Parent – Philosophy & Public Affairs 12, 4 (Fall 1983 – p. 269)