



Internet Monitoring and Workplace Privacy (United States)

This document outlines legislation that regulates Internet and network monitoring in the US. Organizations that are using or intending to implement a form of electronic monitoring can use this document as a starting point to determine their legal rights and responsibilities.

This document is intended as a guide only - it aims to introduce the reader to issues which may be relevant to their organization, and to point out sources from which more detailed information may be obtained. It is **NOT** a substitute for professional legal advice.



WebSpy and Privacy

WebSpy products are used by organizations around the world to monitor the usage of shared electronic resources by their members. This monitoring enables organizations to verify that the resources they provide are being used for the purposes for which they are intended. For any organization currently employing or intending to employ a form of electronic monitoring, it is useful to be aware of current privacy legislation and the effect that it may have upon your monitoring practices.



Current Privacy Legislation in the US

Legislation exists at both the federal and state level to regulate Internet and network monitoring within organizations.

Federal Legislation

Organizations need to be aware of two Federal Acts when employing any form of electronic monitoring;

- Electronic Communications Privacy Act of 1986
- National Labor Relations Act

Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 (ECPA) is the main Federal statute offering members of organizations protection with regards to Internet and network monitoring. It prohibits the intentional interception of electronic communications. However, a number of exceptions exist that facilitate the monitoring of members within organizations.

Under the ECPA, an employer cannot monitor employee telephone calls or electronic mail when employees have a reasonable expectation of privacy. However, an organization may intercept communications when there is actual or implied member consent. Simply notifying members that monitoring takes place can constitute consent.

Consent is not implied if employees are aware that the organization could monitor their emails or calls. The organization needs to notify members that monitoring will actually occur.

Organizations are also permitted to monitor networks for business purposes. Employers may not monitor purely personal calls. However, determining whether a call is personal usually involves monitoring some of the conversation.

Organizations are authorized to monitor members if the employer has reason to believe that the company's interests are in jeopardy.

The ECPA essentially enforces the principle that organizations should not be able to violate a member's reasonable expectation of privacy.

National Labor Relations Act

The National Labor Relations Act (NLRA) guarantees workers the right to join unions without fear of management reprisal. It prohibits employers from committing unfair labor practices that might discourage organizing or prevent workers from negotiating a union contract.

The NLRA may have some relevance to Internet and network monitoring. The National Labor Relations Board (NLRB) has reported that a company's computer network is a "work area". Any rules prohibiting all non-business use of e-mail on a company's network could therefore be considered unlawful under the NLRA. Organizations can also be in violation of the NLRA when the monitoring of members is found to selectively punish labor organizing activities.

State Legislation

Some states have statutes that require organizations to give notice to members before engaging in electronic monitoring activities. However, even in states with legislation covering this issue, organizations wishing to monitor their members are not necessarily restricted. Most state laws covering this issue attempt to impose regulations on the frequency and extent of notification.

If you wish to find out whether or not your state has legislation covering the issue of Internet and network monitoring, please see:

<http://www.epic.org/privacy/consumer/states.html>



Is your organization affected?

The ECPA and the NLRA apply to both private and government sector organisations. Government employees may also have some protection under the Fourth Amendment concerning search and seizures. However, a government employee's expectation of privacy can be affected by office policies and practices.

The Federal Government also has the right to perform searches in the interest of promoting efficient workplace operations. Government employers can also weaken expectations of privacy by informing employees that they do not have an expectation of privacy, or that their desks, computers, and lockers may be searched.



Implications for Monitoring

Internet and network monitoring products such as those developed by WebSpy Ltd. can be used, as long as organizations do not violate their members' reasonable expectation of privacy, and act within the regulations set out in the ECPA.

WebSpy Ltd. recommends that organizations develop comprehensive Privacy and Acceptable Internet and Email Usage policies, and communicate these policies to their members. A privacy policy should at least state the methods and purpose of any monitoring taking place.

When correctly formulated and implemented, such a policy will ensure compliance with the ECPA. However, organizations need to research the legislation regarding Internet and network monitoring in the states they conduct business to determine their responsibilities, before they implement any form of monitoring activity.

The ILO Code of Practice

The International Labor Organization (ILO) is an active organization in the debate surrounding Internet and network monitoring. It has developed a code of practice that may be used as a guideline for other organizations developing their own Privacy and Acceptable Use policies.

The code specifies that workers' data should be collected and used consistently with Fair Information Practices (FIPs).

These practices include:

- **Notice**
Data collectors must disclose their information practices before collecting information from consumers.
- **Choice**
Consumers must be given options with respect to how personal information collected from them may be used for purposes beyond those for which the information was provided.
- **Access**
Consumers should be able to view and contest the accuracy and completeness of data collected about them.
- **Security**
Data collectors must take reasonable steps to assure that the information collected from consumers is accurate and secure from unauthorized use.



Developments

The Clinton Government proposed legislation to amend the ECPA as it applies to hardware and software surveillance.

The legislation called for

- Email interception court orders to be pre-approved by high level justice department officials
- The suppression of illegally seized email
- An annual compilation and publication of government email monitoring

Other bills have been proposed, such as the Notice of Electronic Monitoring Act that requires employees to give "clear and conspicuous" notice of any monitoring activity to employees, unless the employee is engaged in conduct which violates the employers or others rights, or harms the employer.

These bills are still in review.



Resources

There are many useful resources on the web to help you find out about privacy legislation. However, it is always good practice to verify any information you find.

Legislation

- Electronic Communications Privacy Act 1986
<http://www4.law.cornell.edu/uscode/18/2510.html>
- National Labor Relations Act
<http://www.nlr.gov/publications/nlr4.pdf>
- Connecticut State – An Act requiring notice to employees of electronic monitoring by employers
<http://www.cga.state.ct.us/ps98/act/pa/pa-0142.htm>

Related Organizations and Interest Groups

- American Civil Liberties Union
www.aclu.org
- Computer Professionals for Social Responsibility
<http://www.cpsr.org>
- Electronic Privacy Information Center
<http://www.epic.org>
- Labour Start
<http://www.labourstart.org>
- International Labour Organization
www.ilo.org
- National Labor Relations Act
<http://www.nlr.gov/publications/nlr4.pdf>
- Privacy Foundation
<http://www.privacyfoundation.org>
- Privacy International
<http://www.privacyinternational.org>
- Privacy Organisation
<http://www.privacyexchange.org>
- US National Labor Relations Board
<http://www.nlr.gov/index.html>

Other

- Listing of States with applicable legislation
<http://www.epic.org/privacy/consumer/states.html>
- Privacy Rights of Employees Using Workplace Computers in California
<http://www.privacyrights.org/ar/employees-rights.htm>



- Model Acceptable Use Policy
<http://www.efa.org.au/Publish/aup.html>
- Privacy Online: Fair Information Practices in the electronic marketplace, A Report to Congress
<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of WebSpy Ltd.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by WebSpy Ltd, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

WebSpy Ltd. reserves the right to change details in this publication without notice.

Other product and company names herein may be the trademarks of their respective owners.