A. WesTin S.O.W.

DRAFT

Statement of Work
Employee Monitoring

Introduction

The contractor shall execute the following tasks in accordance with the technical proposal submitted December 11, 1985. Any change in this plan must be approved by OTA.

Task 1

The contractor will trace the historical trends of employers' monitoring of workers' activities in the U.S. The trends will extend from the 19th century to the present, as appropriate, to include a portrayal of actual monitoring practices, and the influences over time--on limiting or extending monitoring practices--of factors such as: common law, State and Federal legislation; labor union-management agreements; technological and other capabilities. The past few decades will be emphasized, with focus on the monitoring of office workers' use of employers'information technology resources (telephones, personal computers, mainframe computers); identifying recent trends in the balance of influence among governments (Federal and State), employers, and labor unions; and likely future directions. Representative case examples will be provided to illustrate practices and trends for the above.

The issues to be explored include:

Workers' Legal Rights to Privacy. What have been U.S. workers' (esp. office workers') legal rights to privacy in the workplace and how have these changed over time (historical and current rights)? What have been workers' expectations of privacy and what changes are discernible over time? Provide a definitive description of workers' current privacy rights, and the legal basis for those rights, noting where the law is unclear.

Different kinds of privacy issues. Describe the different types of issues raised by worker monitoring and their significance in terms of protecting workers' rights, e.g., legal privacy, ethical privacy, moral privacy.

Significance of the types of information monitored and methods for monitoring. Are there types of personal information for which monitoring is, or might be, legally unacceptable--monitoring some aspect of workers' private thoughts, attitudes, veracity, emotions, level of concentration, self-esteem, self-confidence--and on what basis would/might such monitoring be unacceptable? What criteria might be used to determine the acceptability or unacceptability of monitoring of any given type of information?

Methods. Explore the methods of monitoring personal information that are, or might be, unacceptable to society--level of detail, continuousness, covertness, recordkeeping capabilities. Existing common law protections of individual privacy safeguard against unreasonable search of one's "person" (briefcases, clothing, purses, others, except in certain limited situations--might these or other laws form the basis for prohibiting methods of monitoring deemed excessively intrusive?

Principles for judgment. What analogies and principles might be useful for society to judge the acceptability of various types and methods of monitoring? Explore the possibility that the level of intrusiveness of specific types of monitoring may well be a relevant factor for the courts in determining whether a worker's privacy is being unreasonably violated. What forms of future challenges are likely to confront the courts because of the increasing capabilities for automated monitoring and recordkeeping brought about by technology?

Practices in Monitoring Office Workers. What are current practices in monitoring office workers in their use of information technology systems? Are there significant trends toward increasingly intrusive monitoring?

Factors Influencing Change. What factors or trends are discernible that are likely to change worker monitoring practices?

Institutional Influences. What is the balance of influence between government, employers, and labor unions in determining the degree of monitoring that is acceptable, and what trends, if any, are occurring in the balance that may warrant changes in Federal and State policies?

Government Whistleblowers. What underlies the public policy that protects government whistleblowers from punishment?

TASK 2

The contractor will examine the roles of legislation, regulation, labor unions, custom and other factors, in about six (the actual number and selection of to be determined through consultation with the Project Director) foreign countries and portray the essential similarities and contrasts between those countries and the U.S. concerning office worker monitoring practices and constraints. The portrayal will describe the mechanisms for determining the acceptability of specific monitoring practices, the workers' privacy rights, methods of settling employee greivances (over monitoring), and other relevant factors. While the focus of this study is on monitoring employees' activities using information technology resources, it is anticipated that a broader setting may be needed to fully characterize foreign views toward workers' rights. The criteria for selecting the countries and the selection of specific countries are to developed with the approval of the Project Director. Representative case examples will be developed to illustrate foreign activities.

Delivery Schedule:

Submission of detailed plan.	2 weeks after contract approval
Progress Report/Meeting with OTA staff	January 31, 1986
Draft of report (except for synthesis	February 26, 1986
Draft of synthesis/policy section	March 10, 1986
Final Report	March 30, 1986

Final Report: The final report is to be of professional quality, about 60-100 pages in length exclusive of appendices. Voluminous data are to be compiled into tables, charts, or graphs. The main findings of the report are to be summarized in an executive summary of about 10 pages in length. The report will have separate sections for each foreign country, and a section devoted, to comparisons of the countries.

Coordination with Concurrent Project Studies: The contractor is required to stay abreast of related, concurrent studies being undertaken by this project, and to coordinate with them. The Project Director will provide a list of current studies to the contractor. The contractor will make use of material from the study Privacy Issues in the Monitoring of Employee Work on VDTs in the Office Environment: Practices, Interests, and Policy Choices, December, 1984, performed under contract to OTA by The Educational Fund for Individual Rights.

Other: US and foreign sources of significant data are to be referenced. English language summaries of foreign policies will be included in the final report.

New Communication Technologies: Implications for Privacy & Security

Statement of Work

Belcore Statement of Work

General:

In support of OTA's study, "New Communication Technologies: Implications for Privacy and Security", the contractor shall provide all of the necessary personnel, equipment and supplies to perform the two tasks described herein. Task 1 involves the preparation of a report on communications and computer security trends and the monitoring of workers' activities using telecommunications and computers. This constitutes 70% of the work effort. Task 2 consists of briefings with OTA on report-related topics, comprising 30% of the work effort.

Task 1 itself has two parts, one related to telecommunications (Part A), and one related to computers (Part B). The general purpose of Part A is to develop a useful scheme for characterizing the nation's telecommunications networks and communications-linked computer systems, the possible abuses that they are vulnerable to, how these systems and potential abuses may be changing over time due to advances in technology and the introduction of safeguards. The general purpose of Part B is to develop a similar characterization for abuses of computers, especially those linked by communications.

For more details see the portions of the assessment proposal (provided separately) related to information systems vulnerability and security, and to monitoring of office worker activity over communications and computer systems.

Specific Task Description:

The contractor shall develop a report providing a clear technical portrayal of the trends in the areas described below, and shall provide consulting services related to these and to the project as a whole:

Task 1: The contractor shall prepare a report which addresses the following:

Part A

Identify and describe an approximate, but credible quantification of the ease (or difficulty) of carrying out various types of abuses, and to understand how these are changing over time. A number of questions are posed at the end on Part A to illustrate the types of insights that are sought through this contract.

Provide a characterization of the various forms and levels of vulnerability to abuse, and the safeguards now available and evolving, to protect against those abuses in telecommunications networks and in communications-linked computer systems, and in personal computer systems (hereafter referred to as information technology systems).[1] As part of this effort, a model of the network(s) shall be developed to facilitate a portrayal of the proportion of total (voice, data, video, graphics) traffic that traverses each network segment of concern, e.g., dedicated private lines, satellite communication systems, microwave radio, cellular mobile radio, packet switched networks, local area networks, electronic mail, and fiber optic transmission systems, and AT&T's CCIS system, and others, as appropriate.

Develop a model for communications-linked computer systems representing current and future configurations to facilitate portrayal of traffic flows and an evaluation of vulnerabilities.The characterization shall include an assessment of the relative vulnerability of different types of signals in various parts of the network(s), an indication of the approximate cost, types of equipment, time, and the technical sophistication required to carry out the particular abuse. This also will include addressal of the probability of success and the risk of the abuse being discovered, where applicable. The same assessment is to be undertaken for three periods of time using the same models and sets of assumptions. The time periods (to be agreed upon by the contractor and the Project Director), as an example, may be 1975, 1984, and 1990, however the future date will be chosen to represent an ISDN environment and to account for the expected greater use of fiber optic systems, and to inject selected computer safeguards that are now in the R&D stage.

[1] These terms, as used here mean the following:
-Forms of abuse: the different methods of accessing telecommunications signals, such as interception of over-the-air radio signals, the reception of electronic emanations from electronic equipment, and of gaining unauthorized access to personal and mainframe computer data bases and programs.
-Levels of vulnerability: the relative ease of abuse of some types of telecommunications signals, such as those transmitted over dedicated private lines or cordless telephone systems compared to other types, e.g., signals transmitted over fiber optic or coaxial cable transmission paths, or transmitted using spread spectrum coding techniques, or those carried by AT&T's Common Channel Interoffice Signalling system.
-Safeguards: protections against abuse, or unauthorized monitoring or access that (a)are inherent in the design of the system, such as in fiber optic systems, or (b)are add-ons intended to enhance the security of signals or the data bases, such as encryption and modems with automatic call-back features.

Among the types of questions to be addressed are; whether technological advances and other factors--the divestiture of AT&T, and Government deregulation of the telecommunications services industry and related actions--have collectively tended to improve or exacerbate the vulnerability of telecommunications systems to such abuse and to what degree?; what is the relative ease or difficulty (work factor) of intercepting or monitoring telecommunications covertly, and how can the work factor best be characterized?; and how are these changing over time?; are there now, or will there soon be, available adequate safeguards against abuses from all except the most sophisticated, well-financed, and determined adversaries?

Part B

Provide a thorough description of the capabilities available now, and becoming available through ongoing R&D, for monitoring employees' use of Federal agencies' (and private business') information technology systems,[2] and for detecting unauthorized use of these systems. In particular, this applies to capabilities that not only enable monitoring of employees' activities but also may intrude on individual privacy.

Among the types of questions to be addressed are: what are these capabilities today, and--considering new product developments and directions of R&D, such as digital telephones, digital PABX's, word recognition, speaker identification, and positive user identification generally--what new or improved automated monitoring capabilities are likely to be available within the next decade? What are ways in which evolving technology might be used to mitigate these intrusion capabilities? Of particular interest is the capability for monitoring personal, or otherwise unauthorized use of information technology systems, such as by employees, hackers, criminal elements and others (to be agreed upon). Examples of the effects of misuses of information technology systems range from excessive telephone bills to theft of service, embezzlement, and to violations of personal privacy rights.

Task 2: The contractor shall provide written/oral comments related to the above including, but not be limited to, meeting with Project staff, providing related tutorials, providing alternate approaches for accomplishing the above work, and identification of the state of R&D in particular fields.

[2] A type of employee monitoring of interest is exemplified by the detailed summaries of telephone use as is now becoming widely available in modern Private Automatic Branch Exchanges equipped with Station Measurement Detailed Reporting features, and in logon/logoff and audit programs used in computer systems.

The contractors will prepare a sociological paper discussing topics related to understanding the uses of information technologies to monitor activities in the work place. Several of the major questions which OTA is exploring in the privacy and security project are:

a) What are American perceptions regarding the monitoring and privacy of Government workers in the work place (particularly office work) and how might these be changing? What factors (including the growing use of information technology such as microcomputers, mainframes, and telephones) are influencing attitudes, perceptions and behavior in this area?

b) what issues with respect to privacy are raised by worker monitoring? How are current developments and changes likely to affect the functioning of democracy and the kind of society we have?

c) how are the topics of privacy and security linked in the use of information technologies? How are privacy considerations brought into information security considerations?

To assist OTA in answering these questions, we propose to pay particular attention to the following tasks :

Task 1: Specification of concepts that help to define and clarify privacy and related issues. This task will be an examination and classification of the nature and types of privacy and related issues independent of technology or the workplace as such. For this task as well as for task 2, a review and analysis will be made of earlier classification and typology schemes such as those of Ware, Westin, Fried, Greenawalt, and the Privacy Commission. Sensitizing questions will be raised for analysis, including but not limited to the following examples. How does our society define privacy and why is it important? How might privacy in the workplace differ from that in other contexts such as the home, a public area or professional relationships? The concepts developed here will be applied to a variety of contexts and technologies.

Task 2: Specification of concepts for comparing and contrasting types of monitoring. This task will help to classify forms of monitoring used in the work place. Using several of the sources listed under task 1 as well as literature listed in the following tasks, we propose to examine a series of sensitizing questions, including but not limited to the following. What are some of the major forms of monitoring in the workplace? How do these differ with respect to efficacy, validity and reliability, intrusiveness, managerial discretion and unintended consequences? What are some of the major sources of variation in the application of monitoring techniques (e.g. informed consent, visibility of monitoring, ways that the results of monitoring may be used)? What are the different goals that monitoring has (e.g.

to protect the worker vs. to protect company property)? To what extent do the goals of managers and employees overlap or conflict here? Concepts developed in tasks 1 and 2 will be applied to materials developed in other project tasks.

Task 3: Review of attitudes toward worker monitoring. This task will be quite limited in scope, involving brief reviews of survey literature and selected interviews. The emphasis in this task will be on monitoring of workers, particularly Government employees, use of telephones, microcomputers, and mainframes. From a brief review of general issues of privacy found in **Public Opinion Quartery, Public Opinion Magazine,** the Roper Center, work done by Dutton and Meadow for OTA's GIT project, and related sources, the contractors will attempt to place worker monitoring within a larger context of attitudes toward privacy and work. Additionally, to the extent that data are available from brief telephone interviews and other methods of data collection with selected stakeholders, the contractors will ascertain ways in which employees, managers, consumers, clients and civil libertarians may have conflicts around basic privacy values, differing in their views of appropriate and inappropriate monitoring. A central question which will be posed is whether the attitudes of Americans are changing as new practices become possible, such as the monitoring of telephone and computer usage and electronically tracking the movement of individuals? How do attitudes today compare to those of a decade ago as reflected in the report of the Privacy Commission?

Task 4: Review of the impact and some correlates of monitoring. This task will be one of the major emphases of the project. What is known about how work performance is affected by monitoring? How do workers respond to the monitoring made possible by new information and related technologies (e.g. attitudes and behavior with respect to the job, feelings of trust and alienation)? When monitoring is seen to be unfair or inappropriate, how do people resist, limit, or otherwise seek redress (including the use of whistleblower protections such as exist for Federal workers)? Both informal reactions (including sabotage and "gaming") and more structured and organizational means of redress for limiting or managing information collection through monitoring will be considered. How has monitoring affected the behavior of managers? How are monitoring decisions undertaken and what are the privacy considerations or understanding of the decision makers? Is monitoring seen to be effective in deterring or preventing unwanted behavior or in increasing productivity? What is its impact on middle managers? What social, cultural, technical and policy factors affect monitoring? Among relevant factors are labor unions, laws, cultural values, and formal procedures. What activities can be prevented by technology, ("target hardening or perpetrator weakening") rather than discouraged through monitoring? Literature to be reviewed for this task includes Zuboff, R. Howard, R. Coser, McEwan, G. Marx, Mirsepassi and Siegenthaler, and the **Scientific American** special issue of September 1982.

Task 5: Explore the relationship between privacy and

Space corrected on final Copy

information security. This task will also be one of the major emphasis of the project. This task will include an analysis of how concepts of privacy and security may be contradictory or mutually supportive, differences in the types of devices /mechanisms/and protections for security and privacy (within leaky as well as in boxed in systems), ways that privacy could become more a part of security considerations, obstacles to such a process, and why there may not be more privacy as technology evolves and information security develops. Questions will be raised concerning who owns information, for whom and toward what ends are security and privacy being developed, and whether security efforts could limit legitimate public access without necessarily limiting misuses of secrecy powers by authorized users? Information on private sector security policies and practices will be discussed as appropriate. Trends in the information security product market will be examined. Sources for this task will be Sherizen's previous work for OTA's GIT project, PCIE projects, studies of law enforcement policies which attempt to balance data security and privacy considerations, examination of the implications of the growing field of competitor intelligence strategies, and private sector initiatives. This task will also include analyses of existing federal security policy and privacy policy statements, including the ongoing work related to NSDD 145, NSDD 196 on polygraph tests for Federal employees, and the new OMB Circular No. A-130 which supersedes A-71, A-90, A-108, and A-121.

Task 6: 2 scenarios of work monitoring in the year 2005. This will involve generating ideal types or extreme cases of the role of worker monitoring in society (with an emphasis on electronic means). One of these would take monitoring to the extremes of control, intrusiveness, and the destruction of what today is understood as privacy; the second would involve the use of technology to further the privacy of workers. There will also be a discussion of what trends or developments seem most likely given what is now known, particularly if projected technological developments rather than legal considerations are major forces of social change. Consideration will be given to factors which tend to encourage or discourage the use of monitoring and to the forces likely to create or inhibit each scenario. Assumptions involved in developing the scenarios will be specified. The construction of these models will be based upon the analysis of trends, the well established sociological literature which examines issues of control (S. Cohen, D. Black, J. Gross), total institutions (Goffman) such as prisons where control is a major goal, and applicable futurological studies.

While all of the above tasks will be undertaken, the primary emphasis will be on tasks 4 and 5. The contractors will provide a broad sociological perspective. Their contribution will reflect an analysis of major social trends, conceptual clarification, specification of the interrelationships of the relevant social processes, and summaries and inferences from relevant bodies of research. The work will be integrative and synthetic but, due to the time limits imposed on the project, will not involve the systematic collection of primary data or offer specialized details concerning personnel management or labor-management agreements. The concern of this project is primarily with issues of privacy and employee rights and responsiblities and the diverse consequences of being able to gather more information about employees.

Submission of Detailed Outline & Briefing of OTA Staff	2 weeks after contract
Interim Report and Interim Briefing to OTA Staff	End of February
Draft of Main Body of Report	March 14, 1986
Draft of Executive Summary & Policy Recommendations	March 21, 1986
Final Report	March 31, 1986