EMPLOYEE MONITORING IN OTHER INDUSTRIAL DEMOCRACIES


Submitted by The Educational Fund for Individual Rights

Prepared by Russell Pipe and Alan F. Westin

FINAL VERSION, August, 1986

This document was prepared by an outside contractor as an input to an ongoing OTA assessment. It does not necessarily reflect the analytical findings of OTA, the Advisory Panel, or the Technology Assessment Board.
ACKNOWLEDGEMENTS

The authors wish to acknowledge that the Norwegian section was substantially drafted by Professor Jon Bing, Director of the Norwegian Center on Computers and Law, and the West-German study was prepared by Frank Kuitenbrouwer, a lawyer and journalist in Amsterdam. Assistance with the West-German section was given by Professor Spiros Simitis, University of Frankfurt Labor Law Center, and Dr Stefan Walz, professional staff, Office of the Hessen Data Protection Commissioner. Very helpful contributions also were provided by Oscar de Vries Reilingh, Director, Geneva Office, International Confederation of Free Trade Unions; Guy Ryder, Secretary for the Industrial Trade Section, International Federation of Commercial, Clerical, Professional and Technical Employees (FIET); John Evans, Director of the Trade Union Advisory Committee to the OECD, Paris, France; Professor Jacques Berleur, Facultés Universitaires, Notre-Dame de la Paix, Namur, Belgium; Erlik Djønn, The Data Inspectorate, Oslo, Norway; Dr Ulrich Dammann, Deputy Federal Data Protection Commissioner, Bonn, West Germany; Dr Ray V Austin, Rapporteur, Commission on Telecommunications and Information Policy, International Chamber of Commerce (ICC), London, England; Werner Vaupel, Commissioner for Data Protection, Hoechst AG, Frankfurt, West Germany; Jan Freese, Director General, Data Inspection Board, Stockholm, Sweden; Antoine Pezé, Chargé de Mission, Commission for Informatics and Liberties (CHIL), Paris, France; Dr Rainer J Schweizer, Data Protection Office, Federal Ministry of Justice, Bern, Switzerland; and Tom Riley, Riley Information Services, Toronto, Canada.
# CONTENTS

## PART I: OVERVIEW OF NATIONAL SITUATIONS IN OTHER INDUSTRIAL DEMOCRACIES

- **INTRODUCTION** ........................................... 244
- **MAJOR VARIABLES IN NATIONAL SITUATIONS** ................. 247

## PART II: EUROPEAN NATIONS: FEDERAL REPUBLIC OF GERMANY

AND NORWAY, AND BRIEFER TREATMENT OF FRANCE,
AUSTRIA, BELGIUM AND SWITZERLAND .......................... 281

**FEDERAL REPUBLIC OF GERMANY** ............................... 281

- Worker surveillance -- background .................................. 281
- Personnel Information Systems .................................... 281
- VDU Monitoring ..................................................... 281
- Co-determination of technical monitoring systems ............ 281
- Telephone monitoring .............................................. 281
- Legislative situation ............................................. 281

**NORWAY** ....................................................... 321

- Worker surveillance--pre-high technology ...................... 321
- Current surveillance situation .................................. 321
- Union of Metal Workers Initiative ............................... 321
- Telephone monitoring ............................................. 321
- Productivity monitoring ......................................... 321
- Video surveillance ............................................... 321
- Use of employee records for surveillance ....................... 321

**FRANCE** ....................................................... 317

**THE NETHERLANDS** ............................................ 322

- Video System Monitoring Production Personnel ................. 322

**AUSTRIA** ....................................................... 324

- Constitutional Ruling ............................................ 324

**BELGIUM** ....................................................... 324

**SWITZERLAND** .................................................. 324

## PART III: BRITISH AND COMMONWEALTH NATIONS: CANADA AND AUSTRALIA

**CANADA** ....................................................... 325

- Background ...................................................... 325
- Union Positions .................................................. 325
- VDTs and Work Monitoring ....................................... 325
- Electronic Surveillance .......................................... 325
- Employee Surveillance .......................................... 325
- Summary ......................................................... 325
AUSTRALIA

New Threats to Privacy ........................................ 352
Intrusive Employment Practices ............................... 353
Official Guidelines Issued ................................... 354
Typical Employee Monitoring Complaints ................. 355
Trade Union Activities ....................................... 358

PART IV: FAR EAST DEMOCRACIES: JAPAN ................. 361

JAPAN ............................................................ 362

Popular Attitudes Toward Privacy ............................. 362
Attitudes Toward Privacy Protection Measures ............. 363
Worker Monitoring in Japan .................................. 364

PART V: INTERNATIONAL TRADE UNION ACTIVITIES ....... 367

Intrusive Practices Identified ................................ 367
Risks of Monitoring Misuse High ............................ 367
Limitations on Monitoring Urged ............................. 367
Surveillance Conditioned on Agreed Practices .............. 367

PART VI: INTERGOVERNMENTAL ORGANIZATIONS: UN, ILO, AND COUNCIL OF EUROPE .......................... 367

UN COMMISSION ON HUMAN RIGHTS .......................... 393

Draft Guidelines for Personal Files ......................... 393
Final Approval in 1986 ...................................... 393

INTERNATIONAL LABOR OFFICE .............................. 395

Compendium of Principles Asked ............................ 395
Technology Threats Raised .................................. 395

COUNCIL OF EUROPE ........................................... 397

Personal Data Convention Ratified .......................... 397
Employment Sector Records Examined ....................... 397

PART VII: OBSERVATIONS ....................................... 399
PART I

OVERVIEW OF NATIONAL SITUATIONS
IN OTHER INDUSTRIAL DEMOCRACIES
INTRODUCTION

Workplace monitoring, as discussed previously in the theoretical section and U.S. materials of our report to OTA, involves a society's value system, institutional arrangements, and legal rules on at least five major social issues of current significance in advanced industrial democracies:

- The nature of work, and individual roles and responsibilities of workers;
- Employer-employee relations, and the role of trade unions;
- Investigation and control of crime at the workplace, and related security-integrity issues (e.g., drug testing);
- The definition and protection of privacy-dignity interests of employees;
- Use of advanced information technologies by private or public authorities.

We also noted that workplace monitoring issues need to be analyzed by taking into account three empirical conditions:

- the employer's declared purpose for and actual uses of monitoring;
- the type of monitoring techniques used; and
- the process by which monitoring is proposed, implemented, and administered.

In this segment of our report to OTA, we explore how other advanced industrial democracies and some multi-national or international agencies are approaching workplace monitoring. Our goal is to collect experiences and social responses; examine legal/regulatory actions where these have taken place or are now being proposed; and to identify social or legal concepts in other societies of potential value for U.S. choices on workplace-monitoring issues.
MAJOR VARIABLES IN NATIONAL SITUATIONS

In examining how other advanced industrial democracies have treated workplace monitoring, we will be concentrating our reports on the OECD nations. While each country has its unique national institutions and processes, several groupings of political/legal cultures are present:

- the British-Commonwealth nations (Britain, Ireland, Canada, Australia, New Zealand), sharing the English common-law legal tradition;

- Northern-European nations with a strong Napoleonic-legal-code and "administrative-state" tradition (France, West Germany, Austria, Switzerland, Netherlands, Belgium);

- the Nordic countries, with a blend of continental legal tradition and Scandinaviant social-welfare institutions (Norway, Sweden, Denmark, Finland);

- the Southern-European nations (Italy, Spain, Portugal), with Latin adaptations of Northern-European legal-political cultures;

- and Far Eastern industrial democracies (with Japan as the principal OECD member).

Among these nations, there are at least three major variables in their national legal-political cultures that directly shape positions on workplace monitoring:

1. the industrial relations system;

2. legal/regulatory treatment of work and workplaces; and

3. attitudes toward technology and privacy protection, and laws evolved in response to new information technology uses;

Each of these merits a brief description.
1. Industrial Relations Systems
   a. Institutional Patterns

   In general, there are two main types of employee representation systems in other advanced industrial democracies (and some countries have both types in operation simultaneously):

   • The union-representation system, the most similar to the U.S., is a voluntaristic system based on labor-management negotiated agreements. Employees have freedom to associate (or not); unions have rights to organize; union members elect representatives; and the union negotiates with management a detailed agreement as to terms and conditions of work. In the event of impasse, the union relies on the right to strike and management on the right to lock out workers who refuse management terms. Voluntary mediation systems and labor courts are used in some countries to resolve contract disputes. Nations with this system such as Britain, Ireland, and Greece, vary in whether there is one national union for all workers in each major industry (auto manufacture, electronics, etc.) as in Sweden and West Germany, or whether several unions, often as many as three to five, share jurisdiction for different groups of workers (usually by skill or trade) within that industry, as in Britain. There can be industry-wide collective agreements (as when the entire steel industry and the steel union sign a contract), or there can be enterprise (one company) agreements. There are also national confederations of trade unions as well, along general lines such as industrial work, white collar work, etc. The union representation system creates a strong shop-steward and local-union presence within individual plants, and
important contract terms are often asserted and negotiated at that level. In Japan, unions are organized primarily along company lines: one union for Toyota, Sony, Hitachi, etc.; these "company" unions also belong to one of two main national confederations of Japanese trade unions. The union-representation system is often called a "power-struggle" process, in which bi-polar positions are asserted and economic/political strength determines the outcome; in this process, attitudes of the political parties and the government in power can play a key role, as can public sympathy -- or lack of sympathy -- toward the position of unions or management.

- The other main industrial relations mechanism is the employee-representation **works council** system. This is created by national legislation that provides for election by all workers at a location of employee representatives to serve on a works council for a plant or facility, composed of representatives of both employees and management; the legislation spells out a set of rights and procedures for this consultative system. Nations such as West Germany, Sweden, Belgium, and the Netherlands have legislated work councils, which operate alongside and are legally independent of the union representation systems in those countries. (In addition, West German co-determination legislation requires 50% representation for employees on the Boards of Directors of stockholder-based companies with more than 2,000 employees. Smaller companies are required to give employees one-third representation on their Boards.) The works councils are to consider all decisions affecting work and workers. There is an obligation on management to discuss and cooperate with employee representatives, and when they can agree, this produces work council decisions
that will be implemented. Traditionally, works councils deal with health and safety, job environment, hiring and firing, wages and hours, work rules, etc. They can also take up election of company officers, investments, staffing plans, and social policies. In the past decade, new technology introduction and its effects have been a major topic of discussion among works councils. When management and employee representatives disagree over whether something should be done, or how, or whether a prior decision is being properly implemented, the issue goes to labor courts for decision. (In West Germany, there is a hierarchy of local, regional, and federal labor courts.) Generally, these courts still recognize a substantial area of management rights, and will allow, for example, very broad latitude to managements in the decisions about designing or adopting new technology, or doing work measurements and performance evaluation. The work-council system is often called a "power-sharing" system.

b. Trade Union Patterns

The percentages of workers who belong to or are represented by unions varies considerably from country to country. The degree of unionization obviously has an effect on how strongly unions can assert demands and campaign effectively to win these, either in labor contracts or in legal/regulatory actions. Analyses of levels of union representation in the early 1980's generally divided industrial democracies into three groups: low, medium, and high unionization.*

---

"Low" levels (23-40%)

United States ............. 22%
France ................... 23
Japan ..................... 30
Canada .................... 35
Switzerland .............. 35
West Germany ............ 40
Netherlands .............. 40

"Medium" levels (50-60%)

Italy .................... 50%
Ireland ................... 50
Britain ................... 52
Austria ................... 60

"High" levels (65-90%)

Belgium ................... 65%
Norway .................... 65
Denmark ................... 70
Finland ................... 85
Sweden .................... 90

Traditionally, union representation tended to be much higher in the industrial sectors than in office and white collar work. However, the expansion of government office work and a surge of white collar union organizing in OECD nations in the 1960's and 70's has brought office-work representation up substantially.

In terms of their general attitudes toward technological change, most European unions were "cautiously optimistic" in the 1950's and 1960's, because of rising employment opportunities and levels, generally good pay and benefits, and the presence of expanding governmental programs to cushion specific problems and provide social-safety-nets. The introduction of microelectronics in the factory and office in the 1970's, accompanied as it was by rising unemployment, fears of permanent job losses, and concern over loss of union/worker influence in the work process, and with world-wide recession and oil-crises as the background, led many European unions to become worried and pessimistic about the
way employers were installing new information technology. One study by a
Swedish trade union expert classified the dominant attitude of unions in
European nations in the early 1980's toward new information technology as
follows:

"Positive" -- West Germany, Italy, Austria, Netherlands, Nordic
countries;

"Negative" -- France;

"Unclear" -- Britain, Switzerland, Ireland

One important facet of recent trade union activity is the negotiation
of Technology Agreements, especially for factory and office automation.
In Britain, for example, a study of union-management Technology Agreements
(primarily signed between 1979 and 1981) found the most frequent subject
to be the design, installation, and operation of Video Display Units. Of 105
agreements examined, 66 had no mention of "machine monitoring" of VDU workers;
22 banned such a practice (though 3 of these contained "ambiguously worded"
clauses); 9 had a "commitment to discuss" by the parties; and 8 accepted
machine monitoring "subject to safeguards."

* Asplund, op. cit., p. 221.

** Williams, Robin and Moseley, Russell, "Technology Agreements: Consensus,
Control, and Technical Change in the Workplace (1)," in Bjorn-Andersen
et al., op. cit., pp. 240-241.
2. Legal/Regulatory Treatment of Work and Workplaces

While many laws and regulations governing work in OECD nations parallel those in the United States (occupational health and safety laws; payroll contribution for health and accident insurance, and old-age pensions, etc.), there are some important differences that can relate to worker monitoring issues. Many European countries promulgate legal standards or set "official guidelines" for work processes or conditions, covering either all workplaces or all workers using a particular machine or process. In the U.S., many of these matters have been left to union-management bargaining (in union-represented establishments) or to employer discretion, especially in private industry. Nations such as West Germany have been particularly active in promulgating ergonomics standards for VDTs, while Sweden and Norway have enacted broad Work Environment laws that oblige employers to pursue healthy, humane, and dignified work settings.

Another major difference is that other industrial democracies have unjust dismissal laws, under which individual workers who are discharged can go before industrial courts or commissions and challenge their terminations. If the employer shows good cause or business justification, the employee loses, but if the employee shows that arbitrary, unfair, or unjustified dismissal took place, the court or commission can award the employee compensatory relief. Potentially, a worker who wanted to challenge a termination on the basis of unfair or incorrect machine monitoring of performance could raise such an issue in an unjust dismissal action. The tribunal would look to see whether the employer's action was within management's powers and was fairly applied, or not.
3. Attitudes Toward Technology and Privacy Protection

A useful snapshot of similarities and variations among OECD nations was provided by an eight-nation public opinion survey conducted in 1985 by Louis Harris International and the Atlantic Institute for International Affairs.* The eight nations were: France, West Germany, Britain, Italy, Norway, Spain, United States, and Japan. As can be seen, these eight nations cover the major types of national legal/political systems among advanced industrial democracies. In all, 9,000 interviews of persons of eligible voting age were conducted, with sufficient numbers in each country to provide representative sampling to the national populations. Similar polls were conducted by the Atlantic Institute going back to 1982.

While the survey reported on many important topics (rising concern over unemployment as a result of technological change, willingness to undergo retraining, degree individuals have already used computers, etc.), we will focus on several responses related to national attitudes on information-technology use, work, and invasion of privacy issues.

---

One question asked whether the use of information-processing systems will cut down on "more tedious tasks" in the workplace. The responses were:

<table>
<thead>
<tr>
<th></th>
<th>FRANCE</th>
<th>GERMANY</th>
<th>BRITAIN</th>
<th>ITALY</th>
<th>NORWAY</th>
<th>SPAIN</th>
<th>USA</th>
<th>JAPAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mostly agree</td>
<td>65</td>
<td>38</td>
<td>79</td>
<td>63</td>
<td>74</td>
<td>75</td>
<td>77</td>
<td>39</td>
</tr>
<tr>
<td>Mostly disagree</td>
<td>23</td>
<td>25</td>
<td>12</td>
<td>27</td>
<td>18</td>
<td>21</td>
<td>19</td>
<td>26</td>
</tr>
<tr>
<td>No answer/ No opinion</td>
<td>12</td>
<td>37</td>
<td>9</td>
<td>10</td>
<td>7</td>
<td>4</td>
<td>4</td>
<td>35</td>
</tr>
</tbody>
</table>

As this indicates, the publics in Britain, the U.S., Spain and Norway approved this view by over 70%, while only 38% of West Germans and 39% of Japanese shared that view. (In the case of Japan, an unusually high 35% had no opinion or did not answer that question.)

A second relevant question asked which groups were among the most important "obstacles" to the "development of new technologies" in their country. The responses as to employers, labor unions, and political leaders were:

<table>
<thead>
<tr>
<th></th>
<th>FRANCE</th>
<th>GERMANY</th>
<th>BRITAIN</th>
<th>ITALY</th>
<th>NORWAY</th>
<th>SPAIN</th>
<th>USA</th>
<th>JAPAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our political leaders</td>
<td>14</td>
<td>20</td>
<td>21</td>
<td>37</td>
<td>12</td>
<td>12</td>
<td>35</td>
<td>16</td>
</tr>
<tr>
<td>Labor unions</td>
<td>21</td>
<td>14</td>
<td>43</td>
<td>21</td>
<td>6</td>
<td>6</td>
<td>25</td>
<td>14</td>
</tr>
<tr>
<td>Employers</td>
<td>8</td>
<td>8</td>
<td>9</td>
<td>9</td>
<td>3</td>
<td>12</td>
<td>25</td>
<td>7</td>
</tr>
<tr>
<td>No opinion/ not sure</td>
<td>18</td>
<td>38</td>
<td>10</td>
<td>25</td>
<td>39</td>
<td>27</td>
<td>4</td>
<td>40</td>
</tr>
</tbody>
</table>
It is interesting that, in the U.S. sample, employers and unions were cited as "obstacles" by an equal number of respondents (25%) while U.S. political leaders were seen as "obstacles" by a significantly higher percentage (35%). Also worth noting is the result that in Britain, 43% of the British respondents cited labor unions as an obstacle, the highest number for any country surveyed. This probably reflects the highly-publicized positions taken by trade unions in industries such as newspaper printing and coal mining.

A final question relevant for our topic asked whether respondents believed it will be increasingly possible to use computer data banks to infringe personal privacy. The responses were:

<table>
<thead>
<tr>
<th></th>
<th>FRANCE</th>
<th>GERMANY</th>
<th>BRITAIN</th>
<th>ITALY</th>
<th>NORWAY</th>
<th>SPAIN</th>
<th>USA</th>
<th>JAPAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mostly agree</td>
<td>71</td>
<td>51</td>
<td>75</td>
<td>37</td>
<td>56</td>
<td>69</td>
<td>68</td>
<td>50</td>
</tr>
<tr>
<td>Mostly disagree</td>
<td>19</td>
<td>20</td>
<td>13</td>
<td>35</td>
<td>35</td>
<td>24</td>
<td>28</td>
<td>18</td>
</tr>
<tr>
<td>No answer/</td>
<td>10</td>
<td>29</td>
<td>12</td>
<td>12</td>
<td>9</td>
<td>7</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>no opinion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Presented in rank order, this shows the following country levels of concern about privacy invasion by computers:

- Britain ................. 75%
- France ................... 71
- Spain ..................... 69
- U.S. ....................... 68
- Norway .................... 56
- West Germany ............ 51
- Japan ..................... 50
- Italy ....................... 37

The 68% figure for the U.S., incidentally, is close to the levels of U.S. survey data obtained in polls from 1979 to 1984, which have found 64-77% of respondents expressing such concern.

Applicability to Data Privacy Laws

In the early 1970s considerable public and press concern in Europe was aroused over the potential invasion of privacy by extensive computerization of personal records. Many of the same issues that led to enactment of the Privacy Act of 1974—intrusive population census questions; forecasting of vast national data banks; and new, invidious powers of control over the citizenry made possible by manipulation of computer data—prompted European governments to prepare personal data protection legislation. Under the parliamentary system, political issues are studied by ministers, who are themselves members of parliament, and once consensus is reached by the cabinet or Council of Ministers, this is tantamount to passage by the national legislature. Sweden began preparing its Data Act in 1971 which resulted in the first national law in 1972. By 1979 Austria, Denmark, France, Germany (FR), Luxembourg and Norway also had adopted statutes along similar lines.

The fundamental motivation of the Europeans has been to ensure that personal privacy was not eroded as a result of data processing applications. Unlike the United States, however, defining what constitutes "undue encroachment on a data subject" (from the Swedish Act), and arriving at remedies or penalties against improper use of personal information is not left to the individual. Rather, an administrative structure or regime was considered necessary, based on certain prescribed personal information handling practices backed up by an independent government agency with supervisory and enforcement powers. Thus the term for "computer privacy" in Europe is "data protection".
In Europe, government historically has had a far greater role in citizens' lives, one consequence being far more personal information is collected by the various bureaucracies from municipal to central government authorities than is the case in the US. This is well-accepted tradition. Data protection legislation was not prompted as a reaction to the excessive collection of personal information by government agencies; it was the introduction of data processing arousing fears that millions of manual records suddenly would be automated, capable of unlimited and unrestricted linkage, reuse and dissemination. Most European governments have or will impose data protection norms on users (responsible keepers) of personal records. In the US, similar normative rules are often referred to as fair personal information practices.

Continental law is usually far more general and all-encompassing than Anglo-American practice of narrow target legislation. This is the case with data protection. Personal information is defined very broadly, essentially any detail that can be linked or identified with a particular individual. Similarly, they cover any process or activity in which data processing is involved. The only real delimitation in some laws, such as in Germany and Norway, requires that personal data collected must be name-retrievable. Architects of European data protection designed the legislation around the notion of static databases (data banks) which could be identified, registered, inspected and, as necessary, erased.

The convergence of data processing and telecommunications renders obsolete the well-ordered concept embodied in these laws. Nevertheless, even the 1984 Data Protection Act of the United Kingdom is founded on registering formal systems of records and describing their main characteristics. The advent of word processing and new telematic services such as electronic mail and EFT are almost impossible for data protection authorities to deal with. Automated, name-linked data are present in these applications, which brings them within the scope of the data protection law, but a formal database may not exist.

Although the word monitor does not appear in any European data protection law, their objectives are certainly to regulate computer-assisted monitoring, defined by Webster as "to watch or check on a person or thing." The principal focus of attention by data protection authorities (DPAs) from 1973 to the present has been to establish national registers of databases containing personal data and prescribe compliance with statutory requirements. DPAs are trying to prevent the build-up of "profiles" or computer "dossiers" on individuals. Such activities are referred to as preventing the monitoring of people, inasmuch as monitoring is seen as the collection and/or linkage of numerous details about individuals into a master record. In this sense DPAs have been involved in employee monitoring matters for some years.
Work monitoring, such as computer-usage monitoring, telephone-call accounting and work measurement, are subject to data protection regulation if data collected can be related to specific employees and data processing is involved in the collection, storage or use of such information. DPA officials have expressed both increased interest and frustration over their inability to regulate applications of what are referred to as "new information technologies". The advent of personal computers and proliferation of terminals make the notion of registering static systems of personal records increasingly obsolete. Either through adaptation of existing data protection law or enactment of "second-generation" legislation, European DPA leaders insist they will become more involved in new forms of potential intrusion on personal information privacy.

It is because DPAs have been preoccupied with their first-line obligations of bringing large government and business personal information collections into compliance with data protection acts that work monitoring has not received significant attention. Trade unions and labor law are the focal point of such monitoring and are likely to continue to be for some time in the future. There appear to be no jurisdictional problems for DPAs to become involved with work monitoring problems along with trade unions, works councils and labor courts. It may be the failure of trade unions to seek DPA assistance that has not accelerated the use of data protection laws in allegedly improper monitoring practices.
Main Provisions of Foreign Personal Data Protection Legislation Relevant to Coverage of Employee Monitoring

<table>
<thead>
<tr>
<th>Provisions</th>
<th>Austria</th>
<th>Canada</th>
<th>Public</th>
<th>Denmark</th>
<th>Private</th>
<th>Denmark</th>
<th>France</th>
<th>Germany FR</th>
<th>Iceland</th>
<th>Israel</th>
<th>Luxembourg</th>
<th>Norway</th>
<th>Sweden</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope of application:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central government</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Provinces/states</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Private sector</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Covers all information traceable to identifiable individuals</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Information collected and/or processed using computers</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Limits placed on personal data collection</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Personal information must be collected for specified, legitimate purposes</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Individuals have right of access to inspect personal information</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Sensitive personal details specified (collection only with data subject's knowledge and consent)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Y = Yes
N = No

1 Covers information concerning private affairs, such as financial situation of individuals.

2 Covers information on an individual's personal status, intimate affairs, economic position and vocational qualifications.

3 Collection of personal data limited unless it is "natural part of the normal operations of an enterprise."

4 Personal information collection is permissible if it serves the purpose of a contractual relationship or there is a legitimate interest in (a business) storing it.

5 State laws may be enacted that for personal data maintained by the public sector
Applicability of Foreign Personal Data Protection Legislation to Employee Monitoring

<table>
<thead>
<tr>
<th>Type of monitoring</th>
<th>Austria</th>
<th>Canada</th>
<th>Public Denmark</th>
<th>Private Denmark</th>
<th>France</th>
<th>Germany FR</th>
<th>Iceland</th>
<th>Israel</th>
<th>Luxembourg</th>
<th>Norway</th>
<th>Sweden</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee computer-usage monitoring (by IDs, terminals and passwords)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y^1</td>
<td>u^2</td>
<td>y^3</td>
<td>y^1</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>Telephone-call accounting</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>u</td>
<td>u</td>
<td>y^3</td>
<td>y^1</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>Work measurement</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>y^1</td>
<td>y</td>
<td>y</td>
<td>y^1</td>
<td>y</td>
<td>y</td>
<td>y</td>
</tr>
</tbody>
</table>

Y = Yes  
U = Uncertain

1 Personal data covered by this law must be organized or filed so as to be retrievable automatically using identifiers that can be linked to a particular person.

2 Information must be related to a person's private affairs, such as financial situation.

3 An official translation (Chapter I, para 2) states that it is an infringement of privacy to:
   a) spy on or trail a person in a manner likely to harass him, or any other harassment; and
   b) "listen in".
Data Protection Becoming World-Wide

Since 1970, national and provisional governments of 12 countries of Europe, Australia, Canada, Israel, New Zealand, and the United States, have adopted laws to provide legal protection to individuals; and in some cases legal entities, over the collection, processing, use and dissemination of their personal details. This section reviews developments in countries and in such international organizations as the Council of Europe, the OECD, and UN Commission on Human Rights. In the first TDR issue each year we provide an update and forecast of legislative developments in this field around the world. (See Table)

A commission of the Brazilian congress is preparing a personal data privacy bill; the government of Colombia intends to submit a data protection legislation soon after making inquiries with European data authorities; and Hong Kong intends to place legal rights over records concerning individuals before the British Colony reverts to the People's Republic of China in 1997. These are examples of the heretofore “computer privacy” phenomenon initiated by OECD countries and Israel that have taken root in developing, newly industrializing and also Eastern European nations.

While granting citizens power to limit the collection and use of their personal details as well as access to such records is a characteristic of democratic nations, seen as a guarantee provided by the UN Convention on Human Rights, certain Eastern European and other countries have or are considering legislation dealing with the handling of computerized personal information. Hungary has adopted a data protection law for the confidentiality and security of personal information. This statute has similarities to Western European statutes, except that access to government held personal data is not granted. The Soviet Union, in fact, adopted a law in the mid-1970s to restrict access and confidentiality of computerized electoral records.

In Western Europe several countries have data protection bills in advanced stages of preparation and their adoption may be forecast in 1986. These are Finland, the Netherlands, Spain and Portugal. Spain has ratified the Council of Europe Data Protection Convention and due to its coming into force on October 1, 1985, is expected to expedite passage of a law in 1986. Other countries have prepared draft data protection bills but because of long consultation periods or changes in government, have not adopted legislation. These include Belgium, Ireland, Italy, Switzerland and Yugoslavia. A draft bill has been under review by the Japanese prime minister's office for some time.

Status of Data Protection/Privacy Legislation - January 1986

<table>
<thead>
<tr>
<th>Country</th>
<th>National</th>
<th>Subnational</th>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>(P)</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td>Austria (Rev)</td>
<td>CL</td>
<td>P</td>
<td>R</td>
</tr>
<tr>
<td>Belgium</td>
<td>P</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Brazil</td>
<td>P</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Canada</td>
<td>L</td>
<td>L(P)</td>
<td>R</td>
</tr>
<tr>
<td>Colombia</td>
<td>L</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td>Denmark (Rev)</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Finland</td>
<td>L</td>
<td>P</td>
<td>R</td>
</tr>
<tr>
<td>France</td>
<td>L</td>
<td>P</td>
<td>R</td>
</tr>
<tr>
<td>Germany (Rev)</td>
<td>L(P)</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td>Greece</td>
<td></td>
<td></td>
<td>RP</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>L</td>
<td></td>
<td>RP</td>
</tr>
<tr>
<td>Hungary</td>
<td>L</td>
<td></td>
<td>RP</td>
</tr>
<tr>
<td>Iceland (Rev)</td>
<td>L</td>
<td></td>
<td>RP</td>
</tr>
<tr>
<td>Ireland</td>
<td>L</td>
<td></td>
<td>RP</td>
</tr>
<tr>
<td>Israel</td>
<td>L</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Italy</td>
<td>P</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Japan</td>
<td>L</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>L</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Netherlands</td>
<td>CP</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>New Zealand</td>
<td>L</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Norway (Rev)</td>
<td>L</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Portugal</td>
<td>CP</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Spain</td>
<td>CP</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Sweden</td>
<td>L</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Switzerland</td>
<td>(P)</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td>Turkey</td>
<td>L</td>
<td></td>
<td>RP</td>
</tr>
<tr>
<td>UK</td>
<td>L</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>US</td>
<td>LP</td>
<td>L</td>
<td>R</td>
</tr>
<tr>
<td>Yugoslavia</td>
<td></td>
<td></td>
<td>RP</td>
</tr>
</tbody>
</table>

Code:
- L Law Adopted
- R Government report/bill prepared
- C Constitutional provision
- P Parliament (Congress) Consideration
- (P) Draft legislation prepared
- RP Government report in preparation
- Rev Law being revised

Source: Transnational Data Report
PART II

EUROPEAN NATIONS: FEDERAL REPUBLIC OF GERMANY
AND NORWAY, AND BRIEFER TREATMENT OF FRANCE,
AUSTRIA, BELGIUM AND SWITZERLAND
Labor relations in the Federal Republic of Germany (FRG) have a strong legal component, as is typical for German society as a whole. There is even a complete separate branch of the judiciary for labor law. It is characterized by the participation of appointees of workers' and employers' organizations on the bench in lower courts; the Federal Supreme Labor Court (Bundesarbeitsgericht, or BAG) has a majority of professional judges. This court system deals with:

1 individual workers' rights (wage matters being by far the majority of cases);

2 problems arising from collective bargaining agreements (occasionally involving settlement of strikes);

3 the Works Council system.

The Works Council is the focus of a statutory system of employee participation in decision making at the company level. In public administration there is a Personnel Council with a somewhat comparable position. Participation does not always mean full decision sharing but covers a range from being informed to consultation and co-determination, the precise scope of which has been subject to frequent litigation. One of the matters within this kind of litigation has been electronic monitoring of employees. In co-determination the Works Council may conclude a formal agreement with the employer. If no agreement is reached the matter may be referred to an Arbitration Commission for disposition.

The FRG traditionally has strong and cooperative labor-management relations. Union influence in day-to-day matters is said to be considerable, but the trade unions share in the difficulties of Western Europe as a whole in these times of rapid technological change, mass unemployment, and not always favorable political environment. Still, social peace in West Germany is a strongly felt value and days lost from strikes are said to be among the lowest in Western Europe. Tensions have risen recently, however, because of government plans to change strike laws. A majority of the trade unions is federated in the Deutsche Gewerkschafts Bund (DGB) with a total of 7.8 million members. The single most important union is the steelworkers' union IG Metall with 2.5 million members, proudly called "the biggest in the free world". Union membership in this sector traditionally is very high, up to 70 percent. Average union membership in 1980
stood at 42.6 percent of the work force but has dropped to about a third. Outside DGB, a union of higher-qualified employees, Deutsche Angestalten Gewerkschaft (DAG), has only half a million members but enjoys a growing influence as DGB is losing some of its appeal, especially to young people.

Worker surveillance—background

Established forms of worker surveillance include time clocks, punchcard systems, multi-movement cameras, so-called produktographs, and telephone monitoring. The use of polygraph tests in labor relations is frowned upon in the FRG, as it is in the rest of Western Europe, but handwriting analysis, graphological testing of people applying for a job is practised and has been accepted by the BAG (provided the person concerned has consented).

The standard questionnaire for job applicants in private industry must be approved by the Works Council, as must standard practices and tests in job interviews. Psychological testing of job candidates is not uncommon; the BAG since 1964 requires that it not be done without good reasons (such as special responsibilities that go with a job). The right of employers to inquire about the health of prospective employees has been tied by BAG (June 7, 1984, DB 1984, p 2706) to the extent and legitimacy of their interest, considering the particular labor relationship at stake. Many companies have their own medical departments that advise management in health aspects of working conditions and also may counsel individual workers at their request.

Employers are allowed to ask job seekers about their criminal history and may require them to produce an official statement from the central criminal records office. It has repeatedly been held, however, that questions of this kind have to be strictly related to the nature of the job (sexual offences in the case of a teacher, road-safety violations in the case of a truck driver) and may not become a "fishing expedition". The legal basis of management collecting data on employees usually has been sought in the general framework of the labor contract, such as the doctrine of subordination (the duty of employees to accept leadership of superiors) and the right of a prospective employer to ask questions. The Federal Data Protection Act of 1977 (Bundesdatenschutzgesetz, or FDPA) does not cover the collection of personal data and centers on storage, communication, modification and erasure of personal data. The BAG has consistently held, however, that the
right of an employer to ask questions is restricted by the general constitutional right of protection of the personality (paras 1(1) and 2(1) of the Federal Constitution. This guarantees every German the right to human dignity. Accordingly, only those questions are permissible that relate to the workplace or the nature of the job.

What might be called the purpose principle also is an element of the FDPA, which moreover requires a broadly worded "legitimate interest" on the part of the employer in order to automatically process personal information. It has been argued that the landmark decision of the Federal Constitutional Court in the 1983 census case, proclaiming a fundamental "right of informational self-determination," makes it necessary for the government to provide more specific and statutory grounds for intrusion on the privacy of workers by their employers.¹

Certain types of monitoring, of course, are prescribed by law: truck drivers are required to have a kind of "black box" in their cabs for purposes of road safety. The FDPA requires the establishment of access controls at computer centers. It remains an unsettled legal issue as to whether these kinds of data may be used by employers for their own purposes.

**Personnel Information Systems (PIS)**

Increasing use of automated data processing in personnel management has provoked growing labor concerns. The focus so far has been mainly the most widely used software package called Personnel Accounting and Information System (PAISY). It has been used by big employers such as the Opel Motor works, the German federal bank and the Bosch and AEG industries of electronic appliances. Use reportedly is rapidly spreading to hundreds of small firms.

PAISY basically is a system for managing wages and salary records. It can be expanded into a more comprehensive personnel information system (PAISY-INFO) but direct linkage to production management or control systems is not envisaged, according to the supplier.² Nevertheless, the specter has been raised that personnel information systems will reduce the employee to a "person of glass", as ran the headline on a story in the widely read weekly Der Spiegel (1982, No 29) that has become proverbial.

The magazine told how Volkswagen reduced its work force by computing a list of
employees that were eligible for civil-defense service and turned the list over to the authorities. The military obligingly called into service quite a number of delinquent employees, easing the company's difficulties. Another firm in need of trimming its staff conducted an electronic search of its personnel files to identify employees that really were dependent upon company buses to come to work. The firm then closed down its bus service citing only reasons of economy; this obliged many women employees to resign their jobs, and the employer did not have to fire them. The story also pointed out an irony: PAISY is in use by major trade unions for their own administration, including the civil-service union OTV that has spoken out strongly against PIS. Unions also have a vested interest in effective information systems of employers, if only to be able to monitor their members' contributions, that are set at percentages of earnings. Flexibility of working conditions and work sharing—both major demands of modern unions—also call for detailed registering of workers' data, apart from the ability to identify groups of radicals and troublemakers.

Still, the German trade unions are on record strongly against PIS. After OTV had spoken out, the full DGB Congress in May 1982 registered its objections. The main concern is that the systems will be used to produce "personality profiles" of employees. Accordingly, a major strategy goal is to prevent linkages of data.

The Labor Tribunal at Oberhausen, a lower court, in 1982 handed down an award in a case brought by the Works Council of Thyssen Foundry against the company. This case is indicative of how labor courts interpret the scope of Works Council powers. The issue was one of the use of PAISY. The parties accepted the injunction to conclude an interim agreement stipulating that:

— the company would undertake to submit to the Works Council within 15 days a draft company agreement governing the introduction of PAISY;

— firm rules for inputting, storing, deleting, changing and transmitting data would be established;

— a protocol would be established for hardware control and access authorization;

— stored data would not be used for purposes other than those defined, without the agreement and prior information of the Works Council. The management also agreed to integrate appropriate monitoring systems;
any extension of the use of PAISY beyond the purposes defined in the award would be submitted to co-determination proceedings.

As a result a company agreement was concluded covering the following points:

Scope  The agreement applied to the use of the PAISY computer system for computing Thyssen works pensions.

Technical utilization  The program will be used exclusively on the dual computer of the Thyssen EDP Center.

Data  All data to be processed by PAISY will be catalogued according to defined data fields.

Use of data  Data may be used only for computing works pensions; all data output will be recorded. No other retrieval, processing or output shall be permitted. Exceptions shall require authorization by the Works Council, subject to requirements of legislation, collective or company agreements. There is to be no linkage between PAISY data and those of other EDP systems, except for creating data support for banks to handle money transfers and for Thyssen to determine pension reserve allocations.

Data correction  Individuals concerned may request the correction or completion of incorrect or incomplete data. Cases of doubt shall be settled by the competent pension committee.

The collection and linkage of many personal details to build an overall profile of individuals, referred to as "personality profiling", also is an anathema to data protection officials at the federal and state levels. In March 1984 the data commissioners from the 11 states, and federal commissioner Dr Reinhold Baumann, issued a statement describing data linkage for the purpose of creating personal profiles as "inadmissible for reasons of principle." The 1983 case served as the basis for this position.

It has been pointed out by the Commissioner for the State of Hessen, Professor Spiros Simitsis, that personal information systems serve as "transit stations" for building dossiers on employees. It has been estimated that some 75 public agencies ranging from social security to local authorities, on the basis of 232 laws and regulations, require up to 239 data elements per employee. Employers are required under 126 different regulations to keep up to 214 types of data concerning each
employee. These data may well be used for internal purposes, Simitis claims, in applications condemned as a violation of the purpose principle by the Conference of Data Protection Commissioners.

For Federal Commissioner Baumann a special problem is the proliferation of personal computers in human-resources management. In his 1984 annual report he describes an investigation at the federal railway system. He studied three decentralized systems, including a pilot project on the assignment of tasks in electrotechnical services which provides complete surveys of work performance and non-attendance of workers by using 54 PCs. Dr Baumann said special safeguards are needed, such as strict control of the personal details that can be retrieved by any company manager, encryption and internal authorization to use both hard- and software.

At the Opel-GM works at Rüdesheim, 25,000 employees in 1985 signed a petition against the PAISY system, especially regarding linkage of data and building of personal profiles. The Works Council for two years had fought to obtain what was termed a "maximum of co-determination," but a labor leader warned that the Rüdesheim system is only part of an "international monitoring of productivity and performance by Opel-GM," which involves controls on a world-wide basis. A specific concern is the use of electronic systems to change work responsibilities of highly paid engineers and scientists by storing their expertise in data bases, which according to Klaus Franz, a union official in Opel-GM, amounts to "expropriation."
VDU Monitoring

Both the West German Trade Union Federation (DGB) and individual unions such as IG Metall have been active in the international trade union movement and within FIET (the white collar international union) to set ergonomic and work-environment standards for use of VDUs. A prohibition of "machine monitoring" or "electronic monitoring" of individual workers is one of the model standards included in this programme. (See our later section on international trade union activities.)

In 1979-1980, West German unions opened a campaign to write "model codes" for VDU work into both industry-wide and plant-level agreements. A study of about 50 such agreements prepared by WSI, the research arm of the DGB, covering agreements concluded between 1978 and 1981, found that work monitoring clauses were often included. A management publication analyzing these clauses concluded:

As regards work performance on VDUs, West German unions have expressed particular concern about the possible use of such equipment to record and measure the output of individual workers as a means of controlling performance levels. The unions have also been concerned about the increased "social isolation" of workers using VDUs for long periods of time. These two concerns have been taken up by union members on works councils with the result that plant-level agreements generally contain provisions precluding the use of VDU equipment by the employer to measure individual workers' performance levels and providing for performance targets to be set so as to allow time for necessary personal breaks and for contacts with other employees in the same department or elsewhere in the plant.

A major force in the campaign to secure such anti-monitoring clauses was the inclusion by IG Metall of that provision in its 1980 Model Agreement on use of VDUs. In Article 6, Working Conditions and Working Time, the Model Agreement states: "It shall not be
permitted to monitor the performance of workers, for the purposes of measurement, control, or comparison, by use of the installed equipment."

Co-determination of technical monitoring systems

A significant feature of the FRG situation is the role of the Works Council. There is no direct statutory basis for its involvement with the introduction of PIS as such, although there are interesting sidelines. The Works Council, for example, has to be consulted in matters of "internal order" in an enterprise, and it has competence to review the questions asked of workers for job placement. It also has a general obligation to follow the implementation of laws that cover working conditions, but it took court action to establish that the FDPA comes within this category.\footnote{9}

At many enterprises PISs have been made subject to a trade-union agreement.\footnote{10} But Professor Guenther Ortmann of Oldenburg University concluded from a poll that four out of ten companies felt consultation with the Works Council in these matters to be "superfluous."\footnote{11}

Involvement of the Works Council has received a substantial boost by decisions on electronic surveillance of the Supreme Labor Court in 1984-1985. At stake was the most specific statutory ground for the Works Council in these matters in the Act on the Works Constitution (para 87). It states in part:

"If no statutory rules or a collective bargaining agreement exist, co-determine:...The introduction and use of technical installations that are intended to monitor conduct or performance of employees."

This high-court ruling extends the power of Works Councils' co-determination with management plans and actions into the introduction and use of computers and automation equipment.
From this may be concluded that various modes of surveillance are outside the scope of co-determination. In a scheme:

```
Monitoring
  of employees of machines
    by a person by an installation
```

Subject to co-determination

When the Works Council Act was revised in 1972 it seems that parliament did not completely foresee the kind of rapid technological change that would follow. "This act was not written for computer terminals," Professor Horst Ehmann of Trier University has protested. The BAG emphatically does not agree. In its so-called computer-terminal case of December 6, 1983 it decided that any system is subject to co-determination if it collects data on conduct and performance of individual employees. Whether the employer actually evaluates the data used is not relevant, only that the system may produce them. The BAG left open whether the "technical installation" should cover the complete monitoring process or suffice that it apply only to part of the processing. The latter question led to the precedent-setting Rank Xerox case, BAG, September 14, 1984, DB 1984, p 2513.

The Works Council of Rank Xerox had filed a complaint against a new reporting system for its 2,000 repairmen. They had to fill in a form with 63 details on matters such as the number of spare parts used, time spent on the job, nature of the failure (after how many copies does a machine have problems) and the personal identifying number of the repairman. These reports were fed into a computer and produced so-called Service Performance Activity Reports (SPARs) that were used to build "call profiles". The Works Council termed it "an almost perfect possibility for surveillance of conduct and performance" and claimed co-determination. The company refused, arguing that the system only served better international supplying of spare parts. Simple processing of written reports anyway does not constitute a monitoring system in terms of the law.
Basing itself on the Census Decision and quoting the "well-known dangers of modern data-processing technology for privacy," if only the "loss of context" and the danger of reducing the employee to an "object", the BAG upheld the complaint. In two later decisions it further bolstered co-determination rights on electronic surveillance. One case (BAG, April 23, 1985, Das Betrieb 1985, p 1897) involved a word-processing system in a publishing house that already was the subject of an agreement between Works Council and management. The company wanted to order VDT workers to file their names. In the so-called "header" (a data inventory) these could be combined with an indication of the processed texts. The employer said the latter could cover anything from a few syllables to part of an article without specifying. Only by adding other data could the performance of individual workers be effectively judged. The company stated it did not have the software to do so. Still, the BAG decided the system change was subject to co-determination, even if it did not fully use the monitored data.

Another case (BAG, April 23, 1985, DB 1985, p 1898) involved eight technical testing stations in northern Germany. The experts and testing personnel in their employment fill forms, with their personal identifying number which is machine-readable. A computer program then processes the data. Although this may not produce specific and final results on employee performance, the programmed processing of test data on the basis of an individual identifier does constitute "monitoring" in the sense of the Act on the Works Constitution of 1972, the court concluded.

While these decisions undoubtedly made the position of the Works Council "more effective", as the federal government has commented, this does not mean that employee representatives are in a position to block workers' surveillance.13 If the Works Council refuses an agreement, the case is decided by an Arbitration Commission. This commission is obliged to balance the interests of the employer, which in a competitive environment may legitimately insist on monitoring workers' efficiency, to the rights of personality of individual employees. Professor Ehmann, who has chaired such a commission, indicates that criteria might be: advance warning before the introduction of the system; stating its purpose and scope; the principle audiatur et altera pars (including the right of workers to have individual circumstances—family, illness—taken into account) and time limits to the storage of data.

An early warning against automated performance controls for public service was sounded by the first Federal Data Protection Commissioner, Dr Hans-Peter Bull, in
his 1981 annual report. He reported a case of programmers who develop software on computer terminals. A system of automated monitoring had been put into effect to compute development costs. But it also helped to form an impression of the performance of individual programmers. The Commissioner thought it "problematical" to use data in such a way for purposes other than intended.

Bull referred to another example in a book he wrote after leaving office. Terminals were monitored to compute the efficiency of the system, such as the number of personnel needed, and to provide a safeguard against possible liability claims. After a great effort, Bull said, he was able to convince the agency concerned that efficiency statistics should and could be anonymous while data on liability should be restricted to a small circle of senior officials. Bull's successor, Dr. Baumann has repeated the objections against automated performance controls.

**Telephone monitoring**

With regard to telephone monitoring in the private sector, there have been conflicting decisions on the question of whether the telephone numbers called by workers may be recorded. A lower labor court ruled against this practice (AG Hamburg, October 10, 1984) while a superior labor court accepted it (LAG Duesseldorf, April 30, 1984).

In public administration this practice has repeatedly been challenged by data protection commissioners. The federal commissioner has made a distinction between official calls and private calls by civil servants from their place of work. He spoke out against registering telephone numbers called for private purposes, and counseled utmost restraint in recording official calls. Linkage of telephone numbers with other employee data should be prohibited; all monitoring data should be erased as soon as possible. The federal government, however, has refused to terminate the practice.

Particularly problematical, in the opinion of the federal commissioner, are calls by worker representatives (or other people in sensitive positions, such as counseling, medical services, etc.). To protect confidentiality, numbers called by them should not be monitored. In 1984 the federal commissioner reported that in one agency, on the basis of an unwritten understanding, calls by the Personnel Council are channeled through a special
conduit at the private branch exchange so that numbers called are not recorded. The commissioner expressed the hope that this would be the start of welcome developments elsewhere.

Hessen Commissioner Simitis also has held that extensive recording of numbers called by civil servants is "inadmissible". "From the point of view of the citizen," he noted, "it is hardly understandable why every call he receives from an official will entail, purely for internal-control reasons of the agency, storage of his own telephone number." Simitis warned against the possible result of creating "telephone profiles" of both citizens and civil servants. The Hessen state government did not wish to stop the practice of recording numbers, but some local administrations have accepted Simitis' recommendations.20

**Legislative situation**

Commissioner Simitis has hailed the Rank Xerox decision as a basis for bringing all personnel information systems within the field of application of statutory co-determination. Any PIS, after all, is a "potential surveillance tool that may be activated at any moment."21 Other observers are not so sanguine and have criticized the decision as judicial usurpation.22

In Hessen a formal change of the co-determination law was needed to bring about the introduction, use and extension of PIS to public administration within the scope of co-determination in the civil service. Other states have followed suit, if only for the public sector.23

In the private sector changes are in prospect, not because of an imminent extension of co-determination rights but because the federal government has formally committed itself to introduce legislation for the protection of employee data. In a statement of December 19, 1985 the Federal Secretary for Labor and Social Affairs confirmed an earlier remark to a parliamentary committee that "statutory rules for the protection of employee data are a necessity" and that the federal government will produce a bill in the next legislative period.24

The federal government, it has been officially reported, "fully recognizes that the fundamental right of informational self-determination, set forth in the Census
Decision, not only affects the public sector but also civil law, such as labor relations. The Minister warned, however, that the sensitivity of the matter "requires a very careful conception and design of the legislation." Clashes are possible with other fundamental rights, to name only one complication. There also are political difficulties. The opposition Social Democrats have introduced a bill of their own that would extend co-determination rights to personnel information systems in private enterprise and mandate appointment of the data protection officer that is called for in the FDPA. The government has not supported this legislation, to say the least, but announced it would study the matter.

The national employers' federation is fundamentally opposed to any new legislation in this field. The trade unions have welcomed it.

The federal commissioner, speaking on behalf of the Conference of Data Protection Authorities, strongly favored the legislation. He urged special attention to the following points:

1 Grounds for storage, use, change and communication of employee data should be more restricted than the "legitimate interest" of the employer that the FDPA now provides.

2 "Personal profiles", the linkage of extensive details about individuals, should be banned.

3 Access controls under the FDPA should not be used as conduct and performance controls.

4 Soft data, such as judgments on employees, should only be processed automatically under strong restrictions.

5 Medical and psychological data should be processed only in a very protected environment.

6 The existing right of access to employee files should be strengthened, in the release of particular by allowing/information identifying users of the data.

7 Co-determination on the planning and introduction of automatic processing of employee data should "unequivocably" be guaranteed.
It is somewhat ironic that neither this list nor the federal government's statement addresses monitoring of employees as such. Unions are increasingly worried just about the aspect of worker surveillance alone. Witness the headline of a story in the textile workers' union magazine of November 1984: Keine Video-Spiele mit Arbeitnehmer—"No Video Games with Workers".

FRG

Notes

1 The Census Decision, BVerfG, December 15, 1983 (published i.a. in New Legal Weekly, 1984, p 419) set forth three principles: Zweckbindung (purpose principle), Normklarheit (transparency of norms) and Verhältnismaßigkeit (proportionality). It generally has been accepted that these principles necessitate specific legal grounds for the processing of personal data.


5 Data Protection Adviser, 1984, No 6. The Federal Data Protection Commissioner calls for a complete ban on his second Annual Report of January 1, 1980, Bfd 2 4.3.5 and has repeated this in his most recent report, issued in July 1986, Bfd 8 Tätigkeitsbericht 5.2.4.

7 Data Protection Adviser, 1983, No 11.


10 Simitis, op cit No 6.


13 Stefan Waltz "Data Protection and Co-determination, a Reform Debate on Personnel Information Systems", Labor and Law, August 1985, No 8. See also Matthes, op cit No 9.


15 Hans-Peter Bull Data Protection or Fear of the Computer (Munich, 1984), p 162.

16 Bfd 8 Eighth Annual Report on the year 1985 (1.1.1986) 5.2.2.


19 Bfd 6 Sixth Annual Report on the year 1983 (1.1.1984) 5.4.3.

21 Spiros Simitis, op cit No 6.


23 See Walz, op cit No 13.

24 German Federal Parliament, Drucksache 10/4594.

25 Bfd 8 Taetigkeitsbericht (1.1.1986) 5.2.4.
EXAMPLE OF A WEST-GERMAN UNION-MANAGEMENT EMPLOYEE SURVEILLANCE AGREEMENT

In 1984 the Commerzbank AG of Frankfurt and the Union for Commerce, Banks and Insurance (HBV) entered into an agreement on the conduct and limits to electronic monitoring of bank employees. It is representative of the provisions that trade unions in the Federal Republic of Germany seek to negotiate with employers.

The following is hereby agreed upon with respect to the possibility that EDP provides of supervising the behaviour and performance of employees:

A. Data storage and the use of programs

1. The performance or behaviour of employees shall not be affected by means of existing or planned EDP systems. Data and programs which serve to verify performance or behaviour shall be erased.

2. Only such data on employees shall be stored as is absolutely essential for work planning. The Bank shall include all such data in an Annex 1 to this Agreement, stating the use to which they will be put and the reason why they are necessary. The Annex shall also make mention of set periods or events after which the data is to be erased. Data shall, furthermore, be examined at yearly intervals to see whether they are still required or whether they can be erased.

3. A guarantee shall be given that personal data on the employees which is a by-product of the working process or which can be deduced from work process data (such as data from the use of identity document readers, short codes, log data, user statistics, EDP utilization statistics, etc.) will not be such as can be used or interpreted as a check on personnel behaviour or performance.

4. Personal data on employees shall not be coupled with data such as is referred to in § 3 above. Personal data on employees may be disclosed only in the cases prescribed by law and, in such cases, the recipient, the reason for the disclosure and the date of disclosure shall be stated in detail. GBA shall be informed of each single or irregular disclosure of data.
FRG: HBV'S MODEL SETTLEMENT ON PERSONNEL DATA SYSTEMS

Following the intervention of the Conciliation Board, a model settlement has been reached between the German insurance company Deutscher Herold and FIET affiliate HBV concerning the operation of the personnel data collection and processing system PAISY. Initial attempts to reach an agreement had been blocked by the refusal of the company to recognise the union's codetermination rights in this field, which was the subject of a FIET Conference in October 1985.

The agreement provides that personnel information can only be collected by the company for limited and specified purposes, such as salary accounting, rent payments and insurance premiums. Statistics drawn from this information can then be used only if they are aggregated and unattributable to individual employees. All operations carried out by the system must be recorded, and the works council has the right to call in lawyers or data experts to examine all aspects of the working of the system without informing the company, and at the company's expense. In addition, the system cannot be extended without the agreement of the works council, or through a further decision of the Conciliation Board.

The importance which employees attribute to this issue may be judged from the fact that a meeting to discuss the terms of the agreement led directly to ten new members of the workforce joining the HBV.
5. The Bank shall, in Annex 2 to be drawn up to this Agreement, mention and briefly describe the program which is to be used for the personalized processing of employee data. This program shall, when put on line and at least once a year on a random basis, be checked for accuracy by a data protection officer or a neutral EDP specialist. The GBR shall receive a copy of the test report. Any addition to Annex 2 shall require the approval of the GBR. No programs shall be set up or run to adjust job profiles, to analyse dead time or compare performances. Exceptions shall be permitted only with the agreement of GBR.

6. Once only or irregular use of programs to evaluate personal employee data (statistics, meter readings, etc.) shall likewise require the approval of the GBR.

7. The agreements on the use of programs shall apply as appropriate to the use of information languages, dialogue interroga tion methods, etc.

B. Recording and verification

1. All data runs relating to individuals shall be recorded. A print-off of the record shall, on request, be sent to the GBR.

2. Entitlement to access data relating to individuals shall be regulated by both organisational and technical programming methods. Access entitlement shall be conferred on a stage-by-stage basis and shall be kept to an absolute minimum. The GBR shall have a list of all persons who, at any given time, have access entitlement. Unjustified access or attempted access shall be recorded and immediately reported to the GBR and employees shall be entitled to report suspected or actual infringements to the GBR or the shop steward.

3. Personnel measures based on information obtained through a culpable breach of the agreement here reached, shall be fundamentally ineffective.

4. Each employee shall, once every 3 years, receive a complete list of all data stored in the personnel data bank and relating to himself.
Should the employee object to any data, the Company shall immediately effect the necessary corrections unless it can prove the accuracy of the data on record.

Claims may at any time be brought requesting information except in cases of abuse of entitlement.

The employee shall be informed of any data communicated to third parties and shall be informed of the entitlement of such parties to access that data and the use to which they intend to put it. The office or department to which the data is communicated is also to be named. The only exception to this rule shall be bulk data supplied for statistical purposes (i.e. not identifying an individual).

C. Training and Staff Information System

1. To ensure that members of the GBR fully understand the rights and obligations created by this Agreement, they may participate in EDP training courses which will provide them with a sufficiency of the qualifications required. The cost of such courses shall be borne by the employer.

2. The agreement of the GBR shall be required in order that the IPAS Personnel Information System may be introduced. Should the Parties be unable to reach agreement, the conciliation board shall, here too, decide.
Norway is traditionally a society characterized by the term "welfare state". After the second world war a long period of predominant social-democratic government emphasized the conditions of workers and employees. Former coalition composed of the Conservative Party, Christian Democrats and small parties was not in disagreement over the major objectives of social policy. Also, this coalition supported the goals of a welfare state. This is expected to be continued by the present Labor Party government.

The Social Democratic party (Arbeiderpartiet) has a long tradition of cooperation with the national union (Landsorganisasjonen, or simply LO). Consequently, there has been a strong influence from the unions on government policy. This is also reflected in the national organizations of employers and employees.

The employers are organized in a national organization (Norges arbeidsgiverforbund, or NAF). There is no obligation to be a member of this organization for an employer and there are other organizations of employers. But these are minor—in practice the NAF is the central organization of employers with substantial power to direct the strategies to be followed in negotiations by its member organizations with the trade unions. The major exception is the government, which is of course a major employer which negotiates separate agreements with organizations of the employees.

Employees and workers have traditionally been organized in LO, which is composed of number of trade- or industry-related unions. This is a very strong organization indeed, and most employees will participate in their relevant union. LO has traditionally maintained a close relationship with the Social Democratic party, for instance through collective membership agreements. This political affiliation has recently become slightly more controversial and a separate national union, Yrkesorganisasjonenes Sentralforbund, or YS. Some characterize LO as a blue-collar and YS as a white-collar organization—though there are numerous exceptions and this can be disputed.

Relations between organizations of employers and employees are maintained on several levels. The national unions enter into general agreements on working conditions and wages. The national trade- or industry-related organizations of both employers and employees enter into more detailed agreements. And the individual employer will negotiate a local agreement with the local union.
These relations are generally characterized as cooperative in nature. There are few wildcat strikes or unauthorized industrial actions in Norway. The system of negotiations is very much an integrated part of the political system. Government will refrain from intervening in a legal conflict until vital social interests are at stake, but will often try to encourage communication and negotiations between the parties to a conflict. The Act on Workers' Protection and the Working Environment of 1977 governs relations between employers and employees. The act contains principles setting limits to employer controls, standards for work environment, etc. The Directorate for Labor Inspection (DLI) is empowered to enforce the act.

Worker surveillance—pre-high technology

Surveillance would be defined as an action taken by an employer which in principle could be subject to actions by the local union or which might be referred to the DLI. Work environment is a general term including physical and psychological elements. Surveillance consequently has an impact on the occupational environment, and therefore comes within the authority of the DLI and the local institutions. In companies employing more than 50 employees, a special occupational environment committee is to be established with equal representation of employer and employees, and reporting to the local branch of the DLI. In all companies with more than five employees a special ombudsman also is nominated among the employees with special responsibilities for their occupational environment.

This structure is defined by the Employee Protection Act but has been developed over the past several decades. Many institutions and procedures have been introduced through the general agreements before being codified by parliamentary acts. Therefore, there have been organizations like the DLI with administrative responsibilities to respond to surveillance issues before the introduction of advanced information technology. Individual cases of surveillance have taken place, but these have not been formally reported.

Polygraph tests definitely have not been in use. This is not due to a prohibition but is because employers have never suggested using them. Introduction of polygraph tests at any time would have been met by a massive reaction from employee organizations and would not have been politically feasible. Psychological testing may have been in use for some very-special-purpose jobs, but then on the
basis of medical examination rather than screening of actual or prospective employees. Telephone monitoring for purposes other than debiting also would have been a violation of the general penal provisions on wiretapping.

Awareness of surveillance may be said to have been rather low before the introduction of advanced information technology. Therefore, specific provisions to control any early actions cannot easily be identified. But the system of general labor agreement and government controls would have been adequate to handle any specific instance of excessive control measures—which would have been opposed by those enforcing established norms. For these reasons employers were discouraged from introducing surveillance methods. Consequently, none can be reported.

In assessing this situation, it should be borne in mind that Norway is a small and extremely open society. A system of personal identification numbers has been introduced, making identification and tracing of an individual rather efficient. Tax assessments are publicly available; access to other government files is quite easy as well. Therefore, it may be maintained that surveillance for screening purposes, identification of political affiliation, general personality profile, etc., may not be a need strongly felt by employers.

Current Surveillance situation

Worker surveillance is currently regulated in several ways. Firstly, the general labor agreement between LO and NAF of 1975, as amended (Section 6 No 7) provides for discussions of internal control measures—the need for such measures, their introduction and design. The general agreement refers to a supplemental agreement on internal control measures. This provides for supplying information to employees and their elected representatives who shall have a right to comment on such proposed measures (Section 3). They have to be clearly necessary and not excessive with respect to the actual requirements of the organization (Section 11). All employees or groups of employees must be equally treated with regard to any controls instituted.

The extent to which the control involves the storage or use of personal data, the period for storage, the data-security measures and erasure routines also should be discussed and defined, according to the agreement. This is in reference to the
Data Protection Act of 1978, and subsidiary regulations. There is an interesting interrelationship between the act and the labor agreements, as the regulation on employee data systems (Sections 2-12) is explicitly referred to in this agreement. The regulations specify 22 categories of personal data permitted in employee systems, but make a general extension provided this is authorized either by an act of parliament or general agreements between the organizations of employers and employees.

In addition to the agreements and the data protection legislation, the DLI has authority as far as the occupational environment is concerned. Frequently, the Data Inspectorate which supervises the Data Protection Act, and the DLI each may have authority to intervene. There are indications that the employee representatives prefer to seek help from the DLI, probably as this is traditionally the institution most closely related to the situation of the employees.

There is some information on the regulation in local labor agreements on inclusion of personal data for control purposes.¹ A common phrase in such agreements is the following (Borchgrevink 1985:375):

"Establishment and destruction of data systems facilitating a detailed control and surveillance of the individual employee in the person's working situation shall not take place without the cooperation of the organization of the employees."

A general agreement between the government and organizations of employees regulates the categories of "no show" which are permitted—"illness", "holiday", "leave" and other "no show" (which include military service, travel, non-authorized leaves, etc.).

**Union of Metal Workers initiative**

One cannot review the current Norwegian situation with respect to advanced technology and employee participation without mentioning the initiative which has become known as the project of the Union of Metal Workers. This union is the largest in Norway. As computerization of works and shipyards has taken place, the impact of new technology has been significantly felt. In view of the importance of these developments, Professor Kristen Nygaard of the Norwegian Computing Center, cooperating with the
union, funded a project to analyze this impact and suggest strategies for relating to them. This project was initiated in the early 70s, and resulted in a massive education of union representatives, a general awareness of the issue in the National Union and eventually a cooperative project with NAF. Based on examples from a number of local agreements (the earliest for 1972), a national general labor agreement on the introduction of advanced technology was reached in 1975. The principles embodied in this agreement were codified in the Employee Protection Act 1977 as Section 12(3): 

"Special regulation of planning and control systems
The employees or their elected representatives shall be informed on systems used for planning and in the work process, including planned changes in such systems. They shall have the training necessary to understand the system, and they shall take part in the design of the systems."

In 1972 the first "computer system representative" was elected. In many companies there are local representatives with a special responsibility for discussing and analyzing the computer systems from the perspective of employee well-being. As early as 1970-1971 there were examples of local unions taking an interest in elements of computerized systems which might be utilized for a control of the employees. An example is the local union of Kongsberg Vapenfabrikk, a major producer of arms systems, gas generators and special-purpose computer equipment. They were using a management system which generated management data on the output of the different work stations. The local union argued for a redesign of the systems, which actually led to the development of a customized in-house system to replace the standard system then in use.

There is no information known to exist on location monitoring of employees beyond time card check-in procedures.

**Telephone monitoring**

Regulations pursuant to the Data Protection Act do not permit the establishment of telephone-monitoring systems—i.e. systems which will record the number of the subscriber to which a call is made. There are two general exceptions, however
(Borchgrevink 1985:288-290). Firstly, the Data Inspectorate has licensed hotels to record telephone numbers from rooms of the guests. It should be emphasized that a corresponding license to record the calls made from the rooms or work stations of employees was not permitted. Secondly, the Inspectorate has licensed recording of calls made from some shipowners. The shipowners charge the expenses to certain customers and these have required specifications. The license authorizes the recording of certain numbers required by customers, but not other numbers. It is implied that the same reason may be an argument for licensing the recording of numbers by private attorneys, consultants, travel agencies, etc.—but such agencies have not as yet applied.

Productivity monitoring

As the Union of Metal Workers early on took part in the development of strategies with respect to computerized systems, one will find that there, in this respect several examples of agreements determining the monitoring functions of such equipment.

An example involves a protocol on the use of a log of a CNC (Computer Numeric Control) machine for a workshop. In this protocol a number of functions were recorded—error correction, reprogramming (testing), re-equipping, maintenance, waiting time, engine polishing and down time. "Waiting time" and "down time" may be exploited for operator surveillance. The protocol states that: "The log shall not be used in surveillance of the operator of the machine." In this case the equipment used also was decided to be undesirable, and was to be returned to the manufacturer at the end of the one-year guarantee period.

Another case involving the same type of equipment resulted in the protocol stating that the recording equipment only is to be used for a limited period of one year, and the recorded data are not to be utilized for surveillance (Borchgrevink 1985:286).

In another case a company purchased a printing press, and negotiated agreement with the organizations of employees in the normal way. The printing equipment, however, contained a device for continuous recording of its operation. This was beyond the agreed terms and the purchase had to be considered in the light of the special computer and control agreements. The equipment remained out of operation until satisfactory terms were reached.
In still another case a hotel used a device that could be plugged into a recording unit while rooms were being cleaned. The receptionist would then be able to see when a room was ready for check-in of a new guest. It did, however, also record the time used in cleaning a room. No local agreement on the practice has been negotiated.  

A recent survey by FIET produced the following report from the bank union in Norway:

The bank union has included in its technology agreement regulations to control the collection of personal information. For example information on work volume may only be collected at the level of the work groups and not of the individual employee. Teller terminals in the banks provide a great deal of information on work speeds etc., but local regulations laid down under the collective agreement are designed to ensure that such information is not used to evaluate employees. The union points out that the only way to assess the impact on employment and working conditions of new technologies such as EFTPOS is by using such work measurement devices. However the union stresses the importance of controlling the use to which the information is put.

Following this summary, we reproduce an article from the November, 1982 European Industrial Relations Review that contains both a useful historical summary on the Norwegian development of data protection in the workplace and an example of a technology agreement negotiated by the Norwegian Lift Installers Union.
Video surveillance

Video surveillance and systematic storage of video records is regulated in the general agreement between LO and NAF (Section 6 No 7). Introduction of such equipment is to be negotiated by the local parties according to the provisions in the general agreement and the supplemental understandings on surveillance. The general agreement has special conditions for direct and continuous video surveillance. The purpose and need for such surveillance is defined as:

"Such surveillance is to be avoided when possible, and the requirement of relevance in the Data Protection Act is to be applied. Systematic storage by video, etc., is to be limited by the Data Protection Act."

The reference to the Data Protection Act is significant because it is by no means obvious that such registers would qualify under the concepts defining the scope of the act.

There is a case decided by the Data Inspectorate where cameras surveyed a certain sector of the area in which a company had its business. The resulting video recording could later be screened. The Union of Metal Workers maintained that the Data Protection Act applied to this system. The Data Inspectorate decided that the video recording contained personal data, but that the criteria in the act for individual retrievability were not met. If the camera surveyed certain work stations, recordings or an index to the resulting \[\text{was established, the recordings would be subject to the law. Otherwise, the act has doubtful jurisdiction.}\]

Use of employee records for surveillance

Agreements in the banking sector have been negotiated on the collection of work statistics. These data should not be individualized. Plans for the introduction
of such systems must be presented to elected representatives of the employees who may refuse to authorize them. Similar examples may be found in local agreements in newspaper unions, where it is stated that "the system shall not function as personnel surveillance in any sector."

A recent example has emerged during the introduction of computerized case-handling systems for the social-security administration. Such a massive computerization of a major government bureaucracy will obviously have organizational consequences. In order to collect information on work procedures, manual time measurement took place until 1984. At that time, the unions for the employees rejected these measurements.

There is general consensus on the objectives of the computerization of social-insurance institutions. But there is disagreement on the effect of rationalization. In order to prove their point, the unions of the employees agreed in 1984 to initiate a pilot project in cooperation with a semi-public computer bureau, the East Region Computer Office (KDo). This office introduced a terminal-based time-measurement system. In November 1985 agreements were reached to extend this scheme to a large number of social-security offices. The system produces each day work statistics, which are also available to the representatives of trade unions and management alike. The data are not to be exploited as organizational management data until further agreements are reached.

This last example illustrates how detailed data on the individual employee is collected, but such information may be used only in aggregates for organizational development. The trade unions have voiced this position to counter the employer supporting theoretical arguments on rationalization effects with empirical data on actual case management.
Norway

Notes

1 This and further examples in this paper are based on Mette Borchgravink Ny teknologi i arbeidslivet, Norwegian University Press, 1985. For this book Borchgravink was awarded a lic.jur degree. The book is the result of a project at the NRCC, supported by the Norwegian Research Council for Science and the Humanities.

2 The project is documented in Kristen Bygarrd/Olav Terje Berge Planlegging, styring og databehandling, Tiden, 1974 (two volumes).


4 This example is discussed in an unpublished report by Dag Wiese Schartum, who is directing the project NORIS (70) "Work process, information technology and service quality in social-welfare institutions", a project financed by the Stiftung Volkswagenwerk and in cooperation with Wissenschaftszentrum Berlin and the London School of Economics and Political Science.
NORWAY

New technology and data protection

Whereas the job security consequences of new technology have become a feature of collective bargaining in several Western European countries in recent years, in Norway, where unemployment continues to remain relatively low (around 2.5% currently), the data protection aspects of new technology have also been given considerable attention.

In this article, we show how unions and employers in Norway have adapted to the advent of new technology as it affects industrial relations, and examine the role of legislation in this field.

The central agreement
Historically, the first attempt to regulate new technology issues in any global way in Norway occurred in 1975, with a central framework agreement between the country's main private-sector employers' organization, NAF, and Norway's largest union confederation LO - EIRR 68, etc. This agreement which, like all collective agreements in Norway, is legally binding, was last revised by the signatory parties in March 1982. Since this date, the agreement has been enshrined in Norway's latest Basic Agreement between NAF and LO, which lays down the basic ground-rules for industrial relations in Norway (EIRR 101).

The new technology agreement or, more precisely, the framework agreement on "technological development and computer-based systems", covers computerized systems used for planning and carrying out work, as well as those used for data storage and the use of personal data - i.e. "all data which either by name or by other identifying code may be traced back to physical persons employed by the individual undertaking".

The agreement acknowledges that the introduction of new technology can affect working and employment conditions, so that before any data-based system is introduced it must be evaluated from a social as well as a technical and economic standpoint. Consequently, company management is required to inform union shop stewards on prospective changes, and Norwegian Parliament adopted an Act on personal data registers which introduced certain statutory restrictions on their content and use. These safeguards apply to all sectors of the Norwegian economy (i.e. not just the private sector as is the case with the NAF/LO agreement) and to all personal registers, whether computerized or manual.

This Act, which took effect in 1980, established a State-run Data Inspectorate to monitor the use of personal files; keep a record of any such files on a central register; and issue permits for the establishment of all computer-based personal files. The Act states that for the registration of personal information to be justified on "objective grounds", consideration must be given to "the administrative and operational activities of the institution or undertaking carrying out such registration". Certain types of information are generally prohibited from being registered - including information concerning a person's race, political or religious beliefs, criminal convictions, state of health, and sexual activities.

grants employees and their representatives general statutory rights to be informed about systems used for planning and controlling work and to be given any necessary training to operate and help in designing such systems.

On privacy and data protection, the agreement states that "collection, storage, processing and use of personal data shall not take place unless due consideration is given to the activities of the undertaking. In each undertaking, it shall be made clear what type of personal data should be collected, stored, processed and used via a computer-based system". The agreement adds that negotiations should take place at undertaking level with a view to securing a collective agreement between management and shop stewards on the use of personal data. Failing any such agreement, the matter may be submitted to NAF and LO and裁决 in central level for resolution.

Statutory back-up
These particular provisions on data protection appeared in the original central framework agreement of 1975 and have remained basically unaltered since then. In 1978, however, the
Where information is stored on a computer, the individual concerned has a right to be informed of the type of data being stored. This right is extended to cover manual as well as computerized files, where such files are stored by central or local Government institutions. The Data Inspectorate has powers to order the correction, deletion or supplementing of any erroneous information.

The Act also contains special rules regulating the activities of organizations which specialize in providing information on individual credit-worthiness or financial reliability; and organizations which specialize in data processing, addressing and distribution, and opinion polls and market research.

Failure to comply with any of these statutory rules can lead to up to one year’s imprisonment and/or a fine – the level of which is not specified in the Act but will vary according to the circumstances of the case.

Local bargaining
In addition to this network of statutory provisions and centrally-agreed rules on new technology, numerous private-sector firms in Norway have negotiated local agreements with unions on data protection – as specifically provided for in the NAF/LO central framework agreement. A wide range of firms are covered by such arrangements including Viking-Askim, which manufactures chemical products, and the Kongsberg arms factory. It is not possible to tell how many local agreements have actually been signed, however, since neither NAF nor LO require their member organizations to register agreements centrally; neither is there a Labour Ministry function. On the other hand, NAF organizes some 9000 firms – a clear indication of the maximum number of local agreements that may have been signed on this issue.

The Reber Schindler case
A typical local agreement on data protection was recently concluded between management and shop stewards at the lift and escalator manufacturing and maintenance firm Reber Schindler Heis, based in Kristiansand in Southern Norway. Below we discuss briefly the background to and contents of this agreement – formally entitled “Directions for compilation and use of personal data”. The full text of the agreement appears in the accompanying box.

Reber Schindler began operations in Norway in 1946. It is part of a Swiss-owned company and today employs 280 people. Towards the end of 1981, management decided to install a computer, to take over many of the control and planning functions previously carried out manually and, at the same time, to transfer much of the personal information on its employees, previously stored in classical written form, to computerized files. (The manual files had been checked in 1980 to ensure that they did not contain any proscribed information as laid down under the Act on personal data registers – see above.)

In line with its commitments as a NAF member firm under the central framework agreement, Reber Schindler management then began negotiations with shop stewards from the country's Lift Installers' Union (which represents most of the firm's employees). The aim of the negotiations was to conclude an agreement on how personal data could best be processed automatically and what safeguards should be introduced about its uses, regardless of form.

According to company management and shop stewards, the negotiations spanned a period of some six months – largely because more pressing day-to-day concerns were given priority – and the final agreement materialized towards the end of March 1982.

The agreement states that personal data registration will only be permitted so long as it is considered “reasonable” in the context of the company's activities and the law. Thus, for instance, agreement was reached that information on an employee's educational background should only be stored where the courses and qualifications were “relevant” to the job. In any event, the use to which any personal data may be put is subject to prior discussions between company management and local union officials. The agreement also covers safeguards to ensure the confidentiality of information. These include limiting information access to specific authorized individuals, so that where automatically processed data is involved, only those authorized persons “shall know the system keys for necessary access”. The agreement also deals with the statutory rules on individual rights – e.g. to check information for errors, etc.
Directions for the use of personal data:
Agreement of 22 March 1982 between Reber Schindler Heis A/S and the Norwegian Lift Installers Union

1. Introduction
The directions build upon:
1. The Act on Personal Registers, etc of 9 June 1978, together with associated provisions.
2. The Basic Agreement between LO and NAF (union and employer confederations respectively – EIRR 101).
3. The framework agreement between LO and NAF on technological development and data-based systems.

2. Scope
These directions regulate compilation, storage, working with, and use of personal data within the company. By personal data is meant information and assessments which may directly or indirectly be connected with identifiable individuals in the company. The agreement applies to personal data irrespective of its method of compilation, use, or form of storage.

3. Objectives
Registration of personal data shall only be undertaken where there is a reasonable basis for so doing, having regard to the company’s administration and activities, or what is permissible under Norwegian law.

The objective of the company’s storage and use of personal information shall be discussed with the local union branches. Where there is a demand or a wish on the part of the company, the local branches, or the Government, for alterations to, or extension of, the scope of the registers, the purpose and area of use shall be discussed with the local union branches.

4. Compilation, use, storage
Discussions shall be held with the local union branches on the procedures to be followed in the event of the company compiling, using, storing and supplying personal information.

All compilation, use and storage shall be carried out in such a way that all employees or groups of employees receive equal treatment.

5. Control
The company and the local union branches shall co-operate in order to avoid personal information being abused. In this respect, the following guidelines shall apply:
All personal data, irrespective of its form of storage, shall be treated as confidential information under the company’s rules for confidential documents.
The type of personal data to be compiled, stored, worked on, and used, shall be discussed with the local union branches.
Lists and circulars with personal data shall only be requested by, and supplied to, persons who have been specially authorized. Any individual with special authority to receive such lists and circulars shall be responsible for these not being disclosed to unauthorized persons.
As regards personal information which is accessible by way of data terminals or equivalent machine methods, only specially authorized persons shall know the system keys for necessary access. Such authorized persons shall be placed under a duty of confidentiality.
The company shall exercise continuous supervision of all registers which contain personal data and over the information which is contained therein, as well as over who has access to the various reports/registers. In the event of actual alterations, the lists shall be brought up to date immediately. The local union branches shall have a copy of these summaries.
6. Awareness right
Each individual employee shall have a right, on request, to be informed as to what information about himself is stored in the registers. For more detailed methods of access, reference should be made to section 7 of the Act on Personal Registers [concerning the individual's right of access] and to sections 1 to 5 of the provisions [concerning the scope of the Act and the Data Inspectorate's rights and duties].

In the event of any error, the registration shall be rectified immediately, and an extract from the new registration shall be sent, without the need for a request to be made, to the person concerned for checking.

7. Updating, erasing, destroying
Procedures for bringing the registers up to date shall be discussed with the local union branches. The individual shall be sent an extract of his own data for checking and possible correction.

Unless the company is bound by any Act, provision, or agreement, or by any other time limit, personal data on individuals who have ceased to be its employees shall be disposed of not later than the expiry of the following calendar year.

Reports from registers which have lost their currency, shall immediately be destroyed. This applies particularly to automatically processed lists which are produced periodically, and where previous lists are no longer of value.

8. Transitional provisions
Representatives of the management of the company and of the local union branches shall undertake an inventory of all personal registers in the company.

The need for each individual register shall be assessed.

The same shall apply in respect of the need for the items of data contained therein. Any data which is not considered necessary shall immediately be disposed of/destroyed.

9. Questions of Interpretation
If disagreement arises between the parties at the company over how these directions are to be interpreted or their scope, either party may refer the matter to its central organization. The Data Inspectorate may also, in certain instances, be called in where problems of interpretation are concerned.
FRANCE

Automatic monitoring of telephone calls, especially recording the numbers being called, has been repeatedly brought to the attention of the National Commission on Informatics and Liberties (CNIL), by individuals, trade unions, and in some cases employers. There is a difference of opinion on the nature of the practice, because the former fear intrusion of their privacy and the latter want to know the limits of such surveillance. Data collected are considered "indirectly nominative" which obliges government agencies to issue privacy regulations before putting telephone monitoring devices into use. The CNIL must be consulted during the preparation of these regulations. Private companies, however, are only obliged to notify the CNIL that they have introduced such monitoring.

On January 21, 1981 the French Supreme Court in the "Malherbert" case issued a ruling on listening-in on telephone conversations by the director of the staff of a half-way house for young workers. It deemed the practice a violation of human rights. This decision has influenced telephone listening practices in France.

The metal workers union (CFDT) in 1981 objected to the use of electronic badges used in IBM plants, called Access Control Enhancement Program (ACEP). Union representatives challenged the program because it could be used not only for access to the parking lot and machine rooms, but also for other purposes. IBM management insisted that only "anomalies" like people trying to get unauthorized access to locations or people who would like to get access to the plant outside of normal working hours would be affected. The union was unconvinced, press accounts suggest, because they said people sometimes arrive late or are delayed in getting to work and these situations could be identified and used against the particular worker involved.

In 1982 the CNIL was asked its opinion on automated invoicing systems initiated by the PTT for household and office telephones. The CNIL is involved in computer monitoring and computer aided decisions because of Article 2 of the Act under which it is established. Article 2 states: "No governmental or private decision involving an appraisal of human
conduct may be based solely on any automatic processing of data which describes the profile or personality of the person concerned." The CNIL recommended that only part of the telephone number called should be recorded to enable proper invoicing but not revealing too extensive details about the calls. The Commission noted, however, that systems involved in checking whether private conversations are recorded in the working place are difficult to judge. In a Recommendation 84/31 of September 18, 1984 the CNIL set forth its views on this type of practice:

1. Works Councils should be consulted in accordance with Sec. L-432, 2 of the Labor Code;

2. Employees should be informed on (a) the nature and frequency of monitoring; (b) conditions under which private calls must be paid for; and (c) their access rights under the data protection act;

3. There are to be strict limits on data stored, so that data are not kept longer than for invoicing nor used for other purposes; and

4. Special attention should be paid to the rights of employees and representatives of Works Councils and trade unions (because companies tend to be listening to calls made by Works Council members or from their offices). Employee rights were established in the Act on Workers' Freedoms and Co-determination of 1982.

Union concerns were described in the CNIL's 1982 Annual Report with regard to the use of questionnaires to collect data on company personnel. The USINOR steelworks in northern France sought to reduce its staff, in particular, some underqualified personnel. The company distributed questionnaires to these employees asking about their family situation, hobbies and their ambitions as well as their "social capabilities." Those employees unable to competently complete the forms were terminated. Trade unions complained to the CNIL but the Commission said it didn't have jurisdiction because computer processing was not involved. The CNIL urged USINOR's management, however, to give special consideration to this type of activity, especially try to establish union-management discussions before such programs are implemented.
In 1984 in its Annual Report (page 112) the CNIL referred to a case involving the national railway system (SNCF) which had been authorized by the Commission to monitor employee telephone calls. The CNIL emphasized it recommended that such monitoring should be publically known, personnel should be directly informed, profiles and practices should not be prepared, and monitoring must be random, not systematic.
Video System Monitoring Production Personnel

A district court in Holland in 1985 issued an injunction against installation of a video system for monitoring production personnel. The case was brought by the FNV trade union of industrial workers against Koma, a highly specialized firm producing refrigerating machinery. It was planning to install the video system in all its 18 production departments after a successful experiment to link an outside production hall to central facilities. The Workers' Council did not complain, but the trade union protested after finding out that many employees objected to being watched. Management argued that the purpose of the system was not "surveillance" but "guidance" and "help". The acting president of the District Court of Roermond was not impressed. He noted that the purpose of the video system was unclear and that consultation of the Workers' Council had been a mere formality. So the presiding judge ordered the system stopped until a full court case on the merits has been decided or parties concerned have reached a comprehensive agreement. This could be part of a collective bargaining agreement, as had been suggested in court, but the judge warned that any collective formula should pay due respect to the fundamental right of privacy as an individual right. "One of the characteristics (of this) is that a majority cannot deny an individual or a minority a claim to this right."

The decision of the Roermond court opened up new legal ground. The government privacy bill in the Dutch parliament does not address such surveillance methods. The court said that surveillance of employees by employers in their work will not be felt as an invasion of privacy as long as it entails personal contact. "Privacy protection extends to the workplace," the court added. Of course, the personal right is not absolute and will have to be balanced against other values such as safety at work, environmental considerations, efficiency. But this should not be done without due agreement with the employees on the use of the system and safeguards.

Telephone Monitoring

As early as 1977 there were questions in the Dutch lower house of parliament concerning the leasing of telephone monitoring equipment to private companies by the PTT. The Secretary of State for the PTT defended the practice as did the Minister of Justice. They justified this practice because it was mainly for use by small firms. Three acceptable reasons were advanced: (1) monitoring the (technical) quality of calls with external business relations; (2) preventing misuse of telephone facilities such as use for private calls by employees; and (3) assisting company executives to listen-in on certain calls (concerning arrangements and contracts with other companies) to "witness" what is said. The PTT might warn employers that there are privacy risks connected with this kind of system, the Secretary of State noted. The Minister of Justice referred to a criminal code provision against telephone eavesdropping but indicated this constitutes an exception because employers have a legal interest in these conversations as they are placed on their equipment. However, the Minister said the decent thing to do would be to inform employees of this practice.

Electronic Passes

The issuance of electronic passes to Rotterdam harbor workers has been a controversial action. Before they were introduced there had been "moonlighting" on the docks by some non-union workers. In February, 1986, employers and workers reached an agreement for an electronic pass system to be introduced. Members of the Transport Union initially thought the pass might be used to check the time of arrival and departures of trucks. The employers actually did not like the system because it would lead to accusations of invasion of privacy. Nevertheless, the union called for implementation of the pass plan because it had negotiated a strong agreement guaranteeing their members jobs. Consequently, it wanted the passes to make it impossible for non-union workers to take work away from their members.
An agreement signed on April 12, 1984 between the Austrian Data Protection Commission and General Motors (Austria) protects individuals against disclosure of personnel information stored in computerized databases. Conditions and regulations are specified under which GM can store and disseminate personal information on employees and customers in several data systems.

A range of information is collected about customers, such as car sales number, guarantees and warranty documents, the name of the customer, address, car type, registration number, seller details, payment terms, any sale or credit terms, and bank relation information. GM is permitted to use some of this information for market analysis. Otherwise, customer data is not to be disseminated outside the Austrian company.

Information concerning union membership, employee work records and wages is not to be disclosed. Details on wages can be released according to agreement by both GM and the trade union. Income details, the data protection commission stated, must show real income, that is gross salary, with deductions itemized. Wage payments also may be released for research purposes but vacation and sick leave details must be deleted from inclusion of any studies.

The agreement also specifies that control over computerized data must remain in Austria. The computer system cannot be changed or new programs implemented by GM headquarters in the Federal Republic of Germany without consultation with GM Austria and its union. Access to computer data by foreign parties must be strictly controlled; unauthorized attempts to acquire information are to be regarded as illegal. No divulgence of information to any foreign investigation or enquiry may be made without express agreement with GM Austria.

Systems intended to monitor idle machine time cannot directly or indirectly be used without consultation. Data concerning time worked cannot be released nor used in any way for evaluating personnel by regional or GM world headquarters.

CONSTITUTIONAL RULING

In 1975 the Austrian Constitutional Court issued a ruling on telephone monitoring practices by a mid-sized steel works. The Court ruled this practice was "against human dignity" which is a general legal norm for "rights of personality". That is, individuals may not have their intimate private lives (sphere) intruded upon by the state. It is considered a landmark decision "in the defense of worker rights" by trade unions.
BELGIUM

There is no national legislation covering private sector use of electronic monitoring of workers in Belgium. However, labor-management contracts have been concluded containing provisions on personnel monitoring. One such agreement involves the SAIT Electronics Company in Brussels and its union. The agreement contains the following provisions:

(1) Confidential data on personnel may be processed automatically only if they are indispensable to the employer to meet legal obligations;
(2) Access to personnel data banks must be given exclusively to senior management of the enterprise and the data subject; and
(3) When an employee leaves the company, his data will be removed from the database and archived.

Government employees' personal details have been registered in a central data bank since January 1983. A decree giving a right of access and correction of these files has been issued. Although critics say the procedures involved are too complicated, such as those involving access and correction, the decree has not been amended. Some civil servants have complained that information about whether they can be easily relocated in the country has been collected. There is resistance by many Belgian civil servants about their "mobility for re-assignment."
The Swiss Confederation of Trade Unions (SGB) issued a report in March 1984 on "new technology and data protection in the company." It contains a model technology agreement. One of the provisions states that the automated collection and evaluation of data on the work-place to monitor the conduct or performance of the worker is not allowed. Only a few companies, mostly those involved in heavy industry, have endorsed this agreement.
PART III

BRITISH AND COMMONWEALTH NATIONS:

CANADA AND AUSTRALIA
CANADA

**Background**

Canada, with a population of 25 million, is a federal system, with 11 provinces and a national government headquartered in Ottawa. It has a labour force of 12.3 million, with 11 million employed at the end of 1984. This meant an unemployment rate of 11.3%, down from the 1982 high of 12.8% but still constituting a serious effect of the early 1980's recession.

About 35% of Canadian workers are represented by unions. Industry-wide collective bargaining is not common, and enterprise-level agreements are the general rule. Though some unions, such as the Canadian Union of Public Employees (CUPE) have drafted model Technology Agreements, this has not been effectuated to the degree that TA's have in Britain. Nor does Canada have national or provincial co-determination legislation creating works councils and co-determination in the European model.

There are no specific provisions dealing with work monitoring in any of Canada's national or provincial labour codes, nor have there been any regulations on monitoring issued by national or provincial regulatory authorities. Under the common law, no rights to privacy for employees have been found by courts to be legal limitations upon employers, nor have privacy statutes (Part IV of the Canadian Human Rights Act of 1977, the federal Privacy Act of 1982, or the Quebec data protection law of 1982) been held to control employer use of monitoring. What limitations on employer conduct have taken place have been the result of (a few) collective agreement clauses negotiated on that topic, or of arbitrator rulings interpreting rights of employees under contracts.
Union Positions

Prior to the arrival of microelectronics and office automation, Canadian unions had enunciated the traditional trade union position against measuring individual worker output and using this for judgmental purposes, as well as opposition to various forms of pre-computer surveillance -- hidden observation galleries in post offices, still or television cameras photographing workers, use of listening devices, telephone service-observing, etc.

Several examples of union activity on these issues, as compiled by Ken Rubin, a Canadian student of privacy and information technology, present the Canadian union viewpoint and efforts to deal with specific types of worker monitoring:

1. Electronic Sorting Equipment

The postal workers' opposition to individual-centred work measurement began in the 1950s when their postal association realized that their agreement to work measurement in 1953 did not simply imply the detection of faulty operations and methods. The fight was won by 1964 when the Post Office agreed to stop individual work measurement for full-time employees, though not for part-timers.

The issue surfaced again in 1975, when counters were installed on electronic mail sorters to measure individual employee productivity. Following a six-week national strike the Post Office agreed that work measurement studies could be conducted only on groups of ten employees or more. Individual work measurement designed to pressure and speed up productivity continued, however, in violation of the collective agreement. Although the Post Office has continued to press for individual work measurement, the agreement now in effect until September, 1984 (Clause 41.01) prohibits the practice. However, postal workers know this will continue to be a difficult clause to keep and enforce.
2. Closed Circuit Television

Problems associated with camera surveillance are illustrated in the following two cases.

**Puretex Knitting Company Versus the Canadian Textile and Chemical Union**

In November, 1978, employees of the Puretex Knitting Company in Toronto went on strike for better wages, improved seniority and fringe benefits, and to obtain the removal of revolving monitoring cameras in the workplace. The cameras had been installed by the company without consulting the union, following the discovery of systematic theft by an employee.

The strike was settled after a few months, including the removal of one camera by the women's washroom, but the issue of the other cameras was referred to an arbitrator. The 1979 arbitration decision ordered the removal of the remaining cameras in the work production area but granted retention of the cameras in the storage, loading and parking-lot areas with the stipulation that they be used only for security purposes, not to monitor work.

**Post Office Versus Canadian Union of Postal Workers**

In 1978 the Post Office installed closed-circuit TV systems (CCTV) in two Toronto plants and hoped to install similar equipment in all its modern buildings across Canada to prevent mail theft. Older buildings had observation galleries used by management to survey the workplace. The union viewed the action as a management ploy to increase work supervision rather than a security concern. The union argued that if security was the concern, cameras should be installed at points of entry and exit. Furthermore, actions should be taken to prevent further illegal mail-opening abuses by the RCMP, carried out in cooperation with postal authorities.

The 1980 Marin Commission testimony revealed that management did not know what effect CCTV was having on postal losses, what effect it was having on employees, what percentage of mail losses and damage were due to theft, and where in the postal system theft was occurring. CCTV at one of the plants, Gateway terminal, was used 22 times between October 1978 and August 1980. Videotape reels were made of two suspected cases of theft: one suspicion proved to be unfounded, the other led to a prosecution.

Following a strike in 1981 on the issue, among others, of workers' surveillance, the employer agreed to limit CCTV to the two Toronto locations for the duration of the collective bargaining agreement valid until September 1984 (Clause 36.09). The same contract also contained clause 41.02 limiting the use of observation galleries in older buildings to ensuring mail security, and not for evaluating employees' performance.
Electronic eavesdropping has been technically possible for some time. Nationally, however, it was only in 1974 that limits were placed on the practice with the passage of the Protection of Privacy Act. While this Act spelled out specific procedures and conditions for legal wiretapping by authorized police agents, it also added a new section to the Criminal Code, which legalized, without similar conditions, the employer practice of electronically eavesdropping on employees for work productivity observation. As the clause states:

“A person engaged in providing a telephone, telegraph or other communications service to the public who intercepts a private communication (is able to do so) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks.”

Two cases illustrate the consequences of this section.

Airlines Passenger Agents - The Brotherhood of Railway and Airline Clerks (BRAC), which represents CP Air passenger reservation agents, has been concerned with electronic monitoring of employees' conversations, particularly in the Vancouver reservation office.

A voice-activated taping system was unilaterally introduced by management to tape customer calls in order to monitor and coach reservation agents on their 'sales pitch.' BRAC representatives, however, charge that eavesdropping and taping include inter-office employee communications and personal conversations, as well as incoming customer calls, and that the tapes are being used to justify disciplinary actions. The union wants to put a stop to such practices and has threatened legal action. Management has responded with a promise that only probationary employees will be taped without their knowledge. Regular employees will only be taped with prior verbal notice...

Telephone Operators on the Line - Telephone operators are subject to the same kinds of electronic surveillance. Eavesdropping on their workplace communications and the introduction of automated switchboards have led to stress and union opposition.

Random listening and recording of long-distance telephone operators' conversations is used to check for politeness, tone of service and work procedures. Management claims it is a training procedure but, in practice, it is not limited to new employees. Operators must consent to the monitoring of their calls as a requisite for employment, and they are never sure when they are being recorded. Customers are of course unaware that their conversations are also being monitored and possibly recorded.

The Communications Workers of Canada (CWC), which represents several telephone companies' operators, called in its 1982 Convention for legal prohibitions against management measurement of individual production through electronic monitoring. CWC encourages operators who are informed of eavesdropping, after the fact, to automatically file a grievance.

CWC also objects to the recording of operator performance on the newly introduced automated switchboards. Besides resulting in job losses and further centralization, the automated switchboards are capable of recording the time spent on handling calls, and the time spent on the job and at breaks. Overruns are thus monitored and kept within computerized service-analysis records. The machinery, programmed according to management directives, sets the pace and controls the workflow, thus ensuring that there are never surplus operators or 'unproductive' labour. Machine records can also be used to provide regulators with service statistics designed to justify telephone-rate increases.
In each of the areas in which Rubin described union positions and efforts, employers have defended these types of necessary to insure business efficiency and productivity, measurements or observations as socially and ethically justified, and not used in abusive ways. While we are not aware of any Canadian public opinion studies in which questions about these practices were included, it seems fair to conclude that, up to the present, issues of worker monitoring through closed circuit cameras, electronic sorting equipment, or telephone service-observing have not prompted general public concern, nor led to the enactment of legislative interventions.

Whether newer forms of electronic monitoring -- particularly of VDT work -- may be changing this situation is the issue we next examine.

**VDTs and Work Monitoring**

Beginning in the late 1970s, and influenced by European trade union activities relating to microelectronic impacts, a group of Canadian unions whose industries were beginning to experience office automation began conducting research and developing bargaining positions on new OA technology. In the private sector, lead unions included the Communication Workers (CWC), Brotherhood of Railroad and Airline Clerks (BRAC), Newspaper Guild, International Typographers (ITU), Graphic Arts, and Telecommunication Workers. In the public sector, leaders were the Canadian Union of Public Employees (CUPE) and Public Service Alliance. The national labor federation -- the Canadian Labour Congress -- also became active, especially through its federally-funded Labour Education and Studies Centre in Ottawa.

While the primary thrust of these union concerns was, first and foremost, protection of jobs and employment opportunities,
and, secondarily, health and safety of VDT operators, Canadian unions were also concerned about quality of worklife issues. It was from both the safety and OWL perspectives that "electronic monitoring" came under consideration.

1. VDT Survey by CLC, 1980

In late 1980, the Canadian Labour Congress' Labour Education and Studies Centre conducted a detailed survey of 2,336 workers at 15 workplace sites across Canada. The sites of 12 different employers were surveyed, in both the public and private sectors, in "the transportation, communications, and public service industries." The survey focused on "the health and working conditions of Canadian office workers" as these were being affected by use of video display terminals. The survey report, Towards A More Humanized Technology, was published in 1982. Sites represented by eight of the 11 sponsoring unions were used in the survey.

Several quotations from the Report's Summary cover the relationship of monitoring to the health problems studied:

3. Results of this study confirmed that health symptoms including eyestrain, stress and muscular discomfort are experienced by substantial numbers of Canadian VDT workers. These health problems were especially pronounced in workers making intensive use of VDTs for long hours in rigidly controlled and automated work environments. While ergonomic factors such as excessive glare, poorly maintained terminals, and inadequate chairs often contributed to high levels of reported health problems, psychosocial factors stemming from poor job design and dehumanizing working conditions were also strongly related to levels of reported complaints...
5. A clear picture emerged that VDT work was organized differently from traditional office work. Workers in intensive use applications (which comprise the "production line" and "data entry" job tasks) were generally required to spend the entire work day sitting at their terminals with little or no opportunity to move around or work at non-VDT tasks. The use of telephone headsets in "production line" tasks aggravated worker feelings of being chained to their work stations.

7. The degree of work monitoring by the system and the amount of control workers had over their work speed varied considerably amongst the various types of VDT work. One pattern emerged very clearly, however. The most intensive and most controlled use of both VDTs and workers was found in "production line" work with the "data entry" group following closely behind. The most variety and flexibility in job tasks was noted by the "professional and technical" group. The remaining group of "conversational clerical" VDT workers reported work patterns falling somewhere between these two poles.
Table 39 of the CLC study provided data directly related to health effects of VDT operators working under employer monitoring. (see table on next page) The CLC report commented on the table's results as follows:

Work Monitored by System: Increased levels of the four stress-related health problems were found for VDT workers who reported their work was monitored by the computer system (Table 39). About twice as many such workers reported general tiredness, irritability, headaches, and sleeplessness "almost daily." These results indicate work monitoring to be another stressor in the VDT work environment.

The recommendations that the CLC made, based on the survey, included a coordinated set of proposals covering system design, ergonomics, work rules, worker participation, and further research. On the issue of employer use of monitoring, they recommended:

Since stress symptoms increased greatly when workers were being electronically monitored:

It is recommended that direct electronic monitoring of individual worker's activities and productivity be discontinued.

If productivity monitoring is deemed necessary, other methods of indirect or aggregate monitoring exist for this purpose.
### Table 39 - Stress Problems Experienced "Almost Daily" by VDT Workers: Effects of Work Monitoring and Distance from Co-Workers

<table>
<thead>
<tr>
<th>Stress Problem</th>
<th>No (1745)</th>
<th>Yes (807)</th>
<th>Don't Know (140)</th>
<th>Too Crowded (589)</th>
<th>About Right (1035)</th>
<th>Too Isolated (55)</th>
</tr>
</thead>
<tbody>
<tr>
<td>general tiredness</td>
<td>8</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>irritability</td>
<td>23</td>
<td>31</td>
<td>28</td>
<td>31</td>
<td>24</td>
<td>40</td>
</tr>
<tr>
<td>headaches</td>
<td>11</td>
<td>23</td>
<td>17</td>
<td>22</td>
<td>12</td>
<td>37</td>
</tr>
<tr>
<td>sleeplessness</td>
<td>10</td>
<td>19</td>
<td>18</td>
<td>14</td>
<td>14</td>
<td>35</td>
</tr>
</tbody>
</table>

Total VDT workers = 1742

(Number in each group = )
2. Growth of A Union VDT Campaign

Mobilization of Canadian unions around control of "adverse VDT effects" grew stronger in 1981-84. In 1981, the Ad Hoc Committee on VDTs was formed under the Labour Council of Metropolitan Toronto and began publication of a widely read newsletter, called, "Got The VDTs?" A steady stream of articles in this publication reported health and stress problems experienced by Canadian VDT workers, with monitoring a frequent topic.

Gov't employer abuses contract workbreaks

Rest breaks negotiated by VDT operators can be abused by employers and work against the interest of the employees.

The employer, the Ontario Ministry of Health, however, introduced a work organization system which violates the whole intention of this machine break provision.

Normally, data entry operators at OHIP (Ontario Health Insurance Plan) are required to work 345 minutes per day keying in at a terminal, and 60 minutes daily at housekeeping and materials preparation.

In order to get around the new 10-minute rest break provision, the employer has cut the 60 minute housekeeping time in half (30 minutes), the remaining 30 minutes to be used for rest breaks.

In effect, the operator spends the same amount of time keying in (345 minutes) but now has less time to perform necessary tasks in preparation for machine processing.

The operators who work under strictly monitored quotas based on key strokes per hour have to work even harder to maintain their quotas. Since housekeeping time has been cut in half, they are under greater pressure now than before.

OPSEU is in the process of filing a grievance in response to this recent move.

The moral of the story — make sure the provisions for rest breaks or machine breaks are clearly spelled out and take quota systems into account.

In fact, it is just such quota systems and machine monitoring which should be attacked and eliminated.

VDT operators can't avoid getting the impression that employers — in this case a branch of the Ontario government responsible for health — does not take recommendations for the health of the VDT operators seriously.
Alongside such publicity, Canadian unions began a campaign to secure technological change agreements covering VDTs. Two influential examples -- *Tech Change: A Handbook for Negotiations* issued by the Canadian Labour Congress in 1982, and a Model Contract on Technological Change drafted in 1982 by the Canadian Union of Public Employees -- included proposed bans on work monitoring. Excerpts are reproduced below.

Canadian Union of Public Employees, Model Contract on Technological Change, 1982.

**Article 30 - Technological and Other Changes**

**30.01 Technological Change - Definition**

In this Article "technological change" means any change in:

a) the introduction of equipment, material or processes different in nature, type or quantity from that previously utilized;

b) in work methods, organization, operations or processes affecting one or more employees;

c) in the location at which the work, undertaking or business operates;

d) in the work, undertaking or business carried on by the Employer including any change in function performed and including the removal of any part of the work, undertaking or business.

**30.02 Technological Change - Adverse Effects to be Eliminated**

In carrying out technological changes, the Employer agrees to eliminate all injustices to or adverse effects on employees or any denial of their contractual or legal rights which might result from such changes.

**30.15 Technological Change - No Individual Work Measurement**

It is recognized that volume measurement may be necessary to obtain an objective evaluation of the level of production of a group, a section or an office. However, there shall be no individual work measurement.
Tech Change:
A HANDBOOK FOR NEGOTIATIONS

Canadian Labour Congress (1982)
Surveillance and privacy

Employers are now using microelectronic technology to closely monitor the output of individual employees, the number and frequency of errors, and the time they spend away from their machines. The awareness of constantly being closely watched and paced by a machine greatly increases the stress levels for these workers.

Employees should be protected against such deep invasion of privacy and close surveillance. It is interesting to note that the practice of individual electronic monitoring was prohibited by legislation in Sweden in 1972. This was the result of the union representing Swedish telephone operators bringing the issue of the invasion of privacy to the Minister of Justice.

In Canada, the only successful attempt to prohibit individual work measurement has been the contract clause found in the collective agreement between CUPW and Treasury Board (expiry December 31, 1982):

It is recognized that volume measurement is necessary to obtain an objective evaluation of the level of production of a group, a section or an office and there shall be no individual work measurement.

Another contract clause in the same collective agreement ensures that information obtained through surveillance cannot be used for disciplinary purposes:

The watch and observation systems cannot be used except for the purpose of protecting the mail and the property of the State against criminal acts such as theft, depredation and damage to property. At no time may systems be used as a means to evaluate the performance of employees and to gather evidence in support of disciplinary measures unless such disciplinary measures result from the commission of a criminal act.

Even with a guarantee of no individual work measurement, problems may still arise from management trying to raise productivity by using competition between different groups of employees. The definition of a group may also cause problems since it may be defined as two or more employees. The ideal solution is to negotiate a contract provision guaranteeing that no record of output can be used. Of course, this type of protective clause would not be applicable in workplaces which have bonuses based on individual productivity.

______________________________

A few other collective bargaining contracts (beside the Treasury Board example above) have included clauses banning electronic monitoring of individuals. Examples are the 1982 contract between the British Columbia Open Learning Institute and the British Columbia Government Employees Union and the Ontario New Democratic Party Caucus Workers' Agreement.

______________________________


In March of 1982, the Federal Minister of Labour appointed a Task Force "to examine the implications of microelectronics for all aspects of harmonious and productive industrial relations in Canada." The Task Force heard testimony from a wide range of interested groups -- employers, manufacturers of microelectronic technology, union, scientists, civic groups, etc. This testimony covered the full range of VDT issues, with Canadian unions raising the issue of electronic monitoring in their presentations.

A good example of this appeared in the Brief submitted to the Task Force by the Brotherhood of Railway and Airline Clerks, Airline Division, presented by Staff Representative Christine Micklewright:

**ELECTRONIC SURVEILLANCE**

Again, the introduction by CP Air of a new telephone system, was not considered to be technological change. There was no Union consultation and now that it's in place we discover that it has intensive electronic monitoring abilities.

I would like to take a few minutes to detail for the Task Force, some specific examples of the negative features of electronic monitoring in order to establish that our concerns are neither abstract nor imaginary but are, in fact, real events.

Employees must sign in and out of the telephone system, not just at the beginning and end of a shift but also for all breaks taken. As well reservations agents also sign into their VDT. The computer retains a daily record of each person's activities.

A complete record of an employee includes revenue production and a complexity of statistics relating to telephone calls handled. As well there is a sales programme and employees are exhorted to follow the format to the letter.
Deviation from the format has resulted in harassment and intimidation. One employee was the subject of so much pressure to produce according to format, that following numerous monitoring and tape recordings of phone calls, she finally passed out on the job and ended up hospitalised on a medical leave. Thanks to Union intervention, the mass of documentation was removed from her file but only after much resistance from the company.

Despite such blatant abuse of an employee, this type of harassment is continuing. Another employee recently confided to the Union that she had produced sufficient revenue in 1981 to place her in the top ten in the office - a total of a million dollars in sales - yet in the last six months she has become the subject of intensive monitoring and harassment. She is berated for failing to conform completely with the desired sales patter and has expressed fear that like her co-worker she will suffer a nervous breakdown. The employer has suggested to her that adherence to the sales patter could double her sales production. From being a proud and happy employee, her only objective now is to secure a transfer to another job within the bargaining unit. The cost of an unnecessary loss of such a valuable employee cannot be understated.

The employee told us that what the company really needed was robots, not human beings.

The issue of electronic surveillance will become a major item at the bargaining table. Just as the postal workers invoked their right to strike last summer over issues that included electronic surveillance so other Unions will be forced to take similar action against such dehumanisation of the workplace.

We strongly support the Convention resolution of the Communications Workers of Canada which calls for the prohibition of electronic monitoring to measure the productivity and performance of workers. Computers which have the ability to record for all eternity the smallest of clerical errors which become the subject of disciplinary action simply cannot be tolerated.
The Task Force issued its report in late 1982, under the title, *In The Chips: Opportunities, People, Partnerships*. It urged a comprehensive program of action, covering policies on industrial relations, quality of working environment, health and safety, women's issues, training and education, and research. Among its recommendations was that "Close electronic monitoring of work be prohibited as inconsistent with human rights legislation throughout Canada." In its detailed discussion of this proposal, the Task Force stated:

(iii) **Electronic Monitoring**

The most serious manifestation of the introduction of new electronic office equipment is its utilization to monitor the quantity of work performance. For example, we heard about the added stress on telephone operators — primarily women — who hardly ever have time to breathe, being caught in "endless loops" and being machine supervised to produce more. This type of electronic monitoring also attempts to place limits on workers' freedom to move around. They appear to be tied to their machines under the ever-watching and ever-recording devices.

The Task Force regards close monitoring of work as an employment practice based on mistrust and lack of respect for basic human dignity. It is an infringement on the rights of the individual, an undesirable precedent that might be extended to other environments unless restrictions are put in place now. We strongly recommend that this practice be prohibited by law.
The recommendations of the Task Force were submitted to the Minister of Labor, but proved to be too sweeping, too costly, and too "pro labor" for the Minister of Labor to endorse. In fact, the Report was expressly disavowed by the Minister, and no action was taken on its proposals.

4. Bills in Provincial Legislatures

Between 1981 and 1985, private member bills were introduced in the provincial legislatures of Ontario, British Columbia, and Saskatchewan to set ergonomic and work condition regulations for use of VDTs. The bill introduced by Richard Johnston, of the left-of-center New Democratic Party, contained the following provision:

"No employer of an operator shall use a terminal to monitor the productivity of an operator on an individual basis."

None of these bills were enacted.

* The 1983 Bill introduced by Mr. Johnston was Bill 83, "An Act For the Protection of Video Display Terminal Operators," Private Member's Bill, 3rd Session, 32nd Legislature, Ontario.
5. Continuing Union Advocacy and Public Discussion

During 1982-86, the issue of VDT work monitoring has been discussed at a series of national and local workshops, both those sponsored by union-affiliated groups and general conferences on work, privacy, technology, and industrial relations.

Typical of such meetings was a Workshop on Information Technologies and Personal Privacy in Canada, organized by the prestigious Science Council of Canada and held in Ottawa in October of 1984. Two presentations by union leaders at this Workshop provide both the current outlook of leading unions and information on the strategies they believe need to be followed to control electronic monitoring.

The president of the Communications Workers of Canada, Fred Pomeroy, reviewed developments since 1979 and then criticized current employer practices in work monitoring. In 1981 the Canadian Union of Postal Workers, Pomeroy pointed out, negotiated work measurement by group, prohibiting individual measurement. Canada Post had begun to introduce closed-circuit television equipment in 1974, installing systems in 26 major postal facilities as part of a billion-dollar program of technological improvement. The union also was successful in seeing that monitoring systems could only be used for the protection of mail and not for any disciplinary or work-performance evaluation of employees. In another agreement the Telecommunications Workers' Union was able to gain a commitment from the British Columbia Telephone Company that any data collected on computerized cash registers at Phone Marts could only be used for inventory purposes and not for individual work-measurement or performance evaluation.
Employee Surveillance

The main purpose for collecting this quantity and type of information, Pomeroy asserted, is to speed up and gain greater control of the work process. Frequently, a manager will sit down with a data-entry operator, a telephone operator or an airline-reservation clerk and say "you made 1,000 key strokes/answered 2,000 calls/sold $30,000 worth of tickets last week - let's set a new objective for you to improve that by 10% in future." With this kind of speed-up there is no end. As soon as the objective is reached, a new one is set. Pomeroy feels the quality of the work itself, and the health of the worker, suffer. Customers are not given the service they require, because the employee is not allowed to spend sufficient time on a call. The worker is more likely to make errors, and has been known to break down, under the increased pressure of surveillance.

Not only is this form of surveillance taking place for telephone operators, machinists, airline-reservation clerks and postal workers, it also has implications for those professionals working with computer-based systems. Lawyers, researchers and engineers can have similar data collected on them: the kind of searches they make, how long they spend on each, how many keystrokes they make, whether or not they made any errors, and so on, according to Pomeroy.

Another case, involving Air Canada,* resulted in upholding the right of the employer to monitor airline passenger service agents' conversations. It was ruled that the employee's right to privacy in this situation is not infringed by electronic eavesdropping equipment, providing the intent is for purposes of productivity and efficiency, not to cause emotional distress.

* Air Canada and C.A.L.E.A. (Simmons), unreported.
The second presentation was made by the staff expert from the Brotherhood of Railway and Airline Clerks. A story in the Toronto VDT Newsletter reported her presentation as follows:

Management control

Electronic surveillance threatens workers’ and customers’ privacy

Editor’s Note: The following article has been excerpted from a speech given by Christine Micklewright, Vice General Chairperson of the Brotherhood of Railway and Airline Clerks (BRAC), to a Science Council of Canada workshop on Information Technologies and Personal Privacy. The speech points out once again how work at a VDT can be misused, a violation of both worker and customer.

In the course of their duties supervisors listen silently to conversations of workers. Some conversations are taped and replayed during a performance appraisal. These workers are caught in a dilemma. If they file a grievance or protest this invasion of their privacy in some other manner, they draw further attention to themselves, and the details of the nature of their actions become the subject of office gossip.

Fortunately, union action identified that the new telephone system, which was voice activated, was a violation of the Privacy Act and consequently management was forced to revamp a system, that recorded every word spoken. We will never know the extent of private conversation surveillance but we have eliminated that particular ability of the system to record private conversations between employees, and learned a lesson for other workers in the future.

Workplace surveillance: Management right?

Telephone workers and airline agents work in a highly controlled environment where workplace surveillance is an assumed right of management. The surveillance of each worker begins the moment he or she signs into the telephone system. An account of the worker’s actions through the attachment of the umbilical telephone cord is recorded down to the second — the number of calls, duration, time between calls and time unplugged from the system.

It is fair to say that no manager would tolerate his business calls being secretly monitored by a superior, nor his bathroom breaks recorded. It is also fair to say that most management make personal phone calls during their working hours — a privilege that tends to be denied to their employees.

Surveillance leads to stress

The intensive and wide ranging nature of the surveillance now imposed on workers leads to tremendous stress on the job as workers are exhorted to increase productivity. There can be no doubt that such a working environment leads to health problems for some workers.

The use of computer terminals as a work tool also allows an employer to observe the transactions of an employee from some remote office. Such surveillance raises all kinds of fears about the privacy of electronic mail. The ability of one worker to communicate with another is frustrated by the lack of security.

Regrettably, the intense surveillance of workers by electronic means in an effort to quantify work fails to take into account the human aspect of work. There can be no real measurement of customer service; no real evaluation of whether a repeat customer was generated because of friendly helpful service; no real recognition that a worker’s smile brought business, never mind how fast or slow the employee worked. Quality is being replaced by quantity.
Another presentation at the Science Council Workshop discussed strategies that opponents of electronic monitoring could follow. After reviewing bargaining and legal developments, Ken Mazur argued that amending existing federal laws represents the most effective approach. Amendments to the following statutes he believes to be the most effective strategy: Employment Standards Act, Labor Relations Act and Human Rights Code. Specifically, Mazur suggests:

—The Employment Standards Act could be amended to cover electronic surveillance, but, he notes, "the only difficult part would be that there are no affirmative orders to correct specific violations;"

—The Labor Relations Act might be amended to cover non-unionized businesses as well as unionized firms; and

—The Human Rights Code could be expanded to cover electronic surveillance if the right to privacy were extended to the workplace.

Labor's success, it is argued, will be conditioned on greater public awareness of electronic-monitoring issues.

In 1985, the Co-Ordinator of Occupational Health and Safety for the Ontario Public Service Employees Union, Bob DeMatteo, brought out an expanded and updated version of a book he first authored in 1981, *Terminal Shock: The Health Hazards of Video Display Terminals*. DeMatteo linked close electronic monitoring to the filing of worker compensation claims for stress, and strongly endorsed the monitoring ban included in the International Labor Movement Guidelines on VDTs adopted by representatives from 14 international labor federations in Geneva, Switzerland in 1984. These said: "No video based system should be used to
While we are not aware of any public opinion data on how the Canadian public feels about individual worker monitoring, our strong sense is that this has not been an issue of major public interest nor has it been high on the political agenda of Canadian public affairs. The protests by Canadian labor leaders and intellectuals parallels that in similar U.S. circles in 1984-86, and, in both countries, has not produced legal action from governmental authorities.

One possible avenue for government examination of VDT work monitoring -- and other forms of worker monitoring -- in the next few years may be the current review and updating of the Canadian privacy law under way in 1986. There are informal reports that experts working on modernizing the Privacy Act may have specific language authorizing the Privacy Commissioner to examine electronic monitoring in the workplace, by making this a ground for citizen complaints. Since it is not clear yet how this move will proceed, OTA will want to stay in contact with the office of the Privacy Commissioner to obtain definitive information.
REFERENCES


8. Note 6 supra.

AUSTRALIA

The Law Reform Commission Australia (ALRC), established in 1973 by Act of Parliament, with reference to personal privacy was given the mandate to look into "the extent to which undue intrusions or interferences with privacy arise or are capable of arising under the laws of the Commonwealth or of the Territories, and the extent to which procedures adopted to give effect to those laws give rise to or permit such intrusions or interferences." The commission issued its report in June 1983. Among the main recommendations were the enactment of statutory privacy principles, creation of a permanent statutory Privacy Commissioner, formation of a Human Rights Commission, and "new legislation to control the use of devices for secret intrusion into privacy by (a) listening devices; and (b) optical surveillance devices."

New Threats To Privacy

The commission concluded that privacy in Australia is in danger due to growing official powers, new business practices and new information technology. In addition to new legislation, it called for administrative remedies for interferences on privacy, specifically:

a) conciliation and negotiation should be conducted by the Privacy Commissioner involving disputes in the public sector;

b) publicizing the names of "those who flagrantly or persistently violate privacy principles;" and

c) undertake a public education program so people will be aware of their information privacy rights.

The commission specifically addressed optical surveillance in public and outside public places among its recommendations:

- Public places: So far as public places are concerned, there should be no regulation of optical surveillance. For the purposes of legislation, a "public place" should be defined in the same terms as it is defined in police offences, summary offences and like legislation.
Outside public places. Outside public places the use of optical surveillance devices to observe people who could otherwise reasonably expect to be safe from observation should be prohibited. This prohibition should apply to all Commonwealth officers. It should also apply in relation to the Territories, by prohibiting optical surveillance by Territory residents, or of Territory residents. This prohibition should not be drawn in such a way as to protect wrongdoers who take steps to ensure that they are out of sight. Accordingly, where the surveillance device is used by a person for the purpose of observing what he had reasonable grounds to believe was the commission of an offence, the use of the device should be excused. Further, if the person using the device had reasonable grounds to believe that the use of the device was known to those whose activities were being recorded or observed, the use of the device should be excused.

Finally, there should be the overriding requirement that the particular use of the surveillance device was, in all the circumstances, reasonable. This should apply even if those observed or recorded knew about the surveillance device. The onus of proving these matters should be cast on the person using the surveillance device.

Intrusive Employment Practices

With respect to intrusive employment practices, the ALRC cited weaknesses in basic protection in Australia. "The weakness of the common law rules protecting the liberty and privacy of the individual from invasion by private security guards and agents also renders largely nugatory its protection in institutional settings, particularly that of employment. An intrusive interference with the person is not tortious where consent has been obtained. Consent in certain settings, while it might appear to have been voluntary, will very often not be real. The weaker party, whether a shopper, employee, applicant for employment or institutionalized person, will often not be in a position to deny a request to search property or person. Consent may be an appropriate bar to an action for assault, but it is not necessarily a bar to the invasion of privacy, especially in relationships of unequal power. When the search is of the investigator's property, such as a search by an employer or institution of a locker or desk drawer, the law is of no assistance to the person whose privacy has been invaded."

After describing how optical surveillance systems are used, ALRC asserts that "such practices constitute an invasion of human rights, including privacy." It further observes that "there is at present no legal prohibition upon secret optical surveillance (in Australia)." In the employment contacts, ALRC refers to a statement
by the Committee of Inquiry into Technological Change in Australia, in a 1980 report expressed concern at developing surveillance practices and recommended that "the parties directly involved in electronic systems that monitor individual employees should consult on appropriate standards to be observed."

**Official Guidelines Issued**

The Australian Public Services Board issued **Guidelines on Official Conduct of Commonwealth Public Servants** in August 1982. The guidelines state: "Unless exceptional circumstances apply, covert surveillance devices should not be used in relation to departmental staff, on the grounds of both privacy and good staff relations. Open surveillance methods should be used only where the overall public interest in efficient and economical administration or preventing the misuse of Commonwealth property and facilities outweighs the privacy and other considerations involved. Staff members and staff associations should be briefed on the purpose and use of any such system before it is introduced."

The ALRC report was submitted to the government in 1983, and as of February 1986 the comprehensive privacy legislation it recommended has not been submitted to parliament. Periodic statements from the Commonwealth Attorney General's office indicate that in due course a bill will be put forward. At the state level, however, New South Wales (NSW) established the Privacy Committee Act, that came into force on May 2, 1975.

The NSW Committee has four major functions: (1) research—to develop a general policy toward privacy and advise on particular issues; (2) complaints—to mediate on complaints of unjustifiable invasions of privacy; (3) public education—to act as a clearinghouse for information privacy issues and to stimulate informed public data debate in this field; and (4) recommendation—of changes in the law and administrative and business practices. Although it has authority to mediate disputes, the committee has no power to enforce its recommendations. After nearly a decade of operating without enforcement power, the committee in 1984 urged the government to revise the act, giving it such authority.

In March 1980 the committee issued a background paper on the use of electronic monitoring of telephone calls. The research focused on "employing computers to keep a record of the details of telephone calls made from particular extensions, including the originating extension, the time of day, the duration of the call, the number of the call, and cost of the call." It pointed out five main purposes for
operating such systems: (a) cost allocation between different parts of an organization; (b) control of staff personal calls; (c) system design and management; (d) correction of telephone misuse; and (e) checking on reasonableness of non-itemized charges. After the completion of the paper, the committee issued a set of guidelines to apply to this type of equipment, covering: collection of the minimum necessary data; care in supervision of business calls; recording only the duration of personal calls; security and destruction of the data generated; prior consultation with staff and warning that the system was connected.

Some aspects of the guidelines were objected to by the Labor Council of NSW as inadequate. The Council opposed all use of telephone-surveillance devices.

**Typical Employee Monitoring Complaints**

The NSW Committee's Annual Reports contain accounts of typical complaints. Among the examples provided from 1975 to 1984 are the following:

(a) **Recording telephone conversations for training purposes** (1978). A company wished to measure how effectively its staff dealt with complaints from the public. People ringing in were asked whether they objected to the conversation being taped "for training purposes" and advised that if they did object no recording would be made. Most people did not object and the recording was then listened into by the supervisor and, if appropriate, discussed with the staff member. After discussion the recording was erased.

The Committee had no objection to this procedure particularly as the staff were advised of its existence.

(b) **Control of abuse of Subscriber Trunk Dialing (STD) facilities** (1978). Some large organizations have installed a device which can be attached to particular extensions and will record the time of the making of the call, the area code and the telephone number, suppressing the last two digits and the period of the call. Without the last two digits there is adequate information to request particulars of the call to ensure it was for business purposes without being able to check within the 100 possible numbers as to who the actual recipient was.

Provided staff are made aware of the existence of the system the Committee has no objection.
(c) Objections to an Intercom (1979). Is surveillance of employees unreasonable? This was the issue put to the Committee by a union representing employees engaged in collecting money from the public. The employees objected to their surveillance by an intercom system, especially as they were already monitored by television cameras. They felt that the intercom, which was operated without warning, made life on the job too intrusive.

The employer informed the Committee that the intercom was required to supplement the camera surveillance and make doubly sure that any money collected was not diverted en route to the till. The intercom also helped to enforce a rule that collectors must not converse with their fellow employees.

Whilst the Committee was sympathetic to the need to prevent misappropriation of funds, it also considered that employees were entitled to know when they were being monitored. The Committee recommended that a warning should be given whenever the intercom was in use so that employees would not feel that the employer was out to trap them. This would still enable the intercom to be used to supervise the collection of money.

The employer agreed to install a flashing light to indicate when the system was in use.

(d) Surveillance of Staff by Television Cameras (1981)

In our background paper on employment, the Committee set out its concerns about surveillance of employees by various methods and particularly secret surveillance. In this instance, the employer quite openly introduced television cameras primarily to prevent or observe burglaries in a highly sensitive area. The Union involved, and the Committee, had reservations as to the value of the system, but in view of the fact that the Union had not objected, and of the highly sensitive area subjected to scrutiny, the Committee did not recommend removal at this stage.

The Committee did, however, stress to the industry its concern that unnecessary surveillance systems should not be installed. Individuals do not like to be subjected to surveillance by mechanical or electronic methods, particularly where they are not aware who might be observing them at any particular time. The Committee will closely observe installation of such systems and request employers to discuss proposals with the Committee in advance. The Committee would also be interested to hear from unions or employees about current or proposed systems.

The Committee notes with interest the continual monitoring of diamond sorting, proposed in Western Australia.
A film studio connected a recording device to record all conversations between producers, sound, film crews and other employees involved in a production to isolate co-ordination problems and correct them. The union involved did not object to this but rightly objected to it being connected without the knowledge of or prior discussion with the staff. The company apologised for its lack of consideration. It was agreed that the recordings would be kept in a secure place and only used where there was a specific problem which required solution. They would not be used for spot checking of conversations between employees and would be erased after three months. A switch was also installed so that, at an appropriate time, employees could have a private discussion without its being recorded.
Trade Union Activities

Australian trade unions have paralleled the British unions in assailing the negative impacts of new office and factory automation on workers and the workplace. Bill Richardson, General Secretary of the Australian Council of Salaried and Professional Associations said that current automation practice had three main consequences: it destroys jobs, deskills and degrades the jobs that remain, and is designed to increase managerial control, through worker monitoring.*

In early 1986, the Australian Bank Employees Union wrote the Australian Attorney General asking for the national government to take action on "the ever increasing use by employers of data on their employees, and particularly on the automatic collection of data permitting the monitoring of individual work performance and workplace behaviour." The ABEU forwarded a copy of the November, 1985 FIET Guidelines on "Personnel Data Collection and Processing Systems," which call for such monitoring to be legally prohibited.**


Complaints relating to employee surveillance were not sustained after 1982 becoming less technology related, as reported by the NSW committee. These were of two types: (1) intrusive questions on employment application forms, such as frequency of church attendance, how earnings are spent, political party affiliation, and disclosure of assets and liabilities; and (2) complaints about staff evaluations, access to medical examination results and requests for details on reasons given for dismissal from previous jobs. Employee-management differences over collection, handling and access to personal information, however, remained an active source of complaints throughout the nine hear period.
Australia

Notes


3 Ibid, page LXI

4 Technological Change and its Consequences, Committee of Inquiry into Technological Change in Australia, Report Volume I, para 7.216 (1980).


PART IV
FAR EAST DEMOCRACIES:
JAPAN
JAPAN

Popular Attitudes Toward Privacy

As already noted, and contrary to assumptions among many Western observers, national public opinion surveys show that Japanese society and its leaders now hold concerns about invasion of privacy and register support for data protection measures at levels similar to those in Western OECD nations. In July of 1985, a representative national survey of 3,000 men and women aged 20 or over (a successor to a 1976 privacy survey) produced the following findings:

- 1985 poll: 61% interested in protecting privacy and 25% not interested. In 1976, only 25% said they were interested in protecting privacy.

- 1985 poll: 48% believe cases of privacy violation are on the rise, and 34% do not. In 1976, only 31% believed violations were on the rise. While 71% in 1985 believe such privacy violations will increase in the future, only 57% thought so in 1976.

- 76% of respondents in 1985 believe there is an "urgent need" to take "appropriate measures to keep personal information under protection."

In the detailed sections of the survey, Japanese respondents complained about the flood of direct mail they were being subjected to; inaccurate information circulated about themselves and their families; and collection of personal information "by outsiders" without their knowledge. Information respondents felt it was important to secure privacy protection for included: "annual income, personal property or assets, and the amount of taxes they were paying"; family life; and political or religious creed. While 51% of respondents in the 1976 survey said they had no particular personal information they wanted to keep secret, this percentage dropped to 40% of respondents in 1985.
In the questions relating to computers and privacy, Japanese respondents shared the generally positive attitudes towards information technology voiced by respondents in most OECD nations. 85% of Japanese respondents in 1985 said the computer makes work and daily life easier, and 78% said computers were "indispensable" for modern life. However, 51% said there was danger of private life being violated by the spread of computers, and 69% believe that increasing computerization would increase violations of privacy.

No questions about privacy at work or of surveillance/monitoring of employees were asked in the 1976 or 1985 surveys, or on other national surveys about privacy conducted over the past decade.

**Attitudes Toward Privacy Protection Measures**

As of early 1986, there is no national privacy protection law in Japan, comparable to European data protection statutes or the U.S. Privacy Act of 1974. However, over 125 Japanese cities and towns have passed privacy ordinances on protection of municipal data (which are among the most sensitive in terms of containing citizen and family data).²

Since 1974, reports by the Administrative Management Agency (AMA) of the Prime Minister's Office have discussed privacy protection and stated that this could become an issue in Japanese life.³ In 1983, the AMA issued a thoughtful report enunciating principles for national legislation;⁴ this followed issuance of privacy-oriented findings by a 1982 Committee on the Protection of Privacy (chaired by Professor Kato of Tokyo University).⁵

During the 1970's and early 1980's, there were public discussions of privacy concerns over computerization of family registers; automation of the
"Green Card" for savings accounts; access by patients to their own medical records; creation of automated alien registration files; and creation of a citizen identification number. Again, no public discussion dealt with employee monitoring. Misuse of credit information was highlighted with a well-publicized story in May, 1983 of the leak from a credit data bank ("Japan Data Bank") of debt information about two television directors, and the subsequent harm done to their lives. This incident helped dramatize the dangers to persons when personal data are released improperly.6

How Japanese saw government protection of privacy interests was captured in a 1981 national public opinion study sponsored by the AMA.7 It found that while Japanese citizens were very positive toward computers and their improvement of life, they were also concerned about collection of too much personal information and how it might be used, especially by government agencies. The poll found very strong support for "measures" to be taken to protect privacy in the public and private sectors. Support in the 84-94% range was expressed for requirements to obtain approval to collect personal information; to forbid uses other than the purposes for which collected; to give individuals a right of access and correction; to create an "inspection institution" for databanks; to compensate individuals for violations of personal privacy; and (by 76%) to provide criminal punishment for violators.

Worker Monitoring in Japan

Sources from both employers and unions agree that employers in Japan do not make it a practice to collect performance statistics on employees and use these for compensation, discipline, or termination purposes. Japanese unions replying to a FIET questionnaire on privacy at the workplace reported the situation as follows:8
Some Japanese companies operate personnel information systems which include:

1. Payroll records.
2. Listing of qualifications held.
3. Inhouse service records.
4. Listing of applicants for relocation.

The union's view is that data is used for reassignment of workers, and for education and training. In almost no case is it used to the disadvantage of workers e.g. by measuring work speed or error rates. The main exception to this is attendance records. Although these records are collected primarily to calculate overtime payments, it is clear that a consistently poor attendance record will affect an employee's efficiency rating. No action has so far been taken by unions to regulate these matters.

Interviews conducted in 1985 at one large Japanese affiliate of an American computer firm confirmed this judgment. A Japanese staff expert fully familiar with the practices of Japanese industrial and service companies remarked:

Individual work monitoring is not an issue in Japan. Employers do not measure individual output and make individual judgments on that basis. If they tried to do that, unions would complain, because it would violate the union-company attitude toward worker productivity. The climate in our workplaces is for employees to work hard, and for the whole work group -- employees and managers -- to strengthen the norm of hard work. We would not measure each person.

In fact, the only example of Japanese employers counting keystrokes of individual workers involves a very different purpose and use than the typical monitoring situation. In the early 1960's, key punch jobs in new data processing operations became very desirable work, especially among young women. EDP was seen as a critical industry of the future, and very important for the Japanese national interest. However, a wave of repetitive strain injuries (RSI) broke out among Japanese keypunchers, based on the high number of keystrokes being performed daily and working conditions at the key equipment.

Some companies (including IBM-Japan and UNIVAC-Japan) set voluntary guidelines to limit the number of daily keystrokes, and the Japanese labor
federation covering this area of work (SOHYO) also proposed guidelines. In 1964, the Japanese Ministry of Labor (MOL) issued Guidelines (representing a compromise between the employer and union standards). These set a maximum of 12,000 keystrokes an hour for keypunchers. To enforce these guideline limits, employers could and did conduct test monitoring of individual-worker rates and totals.

The 1964 MOL Guideline also set keypunch working time at a maximum of 300 minutes a day; required 10-15 minutes an hour rest period for all workers in the same work room at the same time; set standards for noise, lighting, temperature, and space in the work environment; and called for medical examination prior to assignment for key punching, with periodic checks thereafter (yearly).

The "voluntary MOL guidelines" of 1964 were widely followed in Japan. They are currently being used as a model for "consensus" building by industry, labor, and government for similar MOL guidelines to be issued in 1986 for VDT work. 10
FOOTNOTES


5. Note 2, supra.

6. Note 3, supra.

7. Ibid.


10. Information compiled by Alan F. Westin, from interviews with industry, legal, and academic experts, Tokyo, May, 1985.
PART V
INTERNATIONAL TRADE UNION ACTIVITIES
International Trade Union Activities

The international trade federations that have been demonstrating the greatest activity and are most directly concerned with issues of work monitoring are the International Federation of Commercial, Clerical, Professional and Technical Employees (FIET) and the International Confederation of Free Trade Unions (ICFTU). The two international unions have conducted surveys, prepared studies and held conferences on computerized personnel information and work monitoring. They have urged the International Labor Conference, the annual meeting of the International Labor Organization (ILO) to take up these subjects and consider adopting appropriate international labor standards to address them.

ICFTU Position

The ICFTU brought its concerns to the attention of the UN Commission on Human Rights Subcommission on Prevention of Discrimination and Protection of Minorities at its 38th session in 1985. As a result of circulating draft guidelines for the regulation of computerized personal data files, ICFTU found strong support for such action by the Commission. The following is an excerpt from a statement by Oscar de Vries Reilingh, Director of its Geneva office:
Our interest in the subject relates, of course, in particular to the use of computerized personnel data systems, i.e. data relating to employees collected by their employer, as distinct from personal data systems in general, which include the first type of data systems but go much wider to cover any data relating to individuals collected by any institution for any purpose. It is indeed very fortunate that the Special Report has clarified this distinction in his introductory statement and that the English title of the draft guidelines has been modified accordingly.

The importance of the protection of data privacy in respect of computerized personnel files is growing because of three factors, namely:

- the increasing use of cheap data processing hardware by small and medium sized enterprises, in addition to the large ones;

- new developments in data base software which makes it easier for users of such systems to change their requirements for information after the system has been set up rather than having to build all such requirements into it from the beginning;

- the growth in new automated methods of collecting data on the performance and behaviour of individual employees, such as telephone monitoring and the use of badges and identification cards to control movements.

General laws on the protection of personal data are very necessary to preserve individual liberties in the face of the increasing use of computer data bases. The regulation of personnel files through such legislation alone is, however, very difficult, because of the need to be specific enough to cover all aspects of data collection, processing and the use at the level of the individual enterprise or workplace. In a number of countries the legislation therefore provides for the right of worker representatives to be involved in the regulation of personnel files within the overall legal framework. In many instances this right is further elaborated in collective labour agreements between the employer and the trade union or unions concerned, regulating the establishment and operation of and changes in computerized personnel information systems and recognizing the principle that not only the individual should have the right of access to and correction of data in a file, but that the trade union or unions involved should have a collective right to monitor the use of computerized personnel files and to approve any modifications made to them.
A clear example of the importance of regulating certain aspects of the protection of data privacy in respect of personnel files through collective bargaining and the conclusion of collective labour agreements is the provision in the draft guidelines which prohibits the storage of information on trade union membership. Such a prohibition would run counter to the practice in several countries, both developed and developing, to have check-off arrangements at the enterprise level, i.e. arrangements through which the employer deducts trade union dues from the wages and transfers these dues to the trade union or unions concerned. In such cases it is absolutely crucial to store information on trade union membership in the data files. Quite naturally, we agree that employers should be prevented from collecting information in order to use it to discriminate against unionized employees. However, it is almost impossible to define in legislation when it is and when it is not necessary. This underlines the need to allow special regulations through collective labour agreements which would be best adapted to the requirements in each individual case.

The proposed draft guidelines are necessarily of a general nature. We therefore strongly support the suggestion in the report that the general principles could be supplemented by so-called "sectoral rules" for activities involving special risks and that the ILO should draw up appropriate guidelines concerning personnel files. As a matter of fact, this idea was again included in a resolution adopted by the ILO Advisory Committee on Salaried Employees and Professional Workers, adopted last April, and in a resolution presented by ICFTU delegates to the last ILO Conference in June this year which, unfortunately, could not be taken up due to lack of time.

As I have already stated, the ICFTU supports in general the revised draft guidelines as presented by the Special Rapporteur. In this connection, I have only two specific remarks to make:

- we hope that it is clear that, under the principles of fairness and of accuracy, the employee, who is responsible for the operation and maintenance of the personal data files, should be guaranteed the right of non-compliance when the employer orders the employee to carry out unlawful activities in connection with these data files;

- under the principle of interested-person access, we would prefer that the phrase "if the need arises" be deleted as it would unduly qualify the strength of this principle.
FIET ACTIVITIES

The International Federation of Commercial, Clerical, Professional and Technical Employees (FIET), composed of unions in 90 countries with a combined membership of 8.3 million, has demonstrated a keen interest in applying privacy restrictions to the collection and use of personnel data. In November 1985 FIET organized an International Trade Union Conference on Personnel Information Systems, attended by delegates from 27 FIET-affiliated unions in 12 countries. A background report described its position "that an effective response is required to meet the specific and growing problems presented to workers by the operation of personnel information systems."

Intrusive Practices Identified

This response, FIET indicated, should go beyond the provisions of the OECD guidelines and Council of Europe convention. A particular concern identified is the "possibility that advanced computer technology may be used to collect additional (personal) information which does not traditionally enter personal files but which can now easily be correlated with such data." Four categories were identified:

a) automatic collection of information on attendance and work performance;

b) telephone monitoring;

c) security-system monitoring;

d) electronic payment systems used to trace employee buying habits.

On the latter point an example given related to a worker being reprimanded for absenteeism after a payment record showed he had purchased seven beers the previous lunchtime in the company canteen.

Risks of Monitoring Misuse High

With respect to automatically collected information, the report notes that word processors, numerically controlled machine tools, point-of-sale systems and other computer-driven devices permit the collection of large quantities of data personally identifying individual employees. On the one hand this is "justified by reference to the need to avoid misuse of systems and breaches in confidentiality." On the other, however, "it also makes possible the collection of information on such matters as: time work began; time work finished; length of rest pauses;
number of key depressions per minute; number of error corrections made, all of
which can be recorded automatically against each employee's name. This permits
much closer supervision and control of individual attendance and performance than
is possible with manual systems. Some systems now in operation make it impossible
for an operator to leave a machine without specifying for the machine's records
the precise reason for the pause. This may well be in the interests of cost-
effectiveness for the employer. It is certainly not in the interests of a humane
work environment."

FIET recognizes that there are acceptable uses for such electronic monitoring,
such as to make it possible for employers to know the reasons for periods of
inactivity in a factory or office so that efforts can be made to eliminate
bottlenecks in the supply of work elsewhere. Equally, information on work speeds
and error rates in theory can be used to identify areas where employees have
an excessive workload and where additional personnel are needed. Unfortunately,
these are not the most common applications of this type of work-related data.
More often it is used to classify employees as above—or below—average
performers, to fix salaries, to influence promotion prospects, etc. It can also
sometimes be used to determine salary levels directly (as in payment-by-results
systems) or to justify disciplinary action taken against employees for bad
attendance or unsatisfactory work performance.

Limitations on Monitoring Urged

FIET believes a number of conditions should be sought by trade unions, to
ensure that monitoring is fairly conducted:

1) that no personal data should be collected automatically by machines without
the knowledge and express approval of the works council/unions;

2) that a complete specification of the programs to be used in connection with
any computer-based equipment should be furnished to worker representatives,
together with similar details of any subsequent amendments to such a program;

3) that the purposes for which automatically collected data are to be used
should be agreed in advance with the union/works council;

4) that a timetable for the erasure of automatically collected data should be
agreed.
Telephone monitoring

With regard to telephone systems, FIET points out that "computer-controlled telephone switchboards can be used to monitor the personal use of telephones by members of staff and to prevent unauthorized personal use." There can be a "significant degree of stress for employees," the report continues, "if they know that every telephone call is being monitored and that they may be called on to justify calls made. On occasions trade-union representatives have found employers using such systems to invoice their union for calls made on union business. Where such systems monitor not just external but also internal communications they can be used also to monitor normal social contacts between work colleagues and to detect any signs of worker discontent which results in abnormal patterns of telephone use. For all these reasons trade unions should insist on strict controls on telephone monitoring systems. Unless they are essential for invoicing purposes, systems which identify the destination of calls made by individual employees should be banned. Only aggregated data should be stored for any length of time."

Security systems

Security systems, by using access/devices, allow management to know where employees are within a facility. FIET observes that such devices can not only be used to prevent authorized personnel from entering certain areas, but also trace the movements of all personnel. "The potential for such systems for disrupting trade-union organization within the enterprise has certainly not escaped many employers," the federation concludes.

Electronic payment systems

Magnetic and microprocessor-based cards used in company canteens and for other purposes can be a monitoring device, FIET claims. "Unscrupulous employers," the union argues, may use information collected about employee purchases against them, as was noted in the incident cited earlier.

FIET personnel data guidelines

Guidelines on Personnel Data Collection and Processing Systems, distributed by FIET at the conference, are "intended as an aid for trade unionists engaged in
negotiating collective agreements on the introduction and operation of personnel data collection and processing systems." (Appendix A) The guidelines stress the full involvement of workers' representatives in planning and operation of information systems that collect data or can otherwise be used to monitor employees. Addressing automatic data collection, the guidelines state: "The automatic collection of data in a manner that would permit the monitoring and recording of individual employees' work performance or workplace behavior should be strictly forbidden. It is unacceptable that the application of EDP techniques in the workplace should be used to collect information, for example, on individual work patterns and error rates, or on normal social interaction in the workplace. If an employer can show a legitimate need to collect automatically data on output and productivity, workers' representatives should insist that such information be capable of being handled only on an aggregated basis so that it is impossible to break down and attribute data to the behavior or performance of individual employees. In this way employers should be prevented from using automatically collected data as the basis of decisions in respect of discipline or promotion."

Surveillance Conditioned on Agreed Practices

No telephone monitoring system should be put into operation "which is capable of recording the origin, destination or duration of individual calls by or to employees." Direct interception and recording of calls by management, FIET states, should be strictly forbidden.

Employers who prove a legitimate need to control the movement of employees may do so but where electronic devices are in operation "workers' representatives should ensure that their use is restricted to meeting well-defined and agreed security needs, and not exploited as a pretext for the establishment of a general system of surveillance of employee movements." However, "data no longer required to meet agreed needs should be immediately erased."

In a statement issued at the conclusion of the conference, the participants:

—welcomed OECD, CoE and UN data-protection initiatives and "strongly emphasized the pressing need to extend protection of internationally recognized basic human rights at the workplace itself";
—called on the ILO to "make a crucial contribution", through the elaboration and adoption of a convention on personnel data processing;
—reiterated the view that "the automatic collection of data permitting the
monitoring of individuals' work performance and workplace behavior should be legally prohibited;" and

—stressed that "legislation alone was unlikely to offer sufficient protection to employees, and needed to be complemented by trade union or works council involvement in the control of personnel data collection and processing."

Notes


2
INTRODUCTION
These international trade union guidelines are intended as an aid for trade unionists engaged in negotiating collective agreements on the introduction and operation of personnel data collection and processing systems. They may be regarded as complementary to the FIET Model Technology Agreement published in 1983 which sets out in 40 clauses the general, procedural, and substantive issues with which trade union negotiators will have to deal in the field of technology. Most of these principles are fully applicable to the specific case of personnel data collection and processing, and are not repeated in these guidelines which may, therefore, be used most effectively in conjunction with the model agreement.

1. GENERAL
The basis for negotiations between an employer and workers' representatives should be a commitment that no innovation in respect of personnel data collection and processing should be implemented without agreement between both parties on all aspects of its introduction and operation. Until such agreement is reached no modification of existing arrangements should be made.

2. SYSTEMS SPECIFICATION
Workers' representatives should be fully involved, from the earliest planning stage, in innovations in all areas of electronic data processing. All relevant information should be made available by the employer, in intelligible form, on the specifications of the software packages, and the overall capabilities of the systems under consideration.

3. TYPE OF PERSONNEL INFORMATION TO BE COLLECTED, STORED AND PROCESSED
The categories of personnel information which the employer is permitted to collect should be set out in the collective agreement. On no account should the employer collect any type of information other than those listed.

4. PURPOSES FOR WHICH INFORMATION IS HELD
The precise purposes for which information is to be held and used should be specified in the agreement. Workers' representatives should ensure that they are restricted to directly work-related issues and legally prescribed objectives.

5. MINIMUM DATA VOLUME
The volume of data stored should be kept strictly to the minimum required for the attainment of the agreed objectives. Provision should be made for the regular erasure of material which is surplus to that requirement. The time intervals agreed for erasure will depend on the nature of the data, but particular attention should be given to the case of employees' disciplinary records.
6. AUTOMATIC DATA COLLECTION
   The automatic collection of data in a manner that would permit the monitoring and recording of individual employees' work performance or work place behaviour should be strictly forbidden. It is unacceptable that the application of EDP techniques in the workplace should be used to collect information, for example, on individual work patterns and error rates, or on normal social interaction in the workplace. If an employer can show a legitimate need to collect automatically data on output and productivity, workers' representatives should insist that such information should be capable of being handled only on an aggregated basis so that it is impossible to break down and attribute data to the behaviour or performance of individual employees. In this way employers should be prevented from using automatically collected data as the basis of decisions in respect of discipline or promotion.

7. COLLECTION OF INFORMATION
   The general principle that information should be legally and fairly obtained should be strictly observed. Information should be obtained only in ways known to, and agreed by, employees.

8. THE ACCURACY OF INFORMATION
   It should be established that the full burden of responsibility for the accuracy of data held should rest with the employer who, equally, should be liable in respect of any adverse consequences for an employee arising from inaccuracies. The employer should also be responsible for ensuring that data is up-dated with sufficient regularity.

9. EMPLOYEE ACCESS TO PERSONAL RECORDS
   Every employee should, at any time, have the right of immediate access to all data held on him, or her, at no personal expense. Workers' representatives should also secure agreement that a full print out of each employee's data file should be made available to him or her routinely at regular intervals.

10. RIGHT TO CORRECT DATA
    Any employee who finds, on inspection, that data held on him or her is inaccurate should have the right to have erroneous items corrected.

11. LIMITATION OF ACCESS TO DATA
    The right of access to the personal files of any employee should be limited to a minimum number of individuals named in the agreement. They should be identified on the basis of the strict requirement of their job responsibilities.

12. SAFEGUARDS FOR DATA SECURITY
    In negotiating the specifications of the personnel data collection and processing systems to be introduced workers' representatives should ensure that the system selected incorporates sufficient technical and organisational safeguards against access by any person other than those authorised in the agreement. In addition, any data run carried out in respect of an individual employee should be recorded with details of when it took place.
and on whose initiative. Information on such data runs should be made available to the individual concerned on request.

13. TELEPHONE MONITORING
Workers' representatives should insist that no telephone monitoring system should be put into operation which is capable of recording the origin, destination, or duration of individual calls by, or to, employees. Direct "listening in" on calls should be strictly forbidden.

14. AUTOMATIC MONITORING OF EMPLOYEE MOVEMENT
Employers may be able to prove a legitimate need to control the movement of employees, particularly for security reasons and when access to some areas is restricted. Such control is increasingly achieved by the use of personal identity cards or badges. Where such devices are in operation, workers' representatives should ensure that their use is restricted to meeting well defined and agreed security needs, and are not exploited as a pretext for the establishment of a general system of surveillance of employee movements. Provision should be made for the immediate erasure of data no longer required to meet agreed needs.

15. COMMUNICATION OF INFORMATION TO OUTSIDE PARTIES
The communication of personnel data to outside parties should be strictly prohibited. Any possible exceptions to this principle should be set out in the agreement and take place only with the consent of the employee concerned. The employer may also be legally required to disclose information to third parties.

16. PROVISION OF TRAINING FOR WORKERS' REPRESENTATIVES
Effective control of personnel data collection and processing systems in accordance with the terms of these guidelines requires that workers' representatives are in possession of sufficient technical knowledge to enable them to understand fully the working and capabilities of the system in question. Therefore, agreement should be reached that such representatives should attend appropriate EDP training courses at the expense of the employer. It is important that this training should be undertaken at a sufficiently early stage in the process of the introduction of any system to allow representatives to participate meaningfully in consideration of its specifications. Trade unions should also give attention to meeting education and training needs arising from personnel data questions.

17. RIGHT OF INSPECTION
The provisions of any agreement are liable to remain a dead letter unless they can be effectively enforced. Therefore a right of inspection of the operation of personnel data collection and processing systems should be included in the agreement. This should provide that designated workers' representatives or, on their request, members of an independent data inspectorate, should have the power at any time, and without previous notice, to examine the functioning of a system. They should be guaranteed free and unrestricted access to all aspects of the system and be able to report their findings to the relevant works council, trade union, or, where appropriate, data authority.
PART VI

INTERGOVERNMENTAL ORGANIZATIONS:
UN, ILO, AND COUNCIL OF EUROPE
The intergovernmental organizations that have expressed an interest in employee privacy and/or worker monitoring have done so because of their mandates in human rights or labor-management relations and working conditions. The early and continuing leadership on the field of personal data protection by the Council of Europe, strongly supported by many member states, clearly influenced the UN Commission on Human Rights initiative in this field. The Council of Europe (CoE), a regional body with 21 member countries, was established in 1948 to implement the European Convention on Human Rights. Beginning in the early 1970s the CoE Committee on Legal Affairs took up how personal privacy may be affected by the introduction of computerization in member countries. This led to two recommendations on how the public and private sectors should treat personal information and finally in 1981 approved a legally binding convention on the subject which came into force in October 1985.

The UN Commission on Human Rights has been concerned about how science and technology have been affecting human rights since 1967, and first took up the question of whether special attention should be given to the computerization of personal records in the mid-1970s. The matter has been under consideration by the Subcommission on Prevention of Discrimination and Protection of Minorities since 1982. Louis Joinet, a French magistrate, former chairman of the Council of Europe Committee on Data Protection, was asked to prepare Draft Guidelines for the Regulation of Computerized Personal Data Files. This report was approved, with modifications, at the subcommission's 1985 session. It is being distributed to UN members and should be ready for final consideration when the subcommission meets next year. If approved, the guidelines would be submitted to the full Commission on Human Rights and then the UN General Assembly.

The importance of employee information privacy and worker monitoring being considered human rights issues subject to international guidelines and codes governing acceptable behavior and national legislation, is that they cast these issues in a moral and ethical context. Proponents of extensive employee rights vis-à-vis applications of information technology by management can exploit endorsements by human rights organizations to demonstrate the rightness of their case.
The International Labor Organization (ILO), a UN agency with some 144 member countries, has a 65-year record of "promoting international action aimed at achieving full employment, the raising of living standards and improvement in the conditions of labor." The means of collection and uses of employee information are within this official ILO purpose statement. However, employee privacy is only one of a host of issues that face this organization. The communist bloc and a number of Third-World countries show little interest in such issues. On the other hand, if and when an ILO policy statement is negotiated at the full International Labor Congress, this could boost the unions which have been in the vanguard of establishing controls over information technology in the workplace.
UN COMMISSION ON HUMAN RIGHTS

The UN General Assembly in December 1968 (Resolution 2450(XXIII)) asked the Secretariat and other agencies to study "uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society." The Commission on Human Rights, Subcommission on Prevention of Discrimination and Protection of Minorities, undertook a study into whether "guidelines in the field of computerized personal files"\(^1\) should be adopted by the full Commission and possibly by the General Assembly itself. The study was prepared by Special Rapporteur Louis Joinet of France, who participated in drafting the French 1978 Act on Data Processing and Liberties, and served for a term as chairman of the CoE Data Protection Committee.

**Draft Guidelines for Personal Files**

The study's conclusions were endorsed by the subcommission in 1983, and the provisional draft guidelines were adopted at its 1984 annual session. The UN Secretary General, however, was requested to transmit the guidelines to all member states and relevant international organizations for comment. Revised guidelines, taking into account suggested amendments, were approved by the subcommission in August 1985.\(^2\) The guidelines contain many of the principles embodied in the CoE convention, with the addition of a principle of non-discrimination. No enforcement mechanism was proposed to supervise their eventual implementation.

Among the suggestions received by the subcommission was that the "possibility should be left open for supplementing its general principles by 'sectoral' rules." One sector "involving special risks" was identified as personnel files. The International Confederation of Free Trade Unions (ICFTU) in a statement on the guidelines stressed the importance of protection of data privacy with regard to computerized personnel files, because, among other reasons, "the growth in new automated methods of collecting data on the performance and behavior of individual employees, such as telephone monitoring and the use of badges and identification cards to control movements of employees."

**Final Approval in 1986**

The period for comments and suggestions from governments and international bodies has been extended into 1986 when the Special Rapporteur is to integrate them into a final report. The subcommission is expected to complete consideration of the guidelines at its 39th session scheduled for August 1986.
Notes


INTERNATIONAL LABOR OFFICE (ILO)

At the urging of the International Federation of Commercial, Clerical, Professional and Technical Employees (FIET), the International Labor Office's Committee on Salaried Employees and Professional Workers meeting in Geneva during April 1985 adopted a resolution on "Personnel Information Systems and Data Privacy in Commerce and Offices". The resolution invites the "Governing Body of the ILO to request the Director General to carry out studies with a view to establishing, in consultation with other appropriate United Nations agencies, a compendium of principles and good practices for safeguarding the rights of individual workers at the enterprise level."

Compendium of Principles Asked

A resolution along similar lines was introduced at the 1985 ILO Conference in May 1985 but not debated or adopted due to time limitations. Its operative provisions, in addition to (1) calling for studies on problems concerning the collection, storage and use by employers of individually identifiable data relating to their employees, also calls on ILO to (2) organize a tripartite meeting of experts to prepare rules and guidelines governing the regulation of data privacy at the workplace; and (3) include the question concerning regulation of computerized personnel information systems and data privacy in the agenda of a forthcoming session of the annual ILO Conference.

Possible New Standards

Within the current review of the Working Party on International Labor Standards of the classification of existing Conventions and Recommendations the ILO's Governing Body, at its 232nd session (March 1986), included in its draft revised classifications of standards two items under the Industrial Relations topic as possible subjects for new international instruments: (i) Standards on the protection of workers in matters of discipline; and (ii) data protection of workers. The item was included on the suggestion of the Worker members of the Working Party. The Employer members considered that this subject might be regarded as an aspect of conditions of employment. The draft will be discussed at the November 1986 session of the Governing Body.
Technology Threats Raised

The ILO Secretariat supports such projects, if the organization's press office and official publications are any guide. *ILO Information* (October 1985), the monthly bulletin of the organization, carries headlines "electronic spies threaten workers' privacy," explaining that "there's basically nothing wrong with those technological wonders which boost productivity, tighten security or help end boring work. The trouble starts when they are used to spy on workers, invade their privacy and divulge personal data to anybody who presses the right key." These statements are offered by way of introducing the ILO publication *Technological Change: The Tripartite Response 1982-1985*. It is a compilation of studies and country reports on the impacts of computerization—illustrating the technological dilemma facing the world due to computerization.
1 Text of resolution concerning follow-up to 1978 Compendium of Principles and Good Practices relating to the Conditions of Work and Employment of Professional Workers.

Resolution on personnel information systems and data privacy in commerce and offices

The Advisory Committee on Salaried Employees and Professional Workers of the International Labour Organisation,

Having met in Geneva, in its Ninth Session, from 17 to 25 April 1985,

Observing the growth in the use by employers of computerised systems for personnel management in certain countries,

Observing also the increasing use of new technologies in commerce and offices for this purpose,

Aware of the dangers which the misuse of such systems could create,

Noting the work already carried out in other international organisations in the field of data privacy, notably the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and similar guidelines on computerised personnel files currently under discussion by the Subcommission on Prevention of Discrimination and Protection of Minorities of the United Nations Commission on Human Rights,

Considering the importance of protecting the rights of workers in the workplace,

Considering the usefulness of ILO studies on the use and disclosure of personnel data,

Adopts, this twenty-fifth day of April 1985, the following resolution:

The Advisory Committee on Salaried Employees and Professional Workers invites the Governing Body of the International Labour Office to request the Director-General to carry out studies with a view to establishing, in consultation with other appropriate United Nations agencies, a compendium of principles and good practices for safeguarding the rights of individual workers at the enterprise level.

Resolutions Submitted in Accordance with Article 17 of the Standing Orders of the Conference

Resolutions

May 25, 1985

Resolution concerning Computerised Personnel Information Systems and Data Privacy, Submitted by Mr. Ahmed, Workers' Delegate, Pakistan; Mr. Benya, Workers' Delegate, Austria; Mrs. Carr, Workers' Delegate, Canada; Mr. Dolan, Workers' Delegate, Australia; Mr. Karlsson, Workers' Delegate, Sweden; Mr. Mehta, Workers' Delegate, India; Mr. Muhr, Workers' Delegate, Federal Republic of Germany; Mr. Sanchez Madariaga, Workers' Delegate, Mexico; and Mr. Svenningsen, Workers' Delegate, Denmark

The General Conference of the International Labour Organisation,

Noting the rapid world-wide growth in the use by employers of computerised systems to store information relating to individual employees,

Noting also the increasing use of new technologies to collect data on individual performance and behaviour,

Considering the dangers to which freedom of association, freedom of expression, freedom of movement and privacy of the individual worker can be exposed by the misuse of computerised personnel information systems,

Stressing that any data on workers held by an employer should be accurate, should be collected by fair means and should be restricted entirely to those necessary for the worker/employer relationship,

Stressing also that the existence of such data should be known to the individual worker and to the worker representatives, and that such data should be freely available to the worker concerned for verification, should be protected against unauthorised access within the enterprise and should not be transferred to private organisations or public authorities without the permission of the worker concerned,

Noting the work already carried out in other international organisations in the field of data privacy, notably the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and similar guidelines currently under discussion by the Subcommission on Prevention of Discrimination and Protection of Minorities of the United Nations Commission on Human Rights,

Considering that the protection of the rights of employees in the workplace against the misuse of personnel data collected by employers raises specific problems of importance to the International Labour Organisation,

Considering also that regulations governing the collection, use and disclosure of personnel data should be established both by law and by collective agreement;

Invites the Governing Body of the International Labour Office—

(a) to request the Director-General to carry out studies on the problems concerning the regulation of the collection, storage and use by employers of individually identifiable data relating to their employees;

(b) to organise as soon as possible a tripartite meeting of experts to prepare rules and guidelines governing the regulation of data privacy at the workplace;

(c) to include the question concerning the regulation of computerised personnel information systems and data privacy in the agenda of a forthcoming session of the International Labour Conference with a view to the adoption of appropriate international labour standards.

BEST COPY AVAILABLE
Electronic spies threaten workers' privacy

There's basically nothing wrong with those technological wonders which boost productivity, tighten security or help end boring work. The trouble starts when they are used to spy on workers, invade their privacy and divulge personal data to anybody who presses the right key.

Thus some enterprises have introduced card-readers in place of door handles. To leave or enter their workplace employees must insert ID badges into an electronic slot. The stated purpose is protection of the company's sensitive processes or secrets.

"You have a feeling that Big Brother is watching you," a union official complained.

"The computer even knows when you go to the toilet."

A similar spectre looms in offices where word processors can, besides speeding up efficiency and improving working conditions, produce daily statistics showing the number of operations performed, the time worked, the number of errors committed and even graphs indicating operator capability on which to set performance standards.

Electronic spying on workers is bad, but it can be identified and remedies exist on the collective bargaining shelf. Invasion of workers' privacy is a more serious and more complex matter. It is difficult to prove and effective antidotes are in a laboratory stage.

Today details of a whole life can be squeezed on a few centimeters of tape. Hence the temptation and the risk to record personal information that is wholly irrelevant to employer-employee relationship. Some data may be subjective based on dubious sources or secretly recorded by an unauthorised person. However, once they find their way into computer memory they are later treated as objective facts.

The realisation of the danger is growing. A recent international opinion poll showed that 75 per cent of people interviewed in the United Kingdom feared computerised information could invade personal privacy. In France the figure was 71 per cent. in Norway 56 per cent. in the Federal Republic of Germany 51 per cent. in Japan 50 per cent. and in approaches vary, legal provisions usually cover such aspects as the purpose of personal data collection, access to computerised information and restrictions on its disclosure, the right of individuals to verify their files and request changes, as well as penal sanctions for unauthorised divulgations or misuse of computerised personal information.

In Sweden anyone wishing to set up or operate a computerised filing system containing personal data must first obtain a permit from a governmental authority which specifies the purpose of data collection and decides whether or not those who are registered in the file must be informed of its existence. Any individual has the right to obtain a printout of his file and ask for rectifications if necessary.

In Italy access to personal data banks needs express authorisation of the judiciary. All civil servants who illegally use or divulge such information are liable to imprisonment.

A British Data Privacy Act imposes obligation on employers to protect workers against misuse of data held in computers. It also gives "data subjects" the right to apply to the courts for compensation in the case of incorrect use of personal computerised information.

Another common feature of the existing legislation in this field are restrictions imposed on access to and collection of data on race, religion, politics, affiliation to trade unions, co-operatives, cultural associations or any other legally recognised organisation.

Questions of workers' privacy are increasingly discussed at the bargaining table. A pace-setting collective agreement was signed in 1984 at a General Motors subsidiary in Austria stipulating the conditions under which the firm can deal with personal information on workers. It contains severe restrictions on disseminating employee data, some of which cannot be released without prior agreement of the trade union, the ILO survey reports.

At the 1985 International Labour Conference several trade union leaders expressed the view that national measures against possible misuse of computerised personal data needed to be bolstered by international action on a tripartite basis.

Earlier this year the ILO Advisory Committee on Salaried Employees and Professional Workers passed a resolution inviting the ILO to carry out studies with a view to establishing a compendium of principles and practices for safeguarding people's privacy at the workplace.

The ILO Governing Body at its next meeting in November will decide on the effect to be given to this proposal.
COUNCIL OF EUROPE

The Council of Europe, established in 1948 to draft and implement the European Convention on Human Rights, took its first initiative with regard to "privacy and the use of computers" in 1971. An expert group mandated to investigate "automated processing of personal data" suggested that new legislation was necessary in European countries and that the Council of Europe "would serve a useful function by helping member states avoid unnecessary divergence between their laws on the subject." In 1972 a conference of European ministers of justice adopted a resolution calling for the CoE to "consider the possibility of elaborating a draft international convention (treaty) on the protection of privacy in view of the increasing compilation of personal data into computers."

Personal Data Convention Ratified

A decade later, the ministers of the 22 member governments opened a convention for the protection of personal data for signature. The agreement required ratification by five countries in order to come into force. On October 5, 1985 the convention became effective with Sweden, France, Spain, Norway and Luxembourg having ratified it. The convention embodies a number of fundamental principles of data protection, almost identical to those set forth in the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.

The Committee of Experts on Data Protection which prepared the convention, rather than disband when the convention had been approved, was instructed to consider more specific practices for various sectors or types of users of personal data. From 1980 to 1984 the committee completed recommendations on social science and direct research data, medical information, mail and marketing data and social-security records. These recommendations are non-binding but usually seriously considered by governments when drafting or amending national data-protection legislation.

Employment Sector Records Examined

The Committee's present activities involve personal data in police and law enforcement, employment and the "new technologies". The working party on the "use of personal data in the employment sector" distributed a questionnaire to member governments in 1985 "to learn of the texts of laws on regulations concerning the collection and use of personal information within the framework of employer/employee relations, in both the public and private sectors, as well as any important judicial decisions in this field." The questionnaire asks what personal
details are normally collected, if limits are placed on collection of sensitive data (such as data concerning political opinion, religious conviction, intimate life, race). For what purposes the information may be used, if it is disclosed to third parties, and whether employees have access to their records. One item addresses "surveillance of employees," asking for details about "methods of monitoring, if there is (employee) consultation before the introduction of such methods, and what forms of monitoring should be prohibited."

The Working Party is expected to examine questionnaire results in March 1986 and then decide whether to simply prepare a report describing employee-record practices in Europe or draft a recommendation that may become the standard or model for collecting and handling of such data.

It is recommended that OTA establish contacts with the Working Party to obtain the results of the questionnaires, which would contain useful materials from member countries.
PART VII

OBSERVATIONS
OBSERVATIONS

Surveying the national reports and the international union and intergovernmental activities, several main observations seem warranted:

1. No industrial democracy has adopted a conscious and comprehensive approach to employee privacy and worker monitoring through all of its various technological forms. Rather, issues are taken up on a topic-by-topic and situation-by-situation basis, and generally with a pragmatic, accomodation-of-conflicting-social-interests approach, within the social norms of that society and the specific legal and industrial-relations mechanisms it has in place. No nation has under consideration a comprehensive approach to worker monitoring issues either, at this time.

2. The West German concept of "information self-determination" (from the Census constitutional decision of 1983), when linked with the "protection of the personality" and the "legitimate interest" or "purpose" principle for evaluating employer concerns, seems to offer the most explicit and up-to-date approach to balancing new-technology uses with evolving employee-privacy values.

3. The issue of worker monitoring is clearly being articulated and driven in public discussion by the trade unions. They have articulated a variety of bases for seeking bans or limitations on worker monitoring. These correspond to the five bases of social challenge to employer use of monitoring discussed in Part I of this report:

   a. Non-surveillance ("privacy")
   b. Health protection (stress impacts)
   c. Group solidarity (work group and union value)
   d. Struggle over employer "power" and "control"
   e. "Dignity" claim
4. Given the shrinkage of union membership in most industrial democracies during the past decade, the loss of prestige that unions have faced with the general public (and younger workers) in this same period, and the heavy pressures both leaders and the publics of industrial democracies feel to increase productivity and quality-competitiveness in production, the influence of unions to win either collective bargaining or legislative bans on work-productivity monitoring seem quite limited in the near future. However, the fairness, openness, and "decency" with which employers conduct electronic work monitoring seems to be an issue that will grow, since it has the dignity, privacy, and health aspects that are strong values in most industrial democracies. Therefore, how employers use monitoring rather than whether they should be allowed to do this at all, may be the central issue that reaches beyond union advocacy.

5. As the uses of location-control, telephone-call-surveillance, and personnel-information-systems expand in the next decade, these will most likely generate public discussion and probably some legal/regulatory action. It is here that the data protection laws and commissioner activities of other industrial democracies are likely to prompt specific policies. A major issue will be what employers are actually doing with these technologies. There is little empirical data on that issue, partly because these technologies are still quite new (or not used widely as yet).
Request for Reproduction Services

Date 2 Sept

1. Number of Copies: 25
2. Number of Pages: 5
3. Reproduce Both Sides: ☑ Yes; ☐ No
4. Collate: ☑ Yes ☐ No
5. Binding Method:
   ☐ 3-Hole Punch; ☐ Staple; ☐ Band in Sets;
   ☑ Velo Bind; ☑ Perfect Bind; ☐ No Binding
6. Reduction Required: ☐ Yes; ☑ No
7. Date Needed: __________; Time ________
8. Delivery: ☐ Will Wait
   ☐ Call When Ready; Phone No. ________
9. Special Instructions—Use Reverse Side.

Insert into K. Bandy

☑ perfect Authorized Signature
☑ bound report; rebind

Received by __________ Date __________

Total No. of Units 125

OTA Form 4, Revised, June 1978
What Does Foreign Experience Suggest for the U.S.?

Concentrating on electronic work monitoring -- the centerpiece of the OTA inquiry -- what does the experience in other industrial democracies have to suggest about U.S. policy choices?

1. Much of the struggle between unions and managements over individual work measurement and personnel decisions is a direct function of the bi-party, bi-polar, zero-sum-game nature of organized labor relations. This model of workplace administration -- often called the "industrial democracy" model -- is built upon assumptions of conflicting interest and of an inevitable tension between management's drive for increased control of work processes and workers and the union's protection of workers against unfair exploitation. In this context, the work-monitoring issue we have called the "struggle over employer power and control" is the driving force of the challenge to "Big Brother monitoring." Especially in the European and British-Commonwealth nations, the key issue is the traditional, socially-institutionalized political struggle over workplace authority applied now to the new setting of office systems technology.

2. This model is not close in either political or institutional elements to the great majority of U.S. offices in which VDTs are being installed. About 90-95% of private-employer offices are not unionized. Perhaps 25-35% of local, state, and federal offices are union-represented. This means that the basic relationship of employee to employer in the great majority of U.S. offices is one in which there is no organized entity representing employees -- no professional staffs to counter management-staff expertise; no continuing source of data collection independent of management about workplace conditions and effects; no union educational and mobilization process directed
at employees; no demand for advance notice to unions of technological change; and clearly no institutionalized bargaining over the terms and conditions of work. And, union organizing efforts to create such bi-polar, organized relationships in American offices have not had significant success during the first decade of office automation. If anything, dominant social trends suggest that the overwhelming majority of U.S. office workers do not feel a need for unions to represent their interests in working conditions -- including issues such as work monitoring. This is tacitly recognized by the new thrust of the AFL-CIO's outreach to non-union workers -- offering credit card options, insurance programs, legal services, and other non-representational benefits for joining unions.

3. Therefore, to the extent that the conflict over work monitoring in many other industrial democracies arises directly out of the bi-polar conflict model of labor relations, it has relevance only in the small minority of U.S. offices where workers are union-represented. Even here, our field work at 10 such union-represented organizations, both public and private, suggests that it is the health effects dimension -- the harmful stress created in some types of intensive VDT work by the combination of close monitoring, oppressive work quotas, and job insecurity -- that most concerns American workers. Management's measurement of work per se, even with new electronic techniques and continuously, is not seen by American workers as either an illegitimate method or a necessary threat to individual dignity, as is often the cultural norm of workers in European social democracies. In the U.S., we found the cultural norm to accept employer work measurement on an individual basis, as long as it is fair, takes into account qualitative as well as quantitative aspects of the job, helps produce objective comparisons among workers for allocation
of special rewards (premium pay, promotion, etc.), and is conducted in an open, "due process oriented" process.

4. It is also important to observe the effects that office systems technology is having on the nature of office jobs, and how this may affect the "union model" of no-individual-measurement. The large mass of clerical workers doing data entry and customer service work is steadily being divided into two sectors of VDT operations: one sector with highly-repetitive and low-skill keyboarding, low-level customer-relations and low-discretion claims processing and a second sector of higher-level customer-service and claims-analysis work. The former types of jobs are the closest to the "office factory" milieu -- production work, measured output, low pay, quota-based supervision, etc. -- and the jobs where union appeals against oppressive, high-stress monitoring would seem to have the greatest potential.

However, it is precisely those jobs that are most likely to be significantly reduced by advancing computer and communication technologies, and by employer business trends. Optical scanning and direct customer-input from their premises are already reducing the data entry sector; along with the shifting of such work from urban locations to exurban U.S. sites or to off-shore production, there may be a steadily diminishing set of jobs for U.S. unions to address on the "close monitoring" issue.

This leaves the second sector -- customer-service and higher-level claims analysis jobs. If U.S. employers were to apply a heavy-handed Taylorist approach in collecting and using individual measurements in these jobs, this could become a potential sector for unions to raise the banner of "anti-Big-Brother-monitoring." While some private and public employers may adopt such practices, the importance of quality elements in satisfying customers or citizens in VDT-based jobs provides
a strong element of business or government-service self-interest that works against the Taylorite tendency in most employment settings.

5. Recent experiments in employee involvement and quality-circle participation are sometimes cited as the "U.S. answer" to those urging that the European/British model of trade unionism or government-intervention is needed to avoid "oppressive work monitoring." While the use of employee participative mechanisms has not been as common in U.S. offices as it has been in factory settings, such mechanisms have been growing in the past 5-10 years in office work. Almost 40% of the 110 organizations we examined in late 1985 and early 1986 were using employee participation in various aspects of their VDT operations, from involvement in equipment selection to job-design or work-organization matters. However, American labor laws limiting employer associations, the absence of any non-union institutional forms for such efforts, and a lack of enthusiasm by managements for meaningful employee participation in many white-collar sectors are factors that have, thus far, kept employee participation from being the dominant model in office work. This is especially true at the clerical and administrative levels where work monitoring is most often practiced. This suggests that making work monitoring acceptable to most VDT clerical and administrative employees through participative mechanisms is not yet the prevailing practice among American employers, and may not become so in the near future. This makes the future of work monitoring practices as a potential source of employee discontent less easy to predict than if the grievance-resolving presence of meaningful employee participation programs could be taken as the emerging trend in U.S. offices.

6. Finally, on government interventions in foreign nations of either the quality-of-worklife or data-protection type being applied to U.S. work monitoring, there are no signs that we have seen of either a need for such action
being perceived by U.S. policymakers or the desirability of U.S. governments adopting a pro-active role in these areas being registered in national public opinion. The situation here is quite unlike the worker's right-to-know movement. There, U.S. unions convinced the public and policymakers that legislation was indeed needed to disclose the identity of chemicals being used in production, and to provide a process by which harm and potential harms at the workplace could be identified by workers and their representatives before the "gravestone count" indicated problems were present. As a result, state right-to-know laws have been enacted in several dozen states despite the general "anti-regulatory" mood of the electorate. The inability of proponents to win enactment of anti-monitoring laws reflects, we believe, their inability to demonstrate the presence of widespread and harmful health effects as a result of VDT work, or to convince lawmakers and the public that collecting output data and using it for personnel administration is a violation of U.S. privacy norms.

7. The observations made above should be read in tandem with the parallel report we submitted to OTA on work monitoring techniques, practices, and policies in the United States, historically and today. In that report, and in the observations we have just made, our judgment is that the approaches and experiences that trade unions and some government bodies in other industrial democracies have taken toward work monitoring are not in basic harmony with American employee values, U.S. legal and institutional approaches, or the general directions of American public opinion. Therefore, U.S. approaches to VDT work monitoring ought to be developed with the sense that there is more difference than similarity with our sister democracies on this issue.
What Does Foreign Experience Suggest for the U.S.?

Concentrating on electronic work monitoring -- the centerpiece of the OTA inquiry -- what does the experience in other industrial democracies have to suggest about U.S. policy choices?

1. Much of the struggle between unions and managements over individual work measurement and personnel decisions is a direct function of the bi-party, bi-polar, zero-sum-game nature of organized labor relations. This model of workplace administration -- often called the "industrial democracy" model -- is built upon assumptions of conflicting interest and of an inevitable tension between management's drive for increased control of work processes and workers and the union's protection of workers against unfair exploitation. In this context, the work-monitoring issue we have called the "struggle over employer power and control" is the driving force of the challenge to "Big Brother monitoring." Especially in the European and British-Commonwealth nations, the key issue is the traditional, socially-institutionalized political struggle over workplace authority applied now to the new setting of office systems technology.

2. This model is not close in either political or institutional elements to the great majority of U.S. offices in which VDTs are being installed. About 90-95% of private-employer offices are not unionized. Perhaps 25-35% of local, state, and federal offices are union-represented. This means that the basic relationship of employee to employer in the great majority of U.S. offices is one in which there is no organized entity representing employees -- no professional staffs to counter management-staff expertise; no continuing source of data collection independent of management about workplace conditions and effects; no union educational and mobilization process directed
at employees; no demand for advance notice to unions of technological change; and clearly no institutionalized bargaining over the terms and conditions of work. And, union organizing efforts to create such bi-polar, organized relationships in American offices have not had significant success during the first decade of office automation. If anything, dominant social trends suggest that the overwhelming majority of U.S. office workers do not feel a need for unions to represent their interests in working conditions -- including issues such as work monitoring. This is tacitly recognized by the new thrust of the AFL-CIO's outreach to non-union workers -- offering credit card options, insurance programs, legal services, and other non-representational benefits for joining unions.

3. Therefore, to the extent that the conflict over work monitoring in many other industrial democracies arises directly out of the bi-polar conflict model of labor relations, it has relevance only in the small minority of U.S. offices where workers are union-represented. Even here, our field work at 10 such union-represented organizations, both public and private, suggests that it is the health effects dimension -- the harmful stress created in some types of intensive VDT work by the combination of close monitoring, oppressive work quotas, and job insecurity -- that most concerns American workers. Management's measurement of work per se, even with new electronic techniques and continuously, is not seen by American workers as either an illegitimate method or a necessary threat to individual dignity, as is often the cultural norm of workers in European social democracies. In the U.S., we found the cultural norm to accept employer work measurement on an individual basis, as long as it is fair, takes into account qualitative as well as quantitative aspects of the job, helps produce objective comparisons among workers for allocation
of special rewards (premium pay, promotion, etc.), and is conducted in an open, "due process oriented" process.

4. It is also important to observe the effects that office systems technology is having on the nature of office jobs, and how this may affect the "union model" of no-individual-measurement. The large mass of clerical workers doing data entry and customer service work is steadily being divided into two sectors of VDT operations: one sector with highly-repetitive and low-skill keyboarding, low-level customer-relations and low-discretion claims processing and a second sector of higher-level customer-service and claims-analysis work. The former types of jobs are the closest to the "office factory" milieu -- production work; measured output, low pay, quota-based supervision, etc. -- and the jobs where union appeals against oppressive, high-stress monitoring would seem to have the greatest potential.

However, it is precisely those jobs that are most likely to be significantly reduced by advancing computer and communication technologies, and by employer business trends. Optical scanning and direct customer-input from their premises are already reducing the data entry sector; along with the shifting of such work from urban locations to exurban U.S. sites or to off-shore production, there may be a steadily diminishing set of jobs for U.S. unions to address on the "close monitoring" issue.

This leaves the second sector -- customer-service and higher-level claims analysis jobs. If U.S. employers were to apply a heavy-handed Taylorist approach in collecting and using individual measurements in these jobs, this could become a potential sector for unions to raise the banner of "anti-Big-Brother-monitoring." While some private and public employers may adopt such practices, the importance of quality elements in satisfying customers or citizens in VDT-based jobs provides
a strong element of business or government-service self-interest that works against the Taylorite tendency in most employment settings.

5. Recent experiments in employee involvement and quality-circle participation are sometimes cited as the "U.S. answer" to those urging that the European/British model of trade unionism or government-intervention is needed to avoid "oppressive work monitoring." While the use of employee participative mechanisms has not been as common in U.S. offices as it has been in factory settings, such mechanisms have been growing in the past 5-10 years in office work. Almost 40% of the 110 organizations we examined in late 1985 and early 1986 were using employee participation in various aspects of their VDT operations, from involvement in equipment selection to job-design or work-organization matters. However, American labor laws limiting employer associations, the absence of any non-union institutional forms for such efforts, and a lack of enthusiasm by managements for meaningful employee participation in many white-collar sectors are factors that have, thus far, kept employee participation from being the dominant model in office work. This is especially true at the clerical and administrative levels where work monitoring is most often practiced. This suggests that making work monitoring acceptable to most VDT clerical and administrative employees through participative mechanisms is not yet the prevailing practice among American employers, and may not become so in the near future. This makes the future of work monitoring practices as a potential source of employee discontent less easy to predict than if the grievance-resolving presence of meaningful employee participation programs could be taken as the emerging trend in U.S. offices.

6. Finally, on government interventions in foreign nations of either the quality-of-worklife or data-protection type being applied to U.S. work monitoring, there are no signs that we have seen of either a need for such action
being perceived by U.S. policymakers or the desirability of U.S. governments adopting a pro-active role in these areas being registered in national public opinion. The situation here is quite unlike the worker's right-to-know movement. There, U.S. unions convinced the public and policymakers that legislation was indeed needed to disclose the identity of chemicals being used in production, and to provide a process by which harm and potential harms at the workplace could be identified by workers and their representatives before the "gravestone count" indicated problems were present. As a result, state right-to-know laws have been enacted in several dozen states despite the general "anti-regulatory" mood of the electorate. The inability of proponents to win enactment of anti-monitoring laws reflects, we believe, their inability to demonstrate the presence of widespread and harmful health effects as a result of VDT work, or to convince lawmakers and the public that collecting output data and using it for personnel administration is a violation of U.S. privacy norms.

7. The observations made above should be read in tandem with the parallel report we submitted to OTA on work monitoring techniques, practices, and policies in the United States, historically and today. In that report, and in the observations we have just made, our judgment is that the approaches and experiences that trade unions and some government bodies in other industrial democracies have taken toward work monitoring are not in basic harmony with American employee values, U.S. legal and institutional approaches, or the general directions of American public opinion. Therefore, U.S. approaches to VDT work monitoring ought to be developed with the sense that there is more difference than similarity with our sister democracies on this issue.