BOOKENDS

Computers and Data Protection by Eddy Peers and Bill Buckley

Computers and Data Protection is a very useful, brief (59 pages) guide to companies on how they should tackle international data protection issues. It is based on a study jointly funded by the EEC Commission and Deloitte Haskins & Sells of which the authors are partners. The firm carried out a survey of 42 large and medium sized companies in different EEC countries looking at the impact that data protection laws have had on their operations.

The authors have drawn up a number of useful checklists and questionnaires with which companies can assess their need to comply with national laws. A company internal comprehensive survey of automated processing and uses of data has often led to the uncovering of inefficiencies such as duplication of effort by different departments. "This is especially so where the use of microcomputers has spread with little control. Therefore, the census can lead to cost-savings when duplication is eliminated".

The text includes several checklists which can be used by companies with little amendment, like one on subject access:

Subject Access

"In order to monitor the processing of requests for access to data, we suggest that the following basis information is maintained:

* date on which subject access request was received;
* that any necessary fee has been received;
* the name of the person who received the request;
* has the enquirer provided sufficient information to enable the data user to determine if information is likely to be held in computer systems? For example, whether the enquirer is a supplier or customer or employee;
* who will be responsible for gathering the necessary information?
* the name of the employee who will respond to the request;
* the date by which the response must be sent;
* the steps that must be taken to ensure that the information is being sent to the correct person;
* the date on which the response was made;
* a copy of the information sent".

There are more detailed checklists on microcomputer and minicomputer

security.

There are two short chapters which attempt to quantify the impact of data protection legislation. For example:

1) Almost all the companies said that the amount spent on data protection was not more than half of one per cent of total expenditure on automated data processing.

2) In countries with most experience of data protection law, it is not considered a burden. Three-quarters of the firms surveyed thought that it was unnecessary to hire more staff to deal with data protection.

3) Companies should pay more attention to data security. Two-thirds of the companies believe that internal data protection standards are necessary.

The final section gives basic information about the status and type of data protection proposals and legislation in each EEC country. Inevitably, some points have since changed, but the authors acknowledge Privacy Laws & Business as a source for keeping them up to date!

Published in 1988 by Deloitte Haskins & Sells, P.O. Box 207, 128 Queen Victoria Street, London, EC4P 4JX., England. Telephone: 01-248 3913.
ISBN 0-86349-125-1 **Price: £7.50p.**

The Complete Computer Virus Handbook by David Frost, Ian Beale & Chris Frost

The second edition of The Complete Computer Virus Handbook manages in a little over 100 pages to pack in just about everything the general business reader might want to know about computer viruses. It is written by the top members of Price Waterhouse's computer audit group. The handbook addresses practical concerns and summarizes essential points in useful checklists.

A computer virus is explained as, "computer code usually designed to carry out two tasks. Firstly the virus is designed to replicate itself from one computer to another. Secondly, the computer virus is designed to locate itself within a computer system in such a way as to make it possible for it to amend/destroy programs and data files, by interfering with the normal processes of the operating system." Each of the most common type of software threats, like worm, Trojan horse, and logic bomb, are described. Then, the risks posed by viruses (destructive and non-destructive), and the secondary impact of a virus attack are explained in straightforward language.

In the chapter on sources of viruses, it is made clear that the major threat posed by computer viruses is to microcomputer systems but that mainframe computers are also vulnerable when connected to microcomputers or to a telecommunications system network. Common sources are: contact with contaminated systems, pirated software, infected proprietary software, fake games, feeware, shareware (many firms have banned their use by staff), and updates of software distributed via networks. This section has a useful

checklist of virus symptoms:

Virus Symptoms

"The presence of a virus can be indicated if one or more of the following symptoms appear on your computer. Any evidence of these or similar events should be an immediate cause for concern. Isolate the PC at once and investigate.

* Unfamiliar graphics or quizzical messages appearing on screens.
* Programs taking longer than usual to load.
* Disk accesses seeming excessive for simple tasks.
* Unusual error messages occurring more frequently.
* Less memory available than usual.
* Access lights turning on for non-referenced devices.
* Programs/files mysteriously disappearing.
* Executable files changing size for no obvious reason.
* File dates changing for no obvious reason.
* Changes to disk volume identifiers."

For the technically knowledgeable, there are sections on how viruses get into systems and some of the techniques used by virus writers both for PC's and for the different versions of the Macintosh system. On how viruses can be prevented, the advice is to remember that "it is impossible to guarantee complete protection against a computer virus." The reason is that a virus may come from outside an organization but be "transmitted inadvertently by people in the company who have legitimate access to computer systems." Nevertheless, there are techniques and software which can both detect a virus and prevent an attack. There is a checklist of steps to be taken if a virus attack is suspected.

The chapter on how the law can help, explains the principles involved and a victim's possible remedies under criminal and civil law. Clearly, the law is still evolving in this area and a victim would need specialist legal advice. There is little certainty from relying on insurance, as most computer insurance does not specifically include or exclude computer viruses.

The second half of the book consists of appendices which:

* examine 40 viruses, their sources and how they work;
* test 24 MS DOS vaccines and give brief details on 15 Macintosh vaccines;
* contain a glossary of terms;

* list DOS interrupts (the glossary explains this term); and

* give references for those who want to know more.

Published in 1989 by Pitman Publishing, 128, Long Acre, London, WC2E 9AN, England.
ISBN 0 273 03255 0 **Price: £14.95p.**

Protecting Privacy in Surveillance Societies:
The Federal Republic of Germany, Sweden, France, Canada and the United States
by David H. Flaherty

Protecting Privacy in Surveillance Societies is the fruit of Professor Flaherty's research throughout the 1980's and as a result offers both a broad sweep and an impressive depth of insight into the detailed workings of the agencies responsible for data protection in the public sector in these five countries. He also includes frequent comparative references to the experience of managing data protection in other countries, and his comments and recommendations (in some 400 pages with 74 pages of notes and index) are relevant to every country with or planning data protection legislation. The author is Professor of History and Law at the University of Western Ontario, Canada and was a consultant to the Canadian Parliament's review of the Privacy Act.

His theme is that the problem of controlling surveillance is finely balanced. "Governments are the worst offenders against privacy, at least in terms of demonstrable abuses against individuals and groups, yet they are charged with promoting such basic societal goals as efficiency and cost controls. They also make the rules by which social programs, for example, are to be operated, many of which incorporate highly intrusive practices. Who is to control the government?"

To answer this question for each country in turn, he examines:

1. The model of data protection it has adopted, for example, the extent to which it is advisory or regulatory, how the law developed and and how the data protection authority is organized.

2. The goals of data protection, such as statutory objectives; philosophical objectives; information management objectives, for example, the role of the law in providing a basis for challenging the government's collection or use of information on individuals.

3. The power of the data protection authority in terms of its independence; its powers of intervention (he is often quite critical); the control of record linkages; the political climate and the use of power; and the courts.

4. The implementation of data protection; analysing the composition and staffing of the data protection authority; describing the decision-making process and its implementation in practice.

5. The section on the regulation of surveillance systems offers several case studies in each country on issues like population registration, Personal

Identity Numbers, and identity cards (Germany), The National Tax Board (Sweden), Project GAMIN: the surveillance of newborn children (France), the security services (Canada), and the regulation of computer matching (USA).

6. The section on responding to privacy and surveillance problems looks at the problems and achievements of implementation and how each law might be strengthened.

Flaherty's research leads him to several conclusions, including:

* "In order to keep governmental surveillance of the population under reasonable control, data protection laws and agencies are essential in Western industrial societies."

* "These laws should define privacy interests as carefully as possible in order to facilitate implementation and in order to confront surveillance practices more directly than they do at present."

* "Data protectors must be active and committed individuals who are very independent in the exercise of controlling power in order to serve as a countervailing force to excessive and intrusive surveillance practices."

* "Data protectors must pursue audits with vigor in order to monitor compliance with fair information practices."

* "On merit, the argument for extending data protection to manual records is strong in that it would reduce incentives for leaving sensitive personal data in manual form."

* "Government agencies are the leading invaders of the personal privacy of citizens, since they maintain systems with the largest scope and most numerous records. Even a system for the seemingly innocuous purpose of paying a benefit can be subverted for surveillance of a particular person..."

* ".....The experience of the 1980's suggests that data protection normally is less of a legislative priority than efficient government."

* "It is important that small data protection agencies encourage the main government departments to prepare their own initial reviews of the impact of new technology, preferably in the form of "privacy impact statements....."

* "..... I am persuaded that statutory data protection is also essential for the private sector."

Professor Flaherty's book is ideal for anyone who would like to understand the rationale and role of data protection authorities. But it is not for the distracted businessman who merely wants to comply with the law. A shorter paperback edition might attract a wider readership.

Published in 1989 by The University of North Carolina Press, Post Office Box 2288, Chapel Hill, NC, 2715-2288, USA. Telephone: (919) 966-5722; or University Book Marketing, Suite 7, 26, Charing Cross Road, London, WC2H 0LN, England. ISBN 0 8078 1871 2 Price: US$49.50