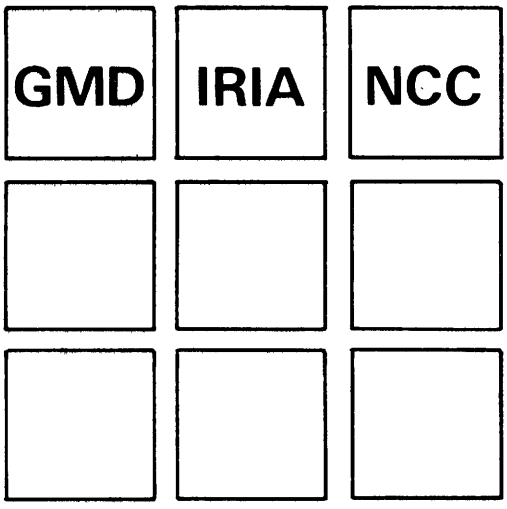


STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

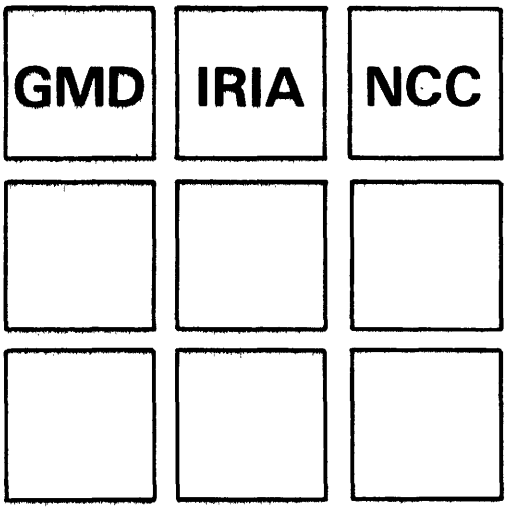
to the Commission of the European Communities

Volume 4 of 6

Section 4: International economic aspects of data protection

by E F M Hogrebe

JULY 1980



STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

to the Commission of the European Communities

Volume 4 of 6

Section 4: International economic aspects of data protection

by E F M Hogrebe

JULY 1980

Contents of all volumes

Contents of section 4

List of tables

4 International economic aspects of data protection

4.1 Definition of the problem and summary

4.1.1 Definition of the problem

Ever since the concept of modern data protection first arose, the discussion regarding the costs of data protection has constituted an integral part of the general data protection business. Whilst the active advocates and defenders of the data protection ideas had written on their banner the motto "As much data protection as is (at all) possible", the somewhat more sceptical voices of the representatives of private and public data processing organisations have adopted the more restricted attitude: "Only as much data protection as is (absolutely) necessary". In addition to the traditional tendency to keep their data and information, as well as the sources of the latter, secret, the latter attitude is largely influenced by the fear of excessive data protection costs. These costs may be roughly divided into the following three categories:

- costs of special (additional) data protection measures
- costs in the form of general inefficiencies in the sphere of data protection and decision-making caused by data protection

- costs in the form of lost benefit arising through certain profitable data processing procedures (including possible products and services based thereon) becoming impossible to carry out owing to data protection regulations (opportunity costs).

Passing outside the framework of the various national societies, there are fears that such data protection costs may arise in a still greater degree in the international field, due either to more or less serious differences, incompatibilities or even contradictions between the various data protection regulations, or simply due to the fact that internationally operating undertakings and organisations, in view of the fact that they must comply with several national data protection regulation systems simultaneously, will incur cumulative data protection costs. There is also theoretically the possibility that - contrary to the wishes of the individual national legislators - the data protection costs thus arising in the international field may so increase in certain sectors or in concrete individual cases that important international data processing applications (including possible further activities thereto) may no longer be economically practicable. It is also feared in circles of private industry that in a similar way more or less considerable international distortions of competition may arise.

It is the task of the present study to estimate - as far as that is generally possible - the costs of data protection on the national level, and also any possible distortions of international competition which may result therefrom. Furthermore, suitable harmonisation measures should be indicated which are calculated to reduce data protection costs, and in particular any distortions of international competition resulting therefrom, so far as this is possible and necessary; at the same time the rights and interests of the citizens affected must also be considered. It should be made clear, however, that the following investigation is primarily concentrated on data protection costs in the sense of costs arising through special additional data protection measures. General inefficiencies and opportunity costs resulting from data protection measures could not be considered in detail within the framework laid down for this study. Apart from the fact that there is practically no suitable empirical material available, it appears questionable in the light of considerable empirical and methodological difficulties whether it is possible at all to estimate such costs effectively and adequately.

Furthermore, regarding the problems of distortions of international competition, it should be emphasised that we are only discussing here distortions of competition caused by data protection costs, not those due to data protection in general.

4.1.2 Summary

In section 4.2 a few basic concepts of economic theory are expounded in their relation to the problems of data protection costs, which assist in the classification and elucidation of the problems of data protection costs, and also offer suggestions and starting points for possible further investigations. In addition certain theoretical and methodological difficulties are discussed and the general theoretical approach and the concrete methodological procedure are explained.

In the following section, number 4.3, various data protection cost estimates, investigations and experiences from the following selected countries are then critically examined and evaluated: United Kingdom, USA, Sweden, the Federal Republic of Germany. Section 4.4 then sums up the general results.

On this basis, in section 4.5, the problem of distortion of international competition caused by data protection costs is then discussed. And section 4.6 finally draws conclusions from the entire investigation of data protection costs, by proposing certain features of cost-effective European data protection harmonisation policy.

4.2 Concepts of economic theory and methodology

4.2.1 Problems of the application of concepts of cost-benefit analysis [1]

Within the framework of an investigation of international economic aspects of data protection, the idea of the application of the concepts of cost-benefit analysis to the individual national data protection laws under consideration seems to be a good one, with the object of then proceeding to a comparative synthesis of the economic effects of data protection in the international field. And in fact, the various data protection laws (each considered as a concrete public project) appear (just because of the decidedly political nature of the object in view, i.e. "protection of privacy from invasion in the course of data processing"[2] and in the light of the fact that the beneficiaries of data protection and those who bear the costs of such protection fall basically into two separate groups) to be extremely suitable subjects for a cost-benefit analysis on the basis of social economics, going beyond the costs and profitability calculations of purely private enterprise economics. By such a cost-benefit analysis the changes to be expected in the benefit obtained by the individual members of society, i.e. the social benefits and costs of the individual data protection laws, would be comprehensively checked for the existence of a favourable

1) The following remarks constitute a revision of Hogrebe 1979, section 8.1, pp 482-487.

2) This is as it was expressed by the German Federal Parliament, Deutscher Bundestag 1976, p 1.

balance. Certainly there is no gainsaying that - apart from the problem of obtaining sufficient empirical data - there are quite considerable methodological problems, requiring comprehensive investigation, regarding the identification and evaluation of the social benefits and costs of data protection.

4.2.1.1 Data protection as a "public good": the problem of the determination of the benefit

As regards the benefits, difficult problems arise as the socially positive effects of data protection - in particular in the field of law and general social relations - are only realised for individual persons in a general way, which cannot be determined or measured, and therefore "data protection" must be regarded to a large extent as a "public good" and in any case as "intangible" without any market price.[1)]

1) For general comments on the question of cost-benefit analysis and with special reference to these concepts see Prest/Turvey 1965, pp 685-705; Recktenwald 1970, 443 ff.; Layard 1972, 496 ff.; and Sugden/Williams 1978, p 148.

   The efforts made for instance by Turn/Shapiro 1972, in particular pp 439 to 440, to determine the "value of personal information" may perhaps afford a certain basis for a monetary evaluation of "data protection". They are however restricted as a concept to the problem of a strategy for the discouragment of breaches of data security, which is somewhat outside the cost-benefit analysis of data protection. This also applies - in spite of the title "Approaches to a cost-benefit analysis of data protection" - to Angermann/Thome 1973, pp 18-22, who as part of an approach which does not make a clear distinction between data protection and data security, and makes use of somewhat incompatible methods, adopt a cost-benefit analysis concept which is more orientated towards business economics.

In the treatment of data protection as a public good it is of no importance that data protection - unlike the classic example always referred to as a paramount example of a public good, viz. "external national security" - is not exclusively "produced" by the Government, but in combination by all subjects of the regulations, whether public or private; incidentally "internal national security" - the other classic example of a public good - is also "provided" to a large extent by private individuals by self-defence and private justice (i.e. by private arbitrators, trade union and association justice, plant and business protection, private detectives, personal bodyguards etc.).[1)]

As is probably better expressed by the terms "social good" and "collective good", which are used without distinction as synonyms of "public good", the concept of "public good" (or "services publicly provided") is primarily based not on its degree of usefulness and profitability.[2)]

Without wishing to cut short the discussion in economic circles on the theory of the public good, which has recently been conducted in increasingly differentiated form, it can be regarded as a decisive characteristic of (genuine) "public goods", that they - unlike (ordinary)

1) See for this example Recktenwald 1970, p 264.

2) See as regards this terminology, inter alia, Hanusch 1970, p 42, note 3, also Hanusch 1972, p 12, note 2.

"private goods", which are made available by means of the market economy, i.e. by transactions between individual consumers and producers, so far as concerns the user served by them and the degree of their actual utilisation - are not restricted primarily to a particular consumer but are equally advantageous to all other consumers; the consumption or use of a public good (e.g. the cleansing of the air by measures, whether private or public, against air pollution) does not take place in rivalry with such consumption or use on the part of other consumers.[1)]

Whilst the consumption or the utilisation of private goods and services (e.g. the consumption of a pint of beer or the taking of a seat in a passenger transport vehicle) inevitably makes the good or service in question unavailable for another individual, the utilisation of public goods and services by several individuals is not competitive, in that sense, because participation of one individual in such utilisation does not prejudice their usefulness to another person; the use which someone achieves in the consumption of a public good is externalised in as much as it is equally available, undiminished, to all other persons.

This fact certainly has the result that the individual consumer, as one among many, is normally not prepared to

1) Regarding the characterisation of public goods after Musgrave, cf Musgrave/Musgrave/Kullmer 1975 pp 5-7.

make voluntary payments to those offering public goods, as he will prefer to enjoy the benefit free of charge of what will in any case be provided by others. This "free-rider" problem, which is incidentally in many cases the reason for State intervention in the form of the removal of certain goods and services from the market economy, leads above all - so far as the exclusion of individuals from consumption (without payment) is impossible, uneconomic or socially undesirable - via the direct problem of the denial of voluntary payments, or the impossibility in practice of collecting involuntary payments, to the fundamental difficulty of the determination of the benefit which would enable the Government to determine how much of which public goods should be made available:

> "Just as the individual consumer has no reason to offer voluntary payments to private producers, similarly he has no reason to make known to the public authorities what is his estimate of the value of the public service."[1)]

1) Musgrave/Musgrave/Kullmer 1975, p 7.

See also Prest/Turvey 1972, p 87:

"Ever since Wicksell, it has been recognised that any attempt to get consumers to reveal their preference regarding collective goods founders on the rock that the rational thing for any individual consumer to do is understate his demand, in the expectation that he would thereby be relieved of part or all of his share of the cost without affecting the quantity obtained."

Data protection made available by means and in pursuance of a data protection regulation can only be interpreted as a "public good" in accordance with the concept here described, as the "consumption" or the "utilisation" of data protection by various individuals is not to be regarded as competitive. Moreover, in the closest possible analogy to "internal security", it is for social reasons practically not possible in the nature of the case to exclude the individual member of society from the "consumption" of data protection, so that owing to the fundamental impossibility of compelling the individual to reveal his preference as far as concerns data protection regarded as an (indivisible) public good, and also in view of the very largely intangible character of data protection, recourse must be had to complimentary differentiated methods of assessment of its usefulness.[1)]

1) See for instance the methodical efforts of Recktenwald 1970, p 249-266, to assess the usefulness and efficiency in the sphere of internal security.

Furthermore even when it is possible to some degree to ascertain individual preferences as regards data protection - e.g. in the sphere of fees for requests for access - there is still the problem - quite different from the problem of public goods - of the divergence between individual and collective evaluations of the usefulness of data protection.

In this connection, cf. in particular the discussion on Musgrave's concept of merit wants: Musgrave/Musgrave/Kullmer 1975, pp 76-78; Recktenwald 1963, p 81; Recktenwald 1970, p 251, note 5; Hanusch 1972, pp 139-141 with further evidence and Sugden/Williams 1978, pp 179-180.

See also Mishan 1975, p 124 who points out that contrary to private goods, in the case of public goods individual marginal utility varies for different people.

As will be made clear below, benefits also arise from data protection which are jointly or individually achieved by and for the "provider" of the data protection, that is by and for the private and public bodies applying the data protection law. The determination of these benefits, which must be considered in particular in ascertaining the net debit of the data protection providers in accordance with business economics, is just as difficult as the determination of the benefits of data protection achieved on a joint or individual basis in the case of the data subjects.

4.2.1.2 External and opportunity costs: difficulties of determination

In the determination of the costs of data protection (in a concrete law or as otherwise defined) considerable difficulties are also encountered primarily in adequate consideration of all social costs (direct, external, intangibles etc.) as part of an analysis of social costs and benefits; these difficulties are no less in principle than those involved in the assessment of benefits.[1)]

1) To some extent there is certainly a tendency to underestimate the difficulty of determining data protection costs. For instance Futh 1976, p 228, points out: "Whilst the costs of data protection and data security are fairly easy to ascertain, the quantification of the benefits is however very difficult, in some fields even impossible."

   It is however clear from the context of this quotation that this idea is based on a restricted concept of cost-benefit analysis, oriented towards business economics; furthermore it will be clear in the course of the views to be considered below, that even the determination of the costs of data protection in terms of business economics is not without its difficulties.

Unlike more or less clearly circumscribed governmental investment projects which constitute the classic applications of cost-benefit analysis, the true investment and consequential costs of the "data protection project" appear as extremely widely dispersed, because not only is it necessary to calculate the costs incurred by the government in an enormous number of authorities and organisations, but also those incurred by private trade and industry.

As will be explained below, over and above the difficulty of determining the costs on the basis of business economics incurred by the (private and public) data processing organisations themselves, as well as by the state bodies carrying out the external data protection control, two further vital problems, which are considerably more difficult, arise in connection with the determination of the costs of data protection on a national-economic basis.

The first of these is the assessment for costing purposes of administration, which may in certain instances be considerable, though difficult to evaluate, yet which has been, so far as can be seen, almost completely overlooked in the data protection literature so far existant, which has, depending on the concrete design of the procedures for internal supervision (notification, granting of access, correction, blocking, erasure, etc.) been

unloaded by legislation and practice onto the data subjects, and which is to be considered from the point of view of costing in the framework of national economics as "external costs".[1)]

The second of these problems is that of determining the opportunity costs of data protection, i.e. the loss of benefit which arises due to the fact that as a result of data protection, certain data processing activities, actually desirable and beneficial either to individuals or to society (possibly including products and services based on them) cannot (any longer) be carried on; in addition there are the general inefficiencies in the sphere of data processing and decision-making resulting from data protection, which may arise in the form of less correct decisions or inefficient extra work and expenditure.[2)]

1) This unloading of administrative work onto the data subjects is regarded to some extent as a general problem in relation to government administration, in another connection, in conformity with the demand for "administration favourable to the citizen".

2) On the problems of opportunity costs ("alternative costs") of data protection, cf. Brussard 1975, pp 60-61. A concrete example of the "alternative costs" which may be incurred as the result of such a restrictive law is the comment made by the Insurance Industry Federation in "Deutscher Bundestag" (Federal German Parliament), Innenausschuss (Interior Committee) 1976b, p 131:

"A restriction on this activity (extensive research constantly carried out by the HUK Association regarding the causes of accidents) would lead to unpredictable personal and economic losses. It is generally known that the improvements in the road system made as a result of such research led to a reduction in losses which in its first year alone exceeded the road building costs involved."

The determination of this so-called "shadow price" of data protection, as thus defined, therefore requires an evaluation of alternative information utilisation possibilities prevented by data protection regulations, in other words, the determination of the "costs of the non-processing of data".[1)]

There are people who even maintain that such opportunity costs of data protection may considerably exceed the relatively small direct data protection costs. [2)]

1) The unusual form of the enquiry regarding the "costs of non-processing of data" is to some extent reflected in no less unusual concepts such as "negative information system", "cost of withholding information", "negative value of information" etc., as mentioned by Klempner 1973, pp 111-113, in his criticism, for instance, of the "excess secrecy or over-classification" in connection with the American "national secrecy apparatus".

2) Cf. the very decided remarks of Brussard 1975, in particular p 61 (the variations in the somewhat imprecise terminology are of no importance in this connection):

"The economic cost of protection of privacy is not very high, because most of the measures are required for technical and organisational reasons anyway. The price of privacy mainly consists of social costs in terms of desired ends which cannot be realised if protection of privacy results in restriction of data collection, processing, distribution, and utilization."

Cf. also in this connection Renninger/Branstad 1974, p 24:

"The importance of information in our service-oriented society leads to a consideration of the social costs of limiting access to data in the interest of protecting individual privacy and data confidentiality. Since data collection is often required to plan and operate needed service programs, lack of accurate data will either inhibit the development of these programs or raise the costs of implementing and operating them."

It cannot be denied however that there are quite considerable difficulties in the way of the determination of the so-called opportunity costs of data protection. Apart from the fact that such costs can, in the absence of an adequate empirical data basis, only be estimated, it is desirable to check carefully to what extent it is reasonable to interpret data processing activities as lost benefits, i.e. as opportunity costs, which the legislator deliberately desired to eliminate. Thus it seems fundamentally not very reasonable, to regard the benefits which some individuals would derive from certain acts as opportunity costs of the legal regulations, which label these acts as "illegitimate" and forbid them accordingly. Such prohibitive regulations have of course the aim of excluding certain actions from the sphere of legitimate alternative actions, even though the latter aim at some benefit. Thus for example the economic exploitation - which may possibly be achievable - of the processing and utilisation of very sensitive data, such as health, religion, political conviction, cannot very reasonably be taken into account as loss of benefit and therefore as opportunity costs, in respect of a regulation which deliberately excludes such processing and utilisation as illegitimate. It would be just as reasonable for a contrary approach to bring into consideration the proceeds of robbery with violence as opportunity costs of a legal prohibition of robbery with violence in considering the question of whether such a legal stipulation was useful.

We shall therefore be forced to the conclusion that only the unwanted, accidental and implicit side effects of a data protection regulation must be brought into consideration as opportunity costs. The determination of such effects, which present themselves rather as concealed losses, will however to a large extent have to remain hypothetical in nature.

4.2.1.3 The fundamental relevance of macroeconomic concepts

As regards these difficulties, of course, the desirability of such cost-benefit analysis, or utility value analyses, or other investigations of benefits and costs, has to be acknowledged, as well as the total research deficit, as far as this is discernible.

It should of course be appreciated that here we are advocating neither a pure economist's nor a pure monetarist's approach: naturally there is no question - as Auernhammer [1] has rightly pointed out - in the event of the result giving a negative balance, of mechanically following the path of economic consistency and voting against data protection instead of adopting a political decision oriented to the constitution. And of course by no means should the attempt be made, neither acceptable as regards content nor feasible in practice

1) Auernhammer 1976, p 1.

of setting a monetary value on all relevant positive and negative effects and aspects of data protection.

On the contrary, against the arguments put forward by those financially interested, based on business economics, and primarily profitability-orientated (which for instance in the case of the German Federal data protection law led to considerable concessions - not always justifying positive evaluation - on the part of the legislators to economic interests), recourse should rather be had to the methods and analytical resources of political economy only in support of political, juridical and other assessments, in order to reach rational legislative decisions bearing in mind the interests of society as a whole. In doing so it would be reasonable to make use, in some sectors where monetarist methods could reasonably be applied, of the methods of cost-benefit analysis - as the term itself suggests - to analyse the problem, not to decide the issue, and in addition to pay attention to qualitative aspects, by means of analyses of utility value and other methods of investigation of benefits and costs.

Besides extensively structuring the "expenditure/effect" problem of data protection, economic theory may make important strides, especially in the field of cost-benefit analysis and the theory of public goods, to a progressive conceptualisation of relevant aspects of data protection, which can be mentioned here only in passing

Thus consideration of the external costs of data protection draws attention to the problem of the administrative burden being put onto the shoulders of the citizen. Moreover, data protection as a whole could be regarded to a large extent (e.g. by analogy with requirements for environmental protection) as costs to be borne internally by the data processing organisations, whilst the concepts of the "free-rider" and the "merit-wants", for instance, provide arguments in favour of a policy of fees for requests for access regarding data protection in as much as they support the tendency for rather lower fees, and in any case refute the argument "data protection is worth as much as people are prepared to pay for it".

4.2.2 Limitations to microeconomic costs and benefits

In view of the considerable methodological and empirical difficulties of comprehensive national economic investigations regarding data protection, to which attention has been drawn, and of the terms of reference of the project, the present investigation is essentially concentrated on the problems which arise for the data processing organisations of the costs and profits of data protection in terms of business economics. However, the aspects of business economic profits, and general favourable effects of data protection so far as the users

are concerned, cannot be dealt with in much detail. It is essentially involved in the considerations by the arguments.

The expenses imposed on the data subjects are considered implicitly since the problem of fees for requests for access is investigated. The problem of the de facto burden over and above this, as a result of the imposition of a not inconsiderable administrative burden on the data subjects, already discussed (for example the data subject must in practice keep a record in the case of only one single - i.e. not periodical - notification, in order to have a reliable idea of the degree to which he is exposed overall to data collection procedures, and to make adequate use of his right of access), has not been investigated in detail, but will be considered argumentatively on relevant occasions.

4.2.3 Methodological approach of the study

Apart from an extensive international literature on various individual aspects of data protection costs, the investigation is primarily based on a few comprehensive systematic investigations. Numerous personal discussions and interviews with international data protection experts, and pronouncements of data processing organisations, associations, data protection authorities

and other relevant private and public organisations made it possible to check the existing documentation and to supplement it.

It was necessary to dispense with carrying out an empirical compilation of data protection costs on the level of the data processing organisations. For one thing, such a compilation would have had to be carried out internationally in accordance with the terms of reference, so that the scope of the investigation would have been considerably amplified. For another thing, however, the value of such a systematic compilation would necessarily have remained doubtful in the highest degree. Apart from the fact that in some countries there are still no (generally comprehensive) data protection laws, there are for practical purposes only three countries (Sweden, USA, the Federal Republic of Germany) with a more or less long experience of data protection on the national level. Moreover, German experience is limited in time, and American experience is still limited in terms of the sectors concerned.

In any case it must be made clear that data processing agencies, even though they are subject to data protection regulations, do not, as a rule, carry out an appropriate systematic costing procedure, so that even on the basis of a broadly based investigation in countries with a certain data protection practice, the degree of precision

of the cost assessments to be expected must remain extremely limited.[1] Any serious investigations of data protection costs are therefore distinguished by the way in which they emphasize how rough they are.

In view of this situation, the present investigation refrains almost completely from quantitative statements. It can however be assumed that the present investigation considers the international debate on the costs of data protection fairly exhaustively as regards its essential representative assertions and arguments. In spite of - or rather because of - the lack of quantitative (inevitably unreliable) information, in respect of the following emphatically qualitative considerations and results a high degree of reliability is therefore assured.

1) In this connection, cf. Betriebswirtschaftliches Institut für Organisation und Automation (BIFOA - Business Economics Institute for Organisation and Automation) of Cologne University as reported in the "Datenschutzberater 1979" 15.08.1979, p 10.

"... it was found in the assessment of the economic acceptability (of data security measures) that, owing to the lack of figures based on experience, a very high degree of subjectivity prevails in the assessment of risks and benefits. Morever, accountancy methods, almost without exception, are not detailed enough for accurate cost accounting and allocation, specifically of the organisational measures and the organisational adoption of technical measures. The assessment of the economic acceptibility of data security measures, and even the assessment of the costs incurred, will therefore for a long time still leave a lot to be desired. This will not be changed by various ideas suggested in current literature for the calculation of risks and benefits, as the necessary concrete basis of these is at present almost entirely lacking."

4.3 Costs of data protection: estimates and experience in selected countries

The estimates, investigations and experience in relation to data protection in the following four countries will now be critically considered and evaluated: UK, USA, Sweden and the Federal Republic of Germany. This choice was made in consideration of various aspects concerning content and pragmatic issues.

The three countries USA, Sweden and the Federal Republic of Germany are the countries with the greatest practical experience of data protection on the basis of national data protection legislation (in the case of the USA limited to the federal administration), so that as far as these countries are concerned it is possible to speak of a more or less consolidated experience.

So far as content is concerned, the Swedish model and the German model represent within Europe two essential basic conceptions or antitheses, round which the remaining European data protection laws are crystallising. Britain - whose decision process has not yet concluded - is obviously endeavouring to find an independent solution, and it is not clear how far this may lead to a third basic conception within Europe. The American approach in any case represents - primarily owing to its sectoral orientation, but also as a result of the avoidance of a special data protection control structure - an original conception, with which the European models come into conflict.

From a pragmatic point of view, Germany offers the advantage of a comprehensive data protection literature, whereas Sweden offers the advantage of the concentration of the relevant information and experience in the Data Inspection Board as well as the Swedish Federation of Industries. For both countries therefore, representative pronouncements can be made on data protection cost problems, although no special data protection cost investigations or comprehensive quantitative assertions exist. In the case of Britain, recourse can be had in particular to a very informative data protection cost study which was carried out on behalf of the British Data Protection Committee. As regards the USA, the favourable position prevails of the availability of a comprehensive systematic investigation and also an investigation resting on practical experience with the Privacy Act, with important quantitative contributions in each case.

4.3.1 United Kingdom

4.3.1.1 General data protection debate

Although UK has not yet passed a data protection law, it can already look back to a data protection debate lasting many years. [1)]

As might be expected from the pragmatic mentality of a trading nation involved for centuries with the international finance markets, cost aspects of data protection received fairly considerable attention in comparison to the international debate. [2)]

1) See for instance: Niblett 1971: Committee on Privacy 1972; Home Office (Cmnd 6353), 1975a; Home Office (Cmnd 6354), 1975; Committee on Data Protection (Cmnd 7341), 1978. See with particular reference to earlier legislative initiatives the Committee on Data Protection (Cmnd 7341) 1978, p 3, and as regards the British data protection debate the bibliography attached to the present investigation.

2) See for example the recent publications of Kenny 1976, Samet 1976; Douglas 1976; Anderson 1976; Avison/Crowe 1976; Institute of Data Proecessing 1976; British Computer Society 1976; Donovan 1977; Green 1977; Ellison 1977; Fishlock 1977; Computing Services Association 1977; British Computer Society/Computing Services Association/Data Processing Management Association 1978; Committee on Data Protection 1978; Lamb 1978; PA Computers and Telecommunications (PACTEL) 1977.

Very recently data protection costs have been the centre of interest at various conferences and seminars.[1)]

Essentially, however, the various statements were merely of an argumentative (sometimes even polemical) character and did not get beyond very partial and impressionistic estimates of cost. Even in the area of (technical and organisation) data security [2)] so far as cost aspects are concerned little more has been achieved than "pseudo-precision". [3)]

1) See for instance Institute of Personnel Management/ Computing Services Association: "Personnel, Privacy and Computers: the Cost to Management", 11 November 1976; BIS Applied Systems Ltd., London: "Computer Security and Privacy", 20 October 1977, London with a foreword by J R Ellison: "Assessing the Cost of Privacy Legislation"; National Council for Civil Liberties, London: "Computers, Records and the Right to Privacy", 24 - 25 January 1979, London with a special workshop "Computers and the Cost of Privacy Laws"; National Computing Centre, Manchester: "What Price Privacy?"; 11 April 1979, London.

2) In general, Britain may be regarded as in the lead in the sphere of data processing security in Europe; reference should be made here for example to the distinguished activities in this field of the National Computing Centre, Manchester, as the national focus, e.g. as part of the National Study Group on the Security of Computer-based Systems (1974), also to the various publications of NCC staff; cf. for example Farr/Chadwick/Wong 1973; Wong 1977.

3) Cf. for example F E Taylor 1974, p 1007"... axiom that, if the cost of obtaining information is greater than its value, then it is reasonably secure".

4.3.1.2 Special cost estimates

The following sample survey of various cost estimates which have been introduced into the British data protection debate should be mentioned here as a starting point for the further consideration of the matter:

- A fraction of 1% of data processing costs:

  In a paper read on 1 June 1976 to the British Society for Computers and Law regarding the Home Office White Paper on data protection,[1] Paul Sieghart, basing himself on estimates of the Association of Computer Users Groups, described the continuing additional costs required by data protection as "minimal". He estimated them at that time as "a fraction of 1% of data processing expenses.[2]

- 5 to 50% of the whole costs of the system:

  According to Avison and Crowe the cost incurred by a company on conversion of its whole system carrying out "adequate data protection" may amount to between 5 and 50% n extra. The authors however consider suitable measures for the protection of personal data as a burden which every system should incur, and which should be borne as ordinary business expenses, the same way as safety measures for the users of motor vehicles. [3]

1) Home Office (Cmnd 6353), 1975a.

2) See report of L B Anderson 1976, p 56: "Mr Sieghart, basing his opinion on figures given him by the Association of Computer Users Groups, thought that the additional running costs could be minimal (a fraction of 1%)".

3) Avison/Crowe 1976, p 12: "To add an adequate privacy safeguard to systems will, of course, involve a cost. The systems effort to change the whole of a company's current system could be large indeed, anything from 5 to 50 per cent more.... Nevertheless, adequate provisions for the maintenance of the privacy of individuals should be part of any system, and the costs borne as a standard cost in the same way as provisions are made for the safety of users of motor cars".

- 8 to 220%, or "more than a doubling of the data processing costs":

  According to press reports the Labour Member of Parliament for Basildon, Eric Moonman, is afraid that "the cost of safeguarding privacy for the individual could prove crippling to the smaller computer user".[1] Moonman based this assertion on "a US study which suggested that the cost could range from 8 to 220% of the basic cost of the computer installation".[2] Moonman also quotes the American consultant John Diebold, according to whom "privacy could more than double the basic computer cost." [1]

- data processing capital costs increased by between 11 and 185%, and running costs by 11 to 146%:

  J F Donovan [3] bases his remarks obviously on the investigations of Goldstein, but quotes another publication,

1) Fishlock 1977, p 9.

2) Moonman bases his remarks quite obviously on the study by Goldstein, as reported in Goldstein 1975c, pp 65-59, which is analysed in detail in 4.3.2.2 below. The percentage figures quoted therein relate to "privacy-related annual costs as percentage of original annual system cost", and not "basic cost of the computer installation" as given in Fishlock. Regarding the divergent figures given in the various publications of Goldstein see 4.3.2.2.3 and in particular table 4.6 including note 1, also the critical assessment in general in 4.3.2.2.4.

3) Donovan 1977, pp 18-20.

by Goldstein and Nolan.[1] Donovan therefore bases his remarks on an increase in capital changes for data processing of between 11 and 185%, and an increase in current DP charges of between 11 and 146%. [2]

Donovan also mentions that "another US authority has estimated that anticipated privacy-legislation will double the cost of data processing". [3]

- Price increases on important products and services:
  The Nationalised Industries Computer Committee [4] is reported to have declared in its comments to the Data Protection Committee that it was afraid that data protection legislation in accordance with a strict interpretation of the proposals of the White Paper [5] would be so expensive and costly that important products and services would be increased in price to the consumer. [6]

Without going into detail here regarding the estimates of costs quoted, the questionable nature of these and similar summary estimates of data protection costs is obvious. Even

1) Goldstein/Nolan 1975, pp 62-70.

2) See Goldstein/Nolan 1975, p 66.

3) Donovan 1977, p 19

4) Members: National Coal Board, Central Electricity Generating Board, British Rail, National Bus Company, BBC, British Steel, British Airways, Post Office.

5) Home Office (Cmnd 6353), 1975.

6) See Computing 1977, p 1

when - as in the case of Goldstein's works - the assertions made are supported by systematic investigations, such isolated figures are in practice worthless to the legislator as guides to his decisions, simply because of his inability to check them.

Furthermore, they suggest an unrealistic degree of precision, since the percentage figures frequently given usually relate to a basis which is not properly explained and defined, which in practice is in great need of interpretation and in fact is itself only an estimated figure. Furthermore, even the amounts to which they refer: "data processing expenses", "system costs", "data processing costs" etc. are far from being well defined. [1)]

Another point is that mostly general comments are made regarding the costs of data protection without any explanation of what concrete type of data protection forms the basis of the estimate.

1) In this connection it should be borne in mind that the attempt has already been made here as regards interpretation to achieve a certain degree of terminological predicability. The assertions reproduced are actually less well defined. For instance Moonman, as quoted by Fishlock, uses the extremely vague concepts "basic cost of the computer installation" and "basic computer cost". Sieghart, as quoted by Anderson in 1976, p 6, speaks only of "additional running costs" and also "increased ongoing annual costs". The reference item used by Avison/Crowe 1976, p 12, is "systems effort".

The only conclusion which can therefore be drawn from such estimates is that data protection may cost a great deal or very little, or actually only that there are some people who believe in the possibility of very high costs, and some who only expect low costs. On the whole the British debate regarding the costs of data protection up to the present corresponds for example to the position in the Federal Republic of Germany before the passing of the Federal Data Protection Law.

On the basis of extremely uncertain data and what is essentially a necessarily inadequate methodological foundation, the attempt is made to estimate in advance the cost of data protection in itself or the costs of a non-existent data protection law, the form and methods of application of which are still quite uncertain. At the same time, certain observations and estimates in relation to data protection costs merely serve to influence the eventual British data protection legislation to favour various sectoral interests.

4.3.1.3 The report of the Committee on Data Protection

The Committee on Data Protection (DPC, chairman Sir Norman Lindop) set up in July 1976 by the Home Secretary at that time, Roy Jenkins, attached particular importance both in the course of its work and in its report published at the end of 1978 [1] to the investigation of the cost aspects of data protection.

1) Committee on Data Protection (Cmnd 7341), 1978, chapter 22.

Like the previously published data protection report (White Paper: Computers and Privacy) issued by the British Home Office in December 1975 [1] and taking this as a basis, the DPC made a distinction between user costs and the administrative costs of a Data Protection Authority (DPA).

4.3.1.3.1 User costs: the PACTEL study

As regards user costs required to provide data protection, various views were put to the DPC, the majority of which foresaw considerable cost burdens. However, only a few of these were supported by figures, and where they were, very considerable differences were apparent. As with the views just considered above with regard to such ad hoc estimates, the DPC rightly considered these views as speculative.[2]

4.3.1.3.1.1 Terms of reference

At the suggestion of its costs sub-committee, the DPC therefore entrusted the consultant body PACTEL (PA Computers and Telecommuncations Ltd) with the carrying out of a limited investigation "to improve the understanding of the possible cost impact of data protection legislation". [3] It was hoped that in this way the following questions would be clarified:[4]

1) Home Office (Cmnd 6353), 1975a, paragraphs 32, 35 and 38.

2) Committee on Data Protection 1978, paragraphs 22.02, p 206: "The majority believed that the costs of their operations would be increased substantially by data protection legislation. Few could support their belief with figures, but where they did these varied enormously. Although such estimates were offered only after serious consideration, they were, of course, based on speculation and, at the stage of our enquiries, it could not have been otherwise".

3) The observations made here are based on the summing up of the PACTEL-study, PACTEL 1977, pp 1-15, the essence of which was reproduced as appendix 11 (ii) "Summary of the findings of the cost study consultants" in the report of the Committee on Data Protection 1978, pp 443-448.

4) Committee on Data Protection 1978, paragraph 22.04, p 207.

- "What factors could affect the cost of possible proposals?"

- "Which statutory principles were likely to be the most costly for users to meet?"

- "How sensitive the costs of different users would be to changes in levels of compliance for each principle?"

- "What levels of compliance might be achieved without significant costs?"

4.3.1.3.1.2 Conceptual and methodological approach

On the basis of preliminary work by the National Computing Centre (NCC) [1] and assisted thereby in the entire execution of the investigation, PACTEL covered 26 private and public organisations of a most varied character with a questionnaire and interviewing campaign (see table 4.1).

1) See for example Ellison 1977.

Table 4.1: List of organisations investigated (names not mentioned)

1. Multinational firm (personnel & payroll)
2. Light industrial firm (sales, purchasing, payroll and accounts)
3. Airline (seat reservations)
4. Clearing bank
5. Large finance house
6. Medium finance house
7. Life assurance company
8. Non-life insurance company
9. Bureau for domestic retailers
10. Cooperative retail business
11. Debt collection agency
12. Credit reference agency
13. Large mail order house
14. Credit betting organisation
15. Public attitudes research
16. Charitable organisation
17. Public aid association
18. Information analysis business
19. University
20. Regional health service
21. Electricity supply board
22. Local authority
23. Local authorities computer bureau
24. Governmment department (central records)
25. Government department (payments system)
26. Wholesale printers

Source: PACTEL 1977, p 3.

The questionnaire used [1] builds on a description of possible demands of data protection legislation (known as the "hypothetical basic scenario").[2]

The requirements explained in detail in connection with the questionnaire comply with the following six aims:[3]

1. Informing the data subjects of the fact, contents and purpose of the storage of personal data.
2. Informing the data subjects of the recipients of personal data.
3. Guaranteeing the correctness, relevance, completeness and up-to-dateness of the data.
4. Limitation of storage to the required period.
5. Guaranteeing the security of the data.
6. Protection during the processing of data referring to particular persons, or which can be traced to particular persons for statistical and similar purposes.

By means of several checklists[4] the costs which would be incurred by carrying out various more or less strict potential data protection measures to achieve the respective aims was then ascertained. For instance, in each case the cost was ascertained on the

1) The complete questionnaire is given in Committee on Data Protection 1978, Appendix 11 (i), pp 422-442.

2) Op. cit. pp 427-429.

3) Op. cit. p 445.

4) Checklists B1 to B6 in op. cit. pp 430-435.

basis of various different assumptions in relation to existing systems, for a single short-term conversion or a medium-term incorporation or re-development, also the additional running costs ("extra cost of operation"). In this way, by implication, the degree to which the organisations to whom the questionnaire was submitted already fulfil possible future requirements as regards data protection was established.

In special checklists[1] the amount of work and the costs involved were considered for the one-time short-term conversion for medium-term (hardware and software) system development, and the additional operations data protection costs according to the various cost factors (i.e. system audit compliance specification, equipment, software, machine time, organisation, staff, documentation, training, physical security, consumables, postage etc.).

Apart from general statements regarding total business costs, data processing system development and operating costs, finally details were requested regarding system characteristics, volume of data file and frequencies, processing and printing out statistics, also regarding the corresponding effects of data protection legislation.[2]

1) Checklists C1-C3, in op. cit. pp 436-438.

2) Checklists D1 and D2, in op. cit. pp 439-442.

In view of the limited nature of the resources available[1] the investigation was concentrated from the outset rather on the identification of cost focal points, i.e. the most expensive and cost-intensive elements of the hypothetical basic data protection scenario, and the data processing system elements with a determining influence on data protection costs.[2]

Instead of perfectionist and yet imprecise detailed cost calculations, all that was attempted was a realistic assessment of orders of magnitude[3] and "thresholds of pain"[4] of data protection costs.[5]

4.3.1.3.1.3 Results and evaluation of the study

The most important, in fact crucial, result of the PACTEL study is the conclusion, "that the (cost) impact of likely (data protection) regulations on the various respondent organisations will be very different: some

1) The Committee had only a budget of £9,000 available for the study of costs. See op. cit. p 443.

2) Op. cit. p 424.

3) Op. cit. p 423: "to agree on the order of magnitude of costs which could fall on computer users in various circumstances".

4) Op. cit. p 425.

5) Thus the cost estimates for the conversions or redevelopment were covered by the following scale: already complied with (1); no significant difficulty or cost (2); effort required: the whole team for a week (3); a month (4); a year (5); more than a year (6); cf. op. cit. p 425. The scale of the additional annual operating data protection costs amounts to: additional costs 0% (A); 1% to 2% (B); 3% to 5% (C); 6% to 10% (D); 11% to 20% (E); more than 20% (F); cf. op. cit. p 426.

general conclusions can be drawn, but only as a background against which to understand the considerable individual variations of each case".[1)]

The most important cost factors for the various organisations investigated can be seen in table 4.2.[2)]

The costs incurred in connection with the passing of information to data subjects are particularly striking: particularly the generally high postal charges, but also the costs of administration and the cost of stationery etc. Many organisations expect quite considerable data protection costs.

Apart from a few cases, the study shows smaller software development costs (new programs, data processing staff, modification of data files, etc.) than had been expected.

Additional hardware was generally not considered necessary. In a few cases however, need for additional printers was indicated in order to cope with the presumed extensive duties of informing data subjects.

The most important cost determinant factors[3)]

So far as the cost determinants are concerned, it seems particularly interesting that the technical design of

1) PACTEL 1977, p 2.

2) Source: PACTEL 1977, p 3; see also Committee on Data Protection 1978, pp 443-444.

3) Cf. in this connection op. cit. pp 444-445.

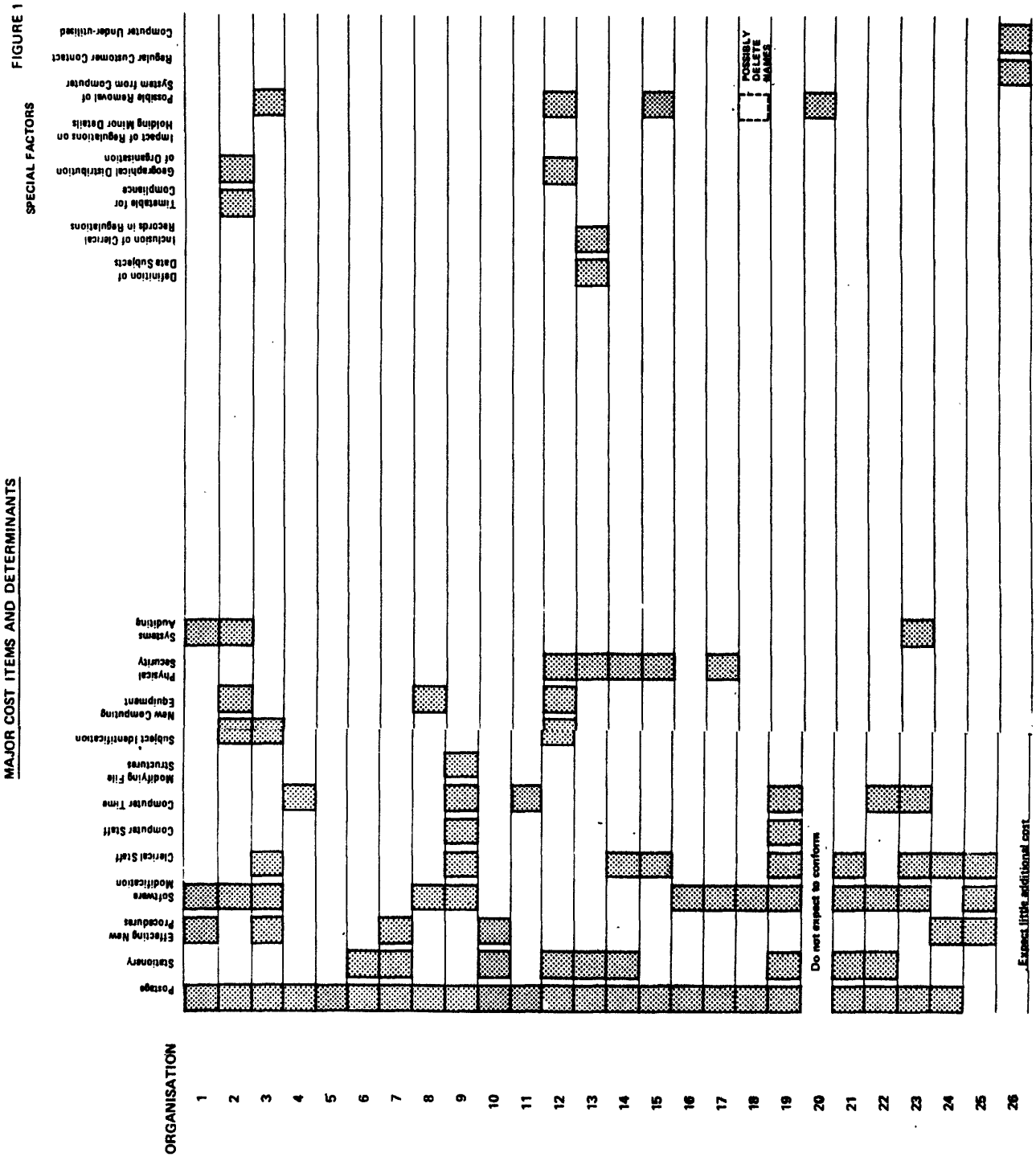


Table 4.2: Major cost items and determinants (PACTEL study)

the system, (e.g. large computer installation using magnetic tapes or a disc-oriented small computer) is not the decisive factor. Two exceptions must however be mentioned: the extensive use of terminals increases data security costs in comparison with centralised systems, and where there is extensive distribution of data files among several systems, the cost of passing information to the data subjects is increased.

As in the basic scenario only the automatic processing of personal data was covered, the question of the definition of automatic data processing is necessarily a cost-determining factor.

Furthermore, the study ascertained that the (additional) data protection cost incurred by a certain organisation is also dependent on how far the organisation in question is already subject to regulations or to supervision.[1] Already-established business principles and practices anticipating or facilitating security-orientated and other data protection measures result in similar effects.[2] The study also identifies as a further cost-determining factor, the question whether the data processing user has a direct or indirect or a continuous and regular or sporadic contact with the data subject.

1) Cf. for example the Consumer Credit Act in relation to credit reporting agencies.

2) Cf. for instance the security standards in the bank sector.

Besides other factors, reference is made in conclusion to the particular importance of flexibility in timing the introduction of the data protection regulations.

The relative cost in relation to the 6 fundamental aims is given in table 4.3.[1] Once more the particularly high costs for passing information to data subjects is very striking. It is no less remarkable that the majority of the organisations questioned do not expect any appreciable additional system security costs. For the rest, the PACTEL study comes to the not very surprising conclusion that the data protection costs in general depend essentially on the strictness of the requirements of the data protection regulations, and that each of the organisations investigated has its own special and individual sensitivity curve in relation to the strictness of the particular data protection regulations. This result is clearly shown in table 4.4.[2]

1) Source: PACTEL 1977, p 8; cf. also Committee on Data Protection 1978, pp 445-446.

2) PACTEL 1977, p 11. Although this table can only be adequately interpreted in conjunction with the original questionnaire, it is reproduced here as it illustrates very vividly the considerable differences in the sensitivity curves; cf. also Committee on Data Protection 1978, pp 446-448.

Table 4.3: Relative costs of meeting the six objectives at assumed levels of compliance (PACTEL study)

Table 4.4: Sensitivity to stringency within the six objectives (PACTEL study)

Evaluation

Obviously the concrete features of the basic scenario adopted and the individual assumptions and conditions on which it is based are of very decisive significance for the results of the whole investigation. It is not possible to repeat here the whole scenario as well as the assumptions and conditions adopted as a basis. However, in addition to the reference to the reprint in the report of the DPC[1)] it is perhaps worth while making the following comments on this scenario.

In particular, regarding the duties of informing data subjects, the basic scenario imposed very extensive, strict and inflexible requirements on users, which inevitably led to high cost estimates, without corresponding to actually expected legislation. Thus very short information time limits, and a probably far too high estimated proportion of requests for information, viz. 1% or even 10% of the total number of data subjects, were stipulated. Furthermore, the assumptions regarding the necessity of special postal notifications and information seem to be very much on the high side.

On the other hand, the data security requirements were not formulated with sufficient precision to give the various organisations under investigation the possibility of assessing what measures need or need not

1) Committee on Data Protection 1978, pp 422-442.

be taken as required for data protection in their concrete case. So far as can be seen, however, no systematic attempt was made by PACTEL in relation to the data security estimates of the organisations questionned to separate the costs required for data protection from those costs which would have to be borne on other accounts (e.g. compensation of a general security deficit, orderlines of data processing). Users have a tendency, due to lack of appreciation of such other elementary requirements, to ascribe data security costs excessively to data protection requirements, as they are often compelled to carry out measures, some of which are overdue, as a result of a newly introduced data protection law. In addition to the banks, the credit agencies are a good example of the view expressed here, as they have already been compelled by the British Consumer Credit Act to carry out certain measures relevant to data protection.[1)]

As regards British cost-consciousness and the recommendation of the DPC in favour of the adoption of a flexible procedure, it can be pointed out in brief that the qualitative cost assessments of the PACTEL study lie probably on - and even above - the upper limit of those costs which a possible future data protection legislation will actually cause.

1) Cf. in this connection, op. cit. p 444.

4.3.1.3.1.4 Conclusions of the DPC

The DPC was fully aware of the fact that "the information provided (by the organisations questionned) was based on the best estimates they could give, not on precise figures".[1)]

The conclusions drawn by the DPC from PACTEL's study of costs were accordingly cautious and very generalised: "The information which we have illustrates that any attempt to apply a simple universal requirement would be fraught with difficulty and could lead, in some cases, to disproportionate effects."[2)]

Furthermore: "The evidence also shows that, if a sufficiently flexible approach were adopted, it would be possible to devise a system of control by which each of the very different organisations included in our study could meet reasonable data privacy requirements at moderate costs".[3)]

"From the cases we studied there is support for the general proposition that if high costs look likely, there is either a serious deficiency in the current practices of the organisation in question, or the specification of privacy regulations to which it is to conform is inappropriate and could be improved."[4)]

1) Op. cit. paragraph 22.05, p 207.

2) Op. cit. paragraph 22.05, p 207.

3) Op. cit. paragraph 22.06, p 207.

4) Op. cit. paragraph 22.07, pp 207-208.

The DPC also found that future data protection legislation, especially in the area of informing the data subjects by the data processing user, would cause considerably less costs than the scenario on which the study was based (e.g. non-permissibility of unspecific "what do you know about me" requests etc.).[1)]

Moreover, the report of the DPC briefly states the most important results of the cost study of PACTEL and then comes to the following three conclusions regarding user costs.[2)]

1. "Our study strongly supports the flexible approach to data protection, based on Codes of Practice."
2. "The circumstances of users are so variable that it is most important that they or their representatives should be involved with the DPA in devising Codes of Practice so that adequate provisions are made both to fulfil privacy requirements and to moderate the cost and effort required from users."
3. "A DPA acting in this manner need not impose inordinate costs on users."

1) Op. cit. paragraph 22.08, p 208.

2) Op. cit. paragraph 22.11, p 208.

4.3.1.3.2 Access fees [1)]

The written comments submitted to the DPC tended to advocate the charging of access fees. Fees of 50p to £2.50 were proposed. As well as purely economic aspects of covering costs, the argument of the disincentive effect with regard to "frivolous requests" was especially put forward. The DPC refers also (besides various practical examples from the public sector), as a precedent, to the Consumer Credit Act of 1974, which in accordance with section 158 provides for a fee of 25p.

The DPC is accordingly of the opinion "that the argument about frivolous requests is sensible and it would be reasonable for a charge to be made for the work involved." [2)]

It therefore recommends "that each Code of Practice should specify the circumstances under which users may be allowed to charge a reasonable fee if they wish to do so." [3)]

In the opinion of the DPC, "reasonable fee" can mean that in some cases no fee at all will be charged, whilst in other cases the full information costs will be charged.

1) Cf. op. cit., pp 213-215
2) Op. cit., paragraph 22.33, p 214
3) Op. cit., paragraph 22.34, p 214.

At the same time the DPC rightly states that "uncertainty about the cost of making an enquiry could be a major disincentive for the data subject." [1] In the opinion of the DPC, any access fee to be paid should therefore be known at the time of the request for access. The basic principle for the approval of the amount of any access fees by the Data Protection Authority should therefore be that suitability for the data subject is given a higher priority than any disadvantages to the users, so that the aims of data protection are not frustrated by unsuitable fees.

4.3.1.3.3 Registration fees of the Data Protection Authority

On the basis of traditional pragmatism and a sense of mistrust of bureaucratic tendencies, the question of function, duties and material set-up of a future data protection authority was always an especially important point in the British discussion on data protection. In this context the variously stressed demand that the DPA (if it should come to that) "should pay for itself" [2] is a specific feature of the British discussion on data protection if an international comparison is made. The question of any registration fee or other fees to be paid to the data protection authority will therefore be of

1) Op. cit., paragraph 22.34, p 214.
2) Cf., for example, Home Office (Cmnd 6353) 1975a paragraph 38, p 11: "The objective, whatever choice is finally adopted, will be to make the Authority financially self-supporting."

significance for the estimation of the data protection costs arising for the users.

The DPC associated itself with the approach of the comment by the British Computer Society [1] in accordance with which the total annual budget of the data protection authority would be provided in the form of annual (licence or inspection) fees charged to the DP users (per installation).

On the basis of estimates (regarded by itself as speculative) the committee calculated an average fee of £26 in the case of a general registration of 20,000 applications with an assumed annual budget of the data protection authority of £520,000. In the case of a selective registration of 10% of the applications this fee would be £260 per application. A single user can be liable to registration in respect to several applications. In view of the principle that those who create the risk should pay, the committee does not regard such fees as excessive. [2]

The British Computer Spociety has rated an annual fee of £50 (per installation, however) as "reasonable". [3]

1) British Computer Society 1976, pp 26-27, Cf. also Committee on Data Protection 1978, paragraph 22.25 p 212.
2) Committee on Data Protection 1978, paragraph 22.26 p 212.
3) British Computer Society 1976, p 27.

The charging of a uniform fee for all registrations is considered by the committee to be indeed simple and cheap to handle, but as perhaps unjust. It therefore advocated variable fees according to application, the amount of which depends on the number of users concerned and the cost which the data protection authority has in developing the specific code of practice. [1] If the authority supplies additional advisory or other services to the users it would be able to charge the special costs arising through this. [2]

4.3.1.4 Summary

It can be stated basically that future British legislation, insofar as it adopts the flexible approach of the DPC, will cause no unreasonable and in general no heavy costs, whether for the data subjects, the DP users, or the public purse. [3]

Of special significance in this case will be the flexible formulation of legislation with regard to the transition time and also to the obligations of notification and information. The problems of notification and

1) Committee on Data Protection 1978, paragraph 22.27 p 212.
2) Op. cit., paragraph 22.31, p 213.
3) Thus also the estimation by the committee itself: "We have concluded that, if implemented in accordance with our recommendations, the scheme of regulation which we propose need not impose unreasonable costs on anyone - users, data subjects or the public purse." Op. cit., paragraph 26, p iii.

information obligations seem, however, to be less serious than the committee assumes. Apart from a few special situations, the users find, as practical experience shows, methods and procedures which enable them to fulfil these obligations at absolutely marginal costs. As opposed to first appearances and corresponding statements [1], especially in the case of automatic systems and periodic direct contact with the data subject, the annual routine notification or giving of information to all data subjects can be the less expensive solution, which in addition can also have certain positive side-effects (public relations etc.).

Even with regard to access fees a more liberal attitude justifies itself. This is so, on the one hand, because with regard to the (as experience shows) generally low number of information requests there is hardly the necessity of disincentive for "frivolous requests". On the other hand, the true costs of collecting the access fees (which for political and legal reasons should in any case be as low as possible) usually exceed the amount of the fees. [2] Characteristically, the majority of German companies waive such fees although these can be set considerably higher in accordance with the German Federal Data Protection Law.

1) Cf. (for example) Ellison 1977, p 2.
2) Cf. the proposals made by the Committee on Data Protection for fees between 50p and £2.50. Committee on Data Protection 1978, paragraph 22.32, p 213.

Even the concept proposed by the DPC with regard to a fully self-financing data protection authority by means of annual registration fees which vary by sector seems worth reconsidering. Apart from the fact that the concept of an annual fee similar to a data protection tax appears to be unusual and possibly is not acceptable to the users, the putting into practice of this concept brings up various practical and legal problems. The Swedish Data Inspection Board, due to such reasons and experience, tends towards a reduction if not an elimination of such registration or licencing fees. In any case, it gives basic priority to a low lump sum which is not necessarily dependent on costs.

It must be noted at least at this point that the licensing system turned down (inter alia) by the British DPC, mainly due to cost reasons, appears to be quite practicable without any unreasonable costs as the Swedish experience shows. [1)]

Above all, it seems worth mentioning in this connection that, within the framework of the British discussion on data protection, the practical usefulness of a licensing system which goes beyond mere registration is recognised to a certain extent by those engaged in the field. An essential argument is, on the one hand, the general

1) Cf. also the positive evaluation of British Computer Society 1976, pp 15 ff and also Douglas 1975, pp 36-37.

calming effect on the public and, on the other hand, the security which a licence, similar to a trade mark, gives to clients and other business partners, quite apart from the security in the sense of foreseeability which arises for the company seeking licensing itself. [1)]

With regard to a future data protection authority and the costs caused by it, the proposal of the DPC that such an authority should prepare about 50 different codes of practice and then monitor their application is of special importance. There is the fear that in this aspect the practicable flexibility expressly aimed at by the committee is turned into costly complication. The notion that one and the same user in certain circumstances with regard to different applications (but using the one and the same computer and operating team) would be subject at the same time to different codes of practice prompts the impression that there must be simpler and cheaper possibilities of practicable data protection both at the level of the data protection authority and the DP user. (Sweden seems to have found such a way.) At any rate, the critical reaction to this by the Law Society, as

1) See especially Benjamin 1978a, pp 5-7, where, amongst other things, the special value of "security certification" by the licensing data protection authority for service computer centres is stressed. Correspondingly and partly with the same wording - European Computing Services Association 1978, pp 5-6.

representative of British legal practitioners, confirms the misgivings expressed here. [1)]

The points of criticism expressed against the report of the DPC cannot be developed further at this point since this would exceed the boundaries of the subject dealt with here. They have solely the purpose to show at this point that future British legislation with suitable formulation would cause rather less effort and costs than the DPC forecast. And yet in this connection it still remains unconsidered that certain measures required by a future data protection law (not only in the sphere of data security) would have to be taken mainly due to other reasons, and that in addition data protection measures would partly bring on considerable and, in certain circumstances, even over-compensating positive effects for the specific user.

The problem of possible distortion of <u>international competition due to data protection</u> is basically merely mentioned by the DPC as also in general in Britain. In this respect it is only the most striking cases which are treated, in which certain international processing of

1) <u>Computer Talk</u>, 27.6.79, p 5: "Although the (Law) Society's preliminary report on the proposals (of the DPC) agrees with the recommendations of the committee it finds that they are too complicated to be practical in the UK legal system.... The Law Society ... argues that the large number of proposed codes of practice and the possible overlaps between them lead to legal confusion."

data concerning persons is explicitly forbidden, especially because there exists no data protection legislation in the specific country which corresponds to that of the country of origin. [1)]

That these are causes of distortion of international competition due to data protection is obvious. And relevant associations such as the Business Equipment Trade Association (BETA) and the Computing Services Association (CSA) insisted in their comments that future British legislation be harmonised with that of other countries and international agreements. [2)]

However, signs or even only fears that distortions of international competition caused by data protection costs which are of practical significance can occur cannot be clearly seen from the report of the British DPC. Obviously such fears have not been expressed, or at least not substantiated, either in the comments of the British industry to the committee.

1) In this case it is a question of the continually quoted few decisions of the Swedish Data Inspection Board not to permit certain processing of Swedish data in England or the export of personal data from Swedish subsidiary companies to foreign parent companies. Cf. Committee on Data Protection 1978, paragraph 4.58, p 34; paragraph 4.58, p 34; paragraph 27.08, p 246; also paragraph 27.16, p 248 where in a footnote Transnational Data Report, vol 1, no 3 June 1978, p 4 is given as the source.
2) Cf. Committee on Data Protection 1978, paragraph 27.22, p 249.

4.3.2 USA

Although the USA does not have general legislation encompassing both the public and the private sector, the American data protection and data security debate, as well as experience in various sectors, have given essential insight into the question of data protection costs. The following statements cannot therefore cover the American discussion and the various experiences in their full breadth.

We shall therefore in the main dispense with going into the individual cost estimates which private industry and its representatives made, especially in the numerous parliamentary hearings on various data protection laws. In this respect reference is made to the evaluation of the corresponding statements in Britain and the Federal Republic of Germany.

The various sector or individual state legislations (such as the Fair Credit Reporting Act, for example) cannot be gone into either. This lack seems, in the main, however, not to be serious. On the one hand (as far as can be seen) there are no comprehensive representative figures etc. available anyhow, and, on the other hand, certain pertinent statements and experience have been integrated into the considerations presented here. The value and representativeness of the statements made here, which are

based on relatively well founded sources, seem therefore to be basically assured.

4.3.2.1 Data security debate

By international comparison, the American data security debate, which has already been in progress for some years together with its ramifications in areas such as computer crime, military security, electronic funds transfer, cryptography etc. seems to be especially broad. [1] To the extent that data security is to be regarded as part of data protection and costs aspects are touched upon, the American data security debate is in principle of interest within the scope of the considerations presented here. [2]

Insofar as the various contributions to this debate are not too technical and do not have mathematical, software or engineering approaches as their theme ("data security engineering"), [3] their essential merit with regard to cost aspects lies in a general analytical structuring of data security efforts and the corresponding costs. [4]

1) Cf., for example, the various publications by Turn and the publications quoted in them. Cf. also Browne 1976.
2) Cf. in particular Turn 1973; Turn 1976a; Turn/Shapiro 1972; Turn 1974a; Turn 1974b; IBM 1974; Woodward/Hoffmann 1974; Chastain 1973; Nielsen 1975; Nielsen/Ruder/Brandin 1976; Anderson Company 1976; Hennings 1976.
3) Cf., for example, Turn 1974a.
4) Cf., for example, Turn 1976a, pp 248-250; Turn 1974b, pp 63-69, pp 101-118.

The basic aim in this case is to arrive at effective and low-cost security strategies. [1] Often concepts such as "cost of safeguards", "value of the (endangered) information for the data bank holder or the intruder", "likelihood of intrusion" are used without a precise definition, going beyond structuring and rough appraisal, being attained through this. [2]

Accordingly, only a few solitary partial estimates are made which do not in any way permit appraisal of the entire data security costs - quite apart from the fact that in the abstract and in general it is not possible anyhow. [3]

1) Cf., for example, the Protector-Intruder Interaction Model of Turn/Shapiro 1972.
2) Cf. IBM 1974, pp 101-118.
3) Turn/Shapiro 1972, pp 442-443, on the basis of other sources gives the following information: Cost of software implementation of (relatively sophisticated) access controls in operating systems:
Main memory requirements: 10-20%, programming time 5%, operating systems code: 10%, recurrent CPU time: 5-10%.

Computing time requirements for applying (substitution type) privacy transformations to 10-bit characters in a CDC 6600 computer (percent of databank operating system overhead): One-time Vernam ciphering: 0.66%, Vigeuère ciphering (table lookup): 3.5% Vigeuère (table lookup); 6.3%.
Chastain 1973, p 116 comes to the result, "security software should not degrade performance by more than 5-10%". He adds, "the determination of the actual effect of security software may be a complex and costly job." And Anderson Company 1976, p 1 comes to the conclusion, "After reviewing the availability of data that could be used in determining costs of computer security, it was concluded that it would be impossible to obtain comprehensive cost data for every item that might contribute to computer security cost."

However, it is the very limitedness of these results that is of indicative value here. It shows how carefully the cost estimates presented by interested parties with regard to data protection in general and to data security in particular have to be regarded. If in the field of data security, i.e. a rather technical field where mathematical precision is expected by the outsider, it is practically impossible to arrive at a general or at least specific definition or even an approximately precise appraisal of effort and costs, then this will be probably less possible in the more comprehensive field of data protection.

A further important aspect in this connection concerns the question of allocation of data security costs to data protection in general. In this case it can be clearly stated that the American data security and computer security research and debate in their coming into being and also in their further course are fully separated from the data protection aspect. The prime motivating aspects include (apart from the military sphere) in particular:

- protection against general computer crimes (fraud, sabotage, espionage etc.)
- protection of the technical data processing and telecommunications equipment as the vital infrastructure

- protection of the data files as valuable economic goods, or as the essential basis for the activities of private and public organisations.

The driving force behind the constantly increasing endeavours to protect computer and telecommunication equipment and the data is quite obviously not personal data protection but the general need of private and public organisations to protect, on the one hand, the economic values concerned and, on the other hand, their action capability. In view of the lack of data protection legislation in the USA which is generally obligatory for the private sector, the intensive interest and the multifarious activities with regard to computer security can only be explained by this. [1)]

4.3.2.2 Analysis of the Goldstein privacy estimation model [2)]

One of the probably most comprehensive systematic studies on the cost effect of data protection is the "privacy cost estimation model" which was developed by Robert C Goldstein in the form of a mathematical computer simulation model and used for estimating the cost effect

1) Cf., for example, the report by Pantages 1976 on a "Computer Security Conference" of the Computer Society Institute.
2) The following analysis of the Goldstein model is a revision of Hogrebe 1979, pp 492-503.

of a number of different data protection regulations on the personal data information systems of six selected data processing users. [1)]

4.3.2.2.1 Structure and function of the model

Since the original purpose of the Goldstein "impact model" consists in evaluating the cost effects of specific alternative data protection laws, 20 individual data protection "regulatory requirements" were formulated, in the course of analysis of a large number of various (American) data protection laws which had been proposed or already passed, in such a way that supposedly each of the data protection laws considered can be regarded as a definite combination of these 20 regulatory requirements. [2)] These requirements contained in this way in the "impact model" form (condensed in each case) the list given in table 4.5.

1) Cf. Robert C Goldstein 1975a: The Cost of Privacy: Operational and Financial Implications of Data Bank Privacy Regulation, 150 pp.
Cf. also the brief summaries in Goldstein 1975c, Goldstein 1975b, Goldstein/Nolan 1975 and Lobel 1975.

2) There are, however, data protection laws in existence or conceivable which, particularly from the point of view of costs, do not completely appear as a combination of these 20 requirements. For this see also the criticism of the Goldstein "impact model" below.

Proposed Privacy Requirements[1)]

The operator of a Personal Data System shall:

Subject Access Requirements

- Record Existence Notification /5/:
  Notify annually each subject of the existence and content of his record.
- Record Existence Inquiry /6/:
  Respond to inquiries from data subjects concerning the existence and content of their records.
- Record Uses Inquiry /7/:
  Respond to inquiries from data subjects concerning the uses of their records.
- Data Accuracy Inquiry /10/:
  Respond to complaints from data subjects concerning the accurancy of their records.

Subject Control Requirements

- Data Supply Obligatory Notification /1/:
  Notify each subject whether he is obliged to provide data.
- Consent for Additional Uses /2/:
  Obtain the consent of the data subject for each use of the data.
- Consent to Transfer Data /15/:
  Obtain the consent of the data subject before transferring data to a less protected system.

Data Usage Requirements

- Check Usage Authorization /3/:
  Check the authorization of each request for data.
- Maintain Usage Log /4/:
  Maintain a log of all accesses to personal data.
- Subject Claim Dissemination /12/:
  Include the data subject's statement with any release of disputed data.
- Retroactive Claim Dissemination /13/:
  Send the subject's statement to all past recipients of disputed data.
- Record Transmission /14/:
  Assure that any system to which data is transmitted will provide adequate protection.
- Legal Process Notification /16/:
  Notify the subject before data is released in compliance with legal process.

Operating Procedure Requirements

- Data Accuracy /8/:
  Assure the accuracy and completeness of the records.
- Additional Data /9/:
  Include any additional data needed to give a fair picture.
- Subject Claim Storage /11/:
  Store a subject's statement of dispute with his record.
- Physical Security /17/:
  Protect against threats and hazards to the security of the data.
- Employee Training /18/:
  Train all users in appropriate privacy procedures.
- System Assurance /19/:
  Assure that his system meets all of the requirements.

- Public Note /20/:
  Publish a description of his system where it will be seen by most data subjects.

Table 4.5 Individual privacy requirements taken into consideration in the Goldstein Impact Model.

1) The condensed wording given here and the division into four categories are taken from Goldstein 1975c, p 68. Cf. also Goldstein 1975a, pp 32-100.

After the (hardware, software and orgware) micro-operations required in each case had been specified for each of the data protection requirements, the type and volume of the corresponding system resources required by the micro-operations were defined for each individual requirement by means of a differentiated empirical survey. In combination with price information with regard to the various resources, the model can in this way determine the entire cost impact of the individual requirements. [1] The system resources (also called "functional elements" by Goldstein) required when doing this are divided into five main categories within the framework of the impact model [2]:

- manpower
- data storage
- computer processing
- data transmission
- capital.

Each of these categories is further subdivided in order to take into account the differences in performance and cost between the individual resources. In addition, the

1) For this see Goldstein 1975a, pp 17-18, and also Lobel 1975, p 938.
2) Goldstein 1975a, p 19. This division is contrary to the usual division of natural cost categories which differentiates between labour costs, material costs, capital costs, outside service costs and taxes; it appears here, however, to be fairly adequate. For the usual division of cost categories see Mellerowicz 1973, pp 36-42.

model differentiates between one-time conversion costs (5 functional elements) and operating extra costs due to data protection (11 functional elements).

In theory it is possible that each of the individual regulatory requirements can use any combination of the 16 functional elements. Which one is actually required by a certain individual requirement and to what extent is determined by the impact model (as already implied) depending on the characteristics (differently described by means of 29 "system attributes") of the information system considered in each case. [1)]

4.3.2.2.2 Application of the model

The impact model was tested on a group of six existing data banks which were selected in such a way that with regard to the whole of the (large automated) data banks carrying personal data a relatively high degree of representativity was attained.

The six systems are characterised in outline as follows: [2)]

1) For the individual "system attributes" see Goldstein 1975a, p 23. See also in general the brief description of the model in Goldstein 1975c, pp 68-69.
2) Cf. with the characteristics of the six systems studied, Goldstein 1975a, pp 29-31.

System 1 with stored treatment records for approx. 1 million persons is operated for a large network of hospitals. Batch operation, data (between 3000-4000 million characters) on magnetic tapes; weekly processing for updating and a large variety of reports; almost exclusively aggregated statistical outputs for management reports and planning; data on individual persons is very rarely called up.

System 2 is operated by a state government agency as an on-line system for identifying about 1.5 million persons arrested in the state in question and can be called up by all police organisations of the state and partly by neighbouring states. Connected to the National Crime Information Centre (NCIC) and to the National Criminal History System (NCHS) of the FBI.

System 3 is a state law enforcement system with on-line data files on all car registrations and driving licences of the state (about 18 million) and also a data file of approx. 30,000 outstanding arrest warrants and car theft notices. Each policeman of the state can either have the data base searched for a stated car registration indirectly via fixed terminals or himself search directly via mobile terminals.

System 4 is operated by a large consumer credit information organisation. The credit information supplied by the subscribing retail firms is stored in an

on-line system and can be called up by telephone via a terminal operator or directly via a small terminal in the store.

System 5 is an on-line personnel information system covering 10,000 employees which enables the interactive calling up of information concerning individual employees. Current function: payroll and similar work; also planned for the future: personnel evaluation and capability inventory.

System 6 is an on-line system operated by a large casualty insurance company and contains financial, legal, medical and general descriptive data on 3.3 million policy holders (mainly car insurance) which can be interactively called up by branch offices distributed throughout the country.

The structurally most important results are listed in extract form in table 4.6 in such a way that both the individual main resource costs and the cumulative financial total burden due to all the individual regulatory requirements outlined above are visible for the individual systems. In this connection the values of the cumulative total burden can be basically understood as being the upper cost limit. However, great caution is required in interpreting this information, as will be shown in more detail below.

Table 4.6: Estimated Privacy Costs for Six Personal Data Systems[1]

System	Data Subjects (thous.)	Charact. in Data Base (mill.)	Users	Trans-actions per Year (thous.)	Develop-ment Cost (thous.)	Old Annual Operating Cost (thous.)	Privacy Conversion Cost (thous.)	Annual Privacy Cost (thous.)
	2	3	4	5	6	7	8	9
1 Medical	1000	3500	50	2500	$ 726	$ 4000	$ 543	$ 1732
2 Law Enforcement No. 1	1500	32000	5000	110	$ 86	$ 477	$ 440	$ 1031
3 Law Enforcement No. 2	30[a]	19	5000	55	$ 3000	$ 2000	$ 348	$ 216[b]
4 Credit	35000	3500	500000	10000	$ 800	$ 14000	$ 1416	$ 20399
5 Personal	10[a]	20	45	50	$ 200	$ 340	$ 142	$ 40[b]
6 Insurance	3300	3600	60000	12500	$ 5000	$ 12500[a]	$ 573	$ 1880[b]

System	Privacy-related costs as Percentage of Original System Cost		Annual Privacy Cost		Percentage of Annual Privacy Cost Attribuable to				
	Initial	Annual	per Trans-action	per Data Subject	Clerical Tasks	Executive Tasks	Mailing	Data Stor-age and Processing	Sum 14–17
	10	11	12	13	14	15	16	17	18
1	75%	43%[c]	$ 0,72[d] ($ 0,69)	$ 1,80[d] ($ 1,73)	25%	41%	13%	18%	97%
2	512%	216%[c]	$ 9,64[d 2] ($ 9,37)	$ 0,71 ($ 0,69)	29%	28%	24%	16%	97%
3	12%	11%	$ 3,93 ($ 3,93)	$ 6,97 ($ 7,20)	29%	4%	5%	3%	41%[3]
4	177%[e]	146%	$ 2,05[d 5] ($ 2,04)	$ 0,58 ($ 0,58)	7%	15%	30%	46%	98%
5	71%	12%	$ 0,80[d] ($ 0,80)	$ 4,00[d] ($ 4,00)	40%	3%	0%	5%	48%[4]
6	11%	15%	$ 0,15 ($ 0,15)	$ 0,57[d] ($ 0,57)	23%	11%	5%	55%	94%

Notes to table 4.6

1 Source: Goldstein 1975a, p 31, figure 3 (columns 1-7 102, figure 39 (columns 8-9); p 115, figure 46 (columns 10-13); the figures in brackets in columns 2, 5 and 9; columns 14-18 are our own calculations on the basis of the figures of figure 39, p 102.

a) designates, for figure 3, p 31, deviating figures which are obviously errors and have been corrected in accordance with the figures on pp 30 and 113 respectively.
b) designates, for figure 39, p 102, deviating figures which are obviously errors and have been corrected in accordance with the figures on pp 108, 111 and 113 respectively.
c) designates, for figure 46, p 115 deviating figures which have been given as 45% and 22% and are obviously errors, and have been recalculated in accordance with information from figure 3, p 31 and figure 39, p 102. Goldstein 1975b, p 16, himself corrects the value for system no 2 and gives 222%.
d) designates such information from figure 46, p 115 which does not agree with the specific information in figures 40-45, pp 105-112, given for the six individual systems; the values found by our own recalculations are merely added in brackets since they are based only on the value already rounded off in columns 2, 5 and 9 and are therefore not necessarily more exact in every case.

2 This value (as also the corresponding value for the annual extra costs) is unusually high since the information system in question was still new and had only a limited operating volume. 57% of the also relatively very high one-time costs (cf. columns 6, 8 and 10) are attributable to the data security measures required by the special sensitivity of the data.

3 This relatively low percentage is explained, amongst other things, by the fact that this system has especially high data security costs, personnel training costs and similar costs. This also explains the high values for the system in columns 12 and 13 (in the case of the latter value the low number of data subjects, column 2, plays a role).

4 This relatively low percentage is also explained by an especially high proportion of data security costs of various categories.

5 The large difference between this value and corresponding value for system 6 (despite practically identical data volume and transaction volume) amounting to 0.67 is explained by the fact that the credit information organisation in contact with the data subjects has very high additional postage costs which do not arise for the insurance company due to its continual normal postal contact with the data subjects. With regard to the residual difference see Goldstein 1975a, p 115. The same applies for the high annual extra costs (column 11).

6 This high percentage is explained by the fact that 58% of the one-time conversion costs (column 8) was charged for training since the system has an unusually high number of potential users. These costs could, however, be passed on to a large extent to the organisations employing the users to be trained.

With regard to notification, information, correction requests etc. by the data subjects the following parameter values are taken as the basis: [1)]

- annual "record existence" notification requests = 1% of the records of a data bank
- "record usage" enquiries = 50% of the record existence notification requests (= 50% of the records)
- cases of dispute = 50% of the record usage enquiries (= 0.25% of the records)
- unresolved and stored cases of dispute = 10% of the total cases occurring (= 0.025% of the records).

4.3.2.2.3 Evaluation and results of the study

A brief evaluation of the Goldstein impact model including its test application is undertaken in the following statements. Without wanting to belittle the essentially positive overall judgement with regard to the differentiated systematic approach and careful empirical application with explicit declaration of the basic assumptions and limitations, a few brief points of criticism and comments are given here which with regard to the evaluation of the Goldstein study are of importance for the wider considerations to be presented here.

1) Cf. with the basic assumptions of Goldstein 1975a, pp 103-104.

Apart from the "technical" model improvements still to be carried out and which have been pointed out repeatedly by Goldstein himself, the necessity of a number of methodological extensions and improvements of the basic approach is to be taken into consideration when carrying out evaluation.

- A basic problem for the evaluation of the test results of the Goldstein study for the international data protection debate consists in the fact that the 20 modular basic regulatory requirements do not represent every existing or discussed data protection law.

- A further essential point of criticism is formed by the still unsolved problem of comparability of the cost burden determined for systems of different users, i.e. in particular to what extent the cost differences determined by the impact model do not only rest on different evaluation principles of the basic costing. [1)]

- The impact model does not sufficiently differentiate between data protection costs in the stricter sense and costs which, due to various miscellaneous aspects, motivations and obligations (especially data security

1) Thus Goldstein 1975a, p 48, himself states: "The cost differences, which may be either real or the result of different accounting conventions, may significantly affect the apparent impact of a requirement."

measures and orderly data processing for the user's own benefit), arise anyhow for the DP user or are (over-)compensated by corresponding benefits. Thus, numerous regulatory requirements analysed as to cost encompass data security elements which are not due to data protection in the stricter sense.

- In general, Goldstein (1975a) shows certain incoherencies and calculation errors in various figures. Thus, divergences arise between different tables and also in comparison with the figures stated in the text. Apart from printing errors, rounding errors and mis-calculations, certain divergences are explained by the fact that apparently figures from different development phases of the computer model are used. Characteristically, frequent deviations of varying magnitude between the figures in Goldstein 1975a and the subsequent statements by Goldstein can be listed. [1)]

In addition to these aspects of method, and apart from the basic problem of transferability of base data and

1) To preserve some coherency the figures from Goldstein 1975a have been taken as the basis in the main. Obvious errors have been cautiously corrected on the basis of these figures. Since these figures have, however, the indicated defects, no overall claim to precision is made here. Certain divergences from other figures stated by Goldstein, partly corrected (and partly also, diverging from each other) in other works are unavoidable but, in the main, are not decisive. Cf. in particular the tables in Goldstein 1975c, pp 66-67; Goldstein 1975b, pp 15-16; Goldstein/Nolan 1975, p 66.

result data related to American conditions, there arises a special problem when interpreting the test results of the impact model in regard to the empirical basis:

Due to the narrow empirical basis with regard to the future behaviour of the data subject and the possibilities of absorbing costs caused by data protection by means of adaptation of management policy and by means of technological progress, the dynamic aspect of the cost-relevant effects of future data protection is clearly neglected. Accordingly, the forecasting value of the specific results is reduced.

However, although the impact model cannot give any general or even any specific answer to the question of precise costs of data protection, it does give valuable service in the sense of "sensitivity analyses". [1)]

1) The possibility of using the "impact model" for carrying out sensitivity analyses becomes clear in comparison with the result data from Goldstein 1975 analysed here and listed in table 4.6 and with those from Goldstein 1975c, pp 66-67. There a report is made on a simulation run, carried out with regard to the same six information systems, which determines the cost effect of the "privacy requirements" which are defined by the Federal Privacy Act of 1974 which is, however, basically applicable only to the American Federal agencies. In spite of a few, partly quite significant, differences, this simulation run confirms the results analysed here with regard to the basic trend and also essential details.

The, in this sense, general results and conclusions which can be obtained from the specific application of the "impact model" to the six personal data banks are now evaluated below with regard to their basic consequences for the different points of view of the legislator, the computer (hardware and software) industry and those responsible for data banks.

4.3.2.2.3.1 Data protection cost structure

The impact model can (with the limitations imposed) assist the legislator insofar as it enables the individual data protection requirements under consideration to be arranged in accordance with their cost intensity, and in this way the discussion carried out up to now intuitively about the economic expenditure connected with certain data protection regulations is put on a rational basis. Thus, by using the model, the considered individual requirements which only cause "nominal costs" can be identified. These include [1]:

- check usage authorization/3/
- maintain usage log/4/
- date accuracy/8/
- additional data/9/
- subject claim storage/11/
- subject claim dissemination/12/
- data transfer consent/15/
- public notice/20/

1) With regard to the specific percentage share of each individual regulation in the total data protection costs of each system see Goldstein 1975a, figure 9, p 48; 11, p 53; 19, p 69; 20, p 72; 24, p 78; 27, p 81; 31, p 83; and pp 99-100.

The most surprising thing in the case of this relatively comprehensive list is the appearance of the "maintain usage log" requirement, i.e. the obligation of keeping a record of all accesses and processing operations with regard to data relating to persons. Whilst other voices regard usage logging as so expensive "that it must be regarded as the ultima ratio of the control of observing data protection provisions"[1], Goldstein states:[2]

> "Most striking is the low cost of maintaining a usage log. This is potentially one of the most useful of the proposed regulations because it provides a lot of information to data subjects and also provides a way for data system operators to inhibit improper activities by their own employees. The low cost stands out because this requirement initially appeared quite expensive.
>
> The cost analysis of Figure 11 confirms that this requirement does not impose a serious burden on any of the systems. The two systems that show relatively large unit costs for maintaining a usage log are those with the smaller number of subjects. Usage log maintenance costs are nearly constant for all the systems, so it appears to be a relatively greater burden for the small ones."

1) Zimmermann, D.1976, p 206

2) Goldstein 1975a, pp 52-53.

System	Percentage of Total Privacy Costs		Annual Cost per Subject
	Conversion	Annual	
1	-	-	-
2	-	-	$ 0.20
3	1%	3%	-
4	9% [1]	-	$ 0.60
5	-	15% [2]	-
6	2%	1%	-

Table 4.7: Cost analysis - maintaining usage log

Source: Goldstein 1975a, figure 11, p 53.

Given the narrow empirical basis, a final comment is not possible here. However, it is expedient in any case not to exclude the logging obligation too quickly from the area of potential data protection regulatory provisions.

Of the regulatory requirements tested, three provisions cause, in general, high one-time (conversion) costs.[3]

1) This value is given in Goldstein 1975a, figure 43, p 110 as 10%; the difference is probably due to different rounding off.

2) This value is given erroneously in Goldstein 1975a, figure 44, p 112 as 23%; for this see also above the remark 1b), to system 5 in table 4.6.

3) For this see Goldstein 1975a, pp 118-120.

One-time costs

(a) "data supply obligation notification"/1/:

This provision causes high conversion costs since it makes existing data acquisition forms obsolete. A suitable period between the passing and the coming into force of a corresponding law would defuse this problem to a great extent.

(b) "physical security"/17/:

The costs arising through this provision are the highest of the one-time costs for the reason that many DP users have neglected data security up to now. Since, however, the data bases are of such value for the users that increased data security is necessary in any case in their own best interests, the inclusion of the total data security costs constitutes a great distortion for data protection costs.

(c) "employee training"/18/:

Data protection training costs can vary greatly depending on the specific situation; in the initial phase in particular they tend to be very considerable. In the frequent cases, in which many users are not employees of the organisation operating the data bank, the costs can, in certain circumstances, be partly passed on to outside users and organisations.

Operating costs

(a) "(annual) record existence notification"/15/:

Since this provision has been recognised from the very start as being very cost-intensive, the "record existence inquiry" provision was tested at the same time, which as expected did not fall within the very costly measures.

(b) "record uses inquiry"/7/:

This provision can lead to high costs in the case of large transaction-intensive systems (here: credit information system and insurance information system) since larger and larger records have to be searched. If one does not wish to dispense with this provision due to the special importance for the data subjects (for these this is the only means to find out who has access to their data and why), then one could consider passing on the cost, at least partly, from the owners of the system. Since in accordance with the impact model this type of "record uses inquiry" costs between 25 and 30 dollars, a total passing on of the costs to the inquiring data subjects would, however, have a prohibitive effect. Apart from different mechanisms for passing on costs, a reduction of these costs by improvement of the technology is therefore of special importance.

(c) "data accuracy"/10/:

The decisive cost element is the personnel cost of dealing with complaints. However, this could at the same time give the system operator a greater incentive to improve the quality of the data.

(d) "physical security"/17/ and

(e) "system assurance"/19/:

These measures represent, on a percentage basis, very high data protection cost elements for the small systems no.3 and no.5, since it is essentially a question of costs which do not correlate with the size of the specific data bank.

4.3.2.2.3.2 Industry aspects

The conclusions which arise for the computer industry show data protection to be a great challenge and opportunity for the development and sales of new products relevant to data protection. The most important potential developments include [1]:

- user and terminal identification equipment
- larger and quicker direct access memories
- computers with secure access-checking devices
- computer assistance in data protection training
- automatic notification systems and interactive information systems for direct use by data subjects.

1) Cf. Goldstein 1975a, pp 122-124.

Viewing the development of such hardware and software products, it can be reliably expected that some of the data protection measures studied here will clearly be able to be fashioned less expensively in the future than it appears at the present time.

4.3.2.2.3.3 User aspects

The fact that fairly effective data protection can to some extent in a specific situation bring about considerable burdens for person-related data banks is certainly unavoidable. However, the Goldstein study also shows a few important possibilities for the operators of data banks to reduce the specific cost burden by data protection.

Thus, after the coming into force of a data protection law, the users will certainly be able to an increasing degree to call on cost-reducing new developments relating to data protection in the field of hardware and software products of the DP industry. Goldstein points out, for example, that the one-time conversion costs arising for programming in the case of systems which use a data management package are probably considerably less than those of other systems.

System	Data Mgmt. Package?	Programming Cost (1000's)
1	No	$ 180
2	No	$ 117
3	Yes	$ 19
4	No	$ 477
5	Yes	$ 9
6	Yes	$ 73

Table 4.8 Impact of using a data management package
Source: Goldstein 1975a, figure 50, p 126.

Flexibility and innovation with regard to the organisation, and business policy relating to data protection, will further contribute to limiting the cost. For example, flexible and fair dealing with individual requests for information, notification, blocking and erasure can in certain circumstances prove to be a cheaper solution. A further important element will be the exhausting of the possibilities of any transferring or passing on of costs to the data subjects, to other direct or indirect system users and also, in principle, to prices.

In addition, there is, technically in terms of figures, an essential reduction of the data protection cost estimates by observing the causation principle of costing. The impact model is not able to differentiate to what extent various measures are to be costed to data protection or to what extent they will (should) be taken in any case in the best interests of the specific organisation in accordance with the principles of orderly data processing (which go far beyond mere data security aspects) or with regard to other aspects, i.e. they are not caused only by data protection, and therefore cannot (to the full amount) be regarded as costs of data protection.

To what extent a differentiating costing can and must reduce data protection costs in this case in terms of figures (to define a realistic decision basis for the legislator) is already shown, for example, by the considerable proportion of the costs (which can be seen in table 4.9) attributable alone to physical data security measures ("physical security") out of the total costs calculated by the Goldstein impact model.

System	Percentage of Total Privacy Costs Conversion	Annual	Annual Cost per Subject
1	20%	-	-
2	57%	9%	$ 0.07
3	38%	19%	$ 1.35
4	8%	-	-
5	81%	30% [1)]	$ 1.20
6	35%	-	-

Table 4.9 Cost analysis - physical security

Source: Goldstein 1975a, figure 34, p 92.

A large part of just such security measures is, if it does not already exist anyway, to be taken in the best interests of the user (protection of the DP equipment, business data etc.) or due to reasons other than data protection. [2)]

1) This value is given erroneously in Goldstein 1975a, figure 44, p 112 as 46%; for this cf. also the remark 2) on table 4.7 and 1b) on system 5 in table 4.6.

2) In this connection see Anderson Company 1976, p 2:

"Goldstein's study is not especially useful even in regard to physical security because it assumes that there was no physical security before and provides no standards on which to relate the estimated one-time costs for securing a site."

4.3.2.2.4 Conclusions

Due to various methodological and practical reasons the Goldstein results, as shown, cannot even be evaluated as a fairly exact calculation of the data protection costs actually arising. The results generated by the model are, however, suitable in certain circumstances, i.e. especially in the specific checking of the correctness and significance of the basic assumptions, in the specific situation in the sense of sensitivity analyses of a low cost data protection strategy at the level of the DP user. [1)]

The cautious evaluation made here of the results of the Goldstein studies is also backed up by the qualifications which Goldstein himself has made in the meantime with regard to the significance of his model. [2)]

1) For this see Goldstein 1978, pp 7-14 and also the corresponding review in Data Processing Digest, no.8 1979, p 11: "Because of the many unproven assumptions in this model, there is little reason to believe that the specific cost figures produced will be accurate for any particular organization. The real value of the model lies in using it to compare alternatives of various kinds."

2) Cf. the report of Edith Myers 1977, pp 240-242: "It was meant for comparative purposes. The comparisons were good, but the numbers it could generate in an actual run were not." And also a new modified model, "still won't be good enough to set a privacy compliance budget with, but it will compare alternative costs and be an aid to improving strategies. Comparisons will be good, not the numbers!"

Thus, he stated very clearly that absolute data protection costs cannot be defined by means of his model, but decision aids for the specific situation can be prepared for defining a low-cost data protection strategy at user level. [1)]

1) Cf. the report of Edith Myers 1979b, pp 79-81:

> "The use of a model tends to lend credence to conclusions reached, and as is often said of statistics, it is possible to produce almost any desired result by proper manipulation of the input data and assumptions. 'Different approaches will result in different costs', Goldstein said. 'Just as it is possible to use the model to identify low cost compliance technique for actual implementation, it could also be used to find cost techniques for lobbying purposes. For example, it will nearly always be true that 'add-on' compliance measures will cost more than ones that have been designed into a system initially.' But models do have their place in estimating privacy compliancy costs in Goldstein's estimation. He believes that they can be put to good use to minimize cost of compliance. This is a valid and potentially very productive use of the model. While it cannot be depended on to give correct cost estimates for specific situations, it can be used to test strategy alternatives to see what their relative impact on costs would be. We can also identify the regulatory provisions that account for large proportions of the total cost. Attention can then be focused either on achieving modification of those provisions or on developing better technological approaches to comply with them."

As a result, it is to be noted here that the figures of the Goldstein study on the total burden due to data protection, on the basis of various stated reasons and considerations, are probably in general to be corrected downwards in the main. In this connection it cannot be denied that certain interested circles of private industry and their lobbies make out the Goldstein model to be not applicable and even dangerous since, according to these voices, important cost factors have not, or not sufficiently, been taken into consideration and therefore unrealistic, i.e. considerably too low, data protection cost estimates have been arrived at. [1)]

4.3.2.3 Experience with the Privacy Act

In view of the various, more or less realistic, and substantially unsystematic speculations about costs which arise in certain circumstances for private industry on the basis of existing or future data protection legislation, the practical experience of the American Federal Administration in the application of the Privacy Act is of special importance.

1) Cf., for example, the statement of Robinson, representative of the Metropolitan Insurance Company in Edith Myers 1976, pp 181-182:

"We tried to use Goldstein's model, he said. It didn't work. ... He sees a potential danger in wide distribution of the model in that it could lead to cost figures lower then are realistic and could refute industry's stand that cost figures are almost impossible to get!"

This is particularly true because the results are available of a comprehensive survey of the Office of Management and Budget (OMB) on the one-time conversion costs and operating costs which were incurred by the Federal Administration up to the summer of 1976 due to the application of the Privacy Act.[1)]

Interestingly, Federal administration agencies were requested by the OMB within the framework of a survey in the summer of 1974, i.e. before the Privacy Act was passed, to draw up cost estimates. This survey was, however, discontinued due to the following reasons: [2)]

- "preliminary returns indicated that the lack of agency experience in implementing such legislation precluded making realistic estimates"
- "the nature of the legislation being considered by Congress was still evolving"
- "there were differences of opinion as to the operational implications for any given bill".

The OMB then made a cautious rough estimate of the application costs of the then draft of the law (H.R. 16373, 93rd Congress). [3)]

1) OMB 1977a; OMB 1977b, pp 22-23. Cf. also Privacy Protection Study Commission 1977b, pp 39-41.

2) OMB 1977a, p 1.

3) According to OMB 1977a there are no considerable cost differences between this draft and the Privacy Act.

It was estimated in this connection that "the cost of implementing H.R. 16373 would be in the order of $200 to $300 million per year over the next four to five years, with an additional one-time start-up cost of $100 million, which would be expended within the first two years (but that) a year's operating experience will be necessary before greater precision in the cost estimates can be achieved". [1)]

The survey of the OMB carried out in 1976 after about one year's experience with the Privacy Act arrived, however, at essentially lower cost estimates. According to these, the one-time conversion costs (start-up costs) (since the passing of the law on 1 January 1975) came to only about $29.5 million for the Federal Administration, whilst the first-year operating expenses came to only about $36.6 million. [2) 3)]

1) OMB 1977a, p 2 and appendix I, p 2.

2) Cf. Table 4.10 in OMB 1977a, p 5; cf. also OMB 1977b, p 23 and Privacy Protection Study Commission 1977, pp 39-40.

3) It is pointed out that these figures are also only educated estimates. The OMB made no attempt to check the basic figures of the individual agencies. OMB 1977a, p 3, itself carefully shows the methodological inadequacies and weak points of the cost estimates submitted, in particular: inadequacy of the cost accounting system, limited experience with the Privacy Act, difficulty of including cost savings due to data protection.

Tab. 4.10: Costs of Implementing the Privacy Act of 1974

(Outlays in Thousands of Dollars)

	SUMMARY-ALL AGENCIES				MAJOR RECORDKEEPING AGENCIES 4/ 5/				ALL OTHER AGENCIES 5/			
	START UP 1/		OPERATING 2/		START UP 1/		OPERATING 2/		START-UP 1/		OPERATING 2/	
Publication Requirements	$13,549	46.0%	$4,405	12.0%	$12,621	46.4%	$4,151	11.7%	$928	41.3%	$254	22.1%
Training	6,825	23.2	3,282	9.0	6,341	23.3	3,141	8.9	484	21.6	140	12.4
Granting Access	914	3.1	10,670	29.2	881	3.2	10,501	29.6	33	1.5	169	14.6
Correcting Records	483	1.6	2,116	5.8	472	1.7	2,091	5.9	11	.5	25	2.2
Security and Control	2,175	7.4	1,345	3.7	1,938	7.1	1,251	3.5	237	10.6	94	8.2
Accounting for Disclosures	667	2.3	9,415	25.7	633	2.3	9,319	26.3	34	1.5	96	8.4
New Data Collection Procedures	1,164	4.0	1,507	4.1	1,117	4.1	1,491	4.2	47	2.1	16	1.4
All Other Costs	3,728	12.7	4,012	11	3,234	11.9	3,615	10.3	494	22.0	377	33.0
Reductions from Records/ Systems Eliminated	-45	-0.2	-62	-0.2	-23	0.1	-38	-0.1	-22	-1.1	-24	-2.1
Collections	-2	--	-91	-0.2	-2	--	-90	-0.3	0	--	-1	-0.1
TOTAL 3/	$29,459	100%	$36,599	100%	$27,213	100%	$35,452	100%	$2,245	100%	$1,145	100%

1/ Start up costs include any one-time costs incurred from January 1, 1975 through September 30, 1976
2/ Operating costs cover the period September 27, 1975 through September 30, 1976.
3/ Totals may not add due to rounding.
4/ Major agencies are defined as those with 45 or more systems according to the data in the President's first annual report. The Civil Service Commission is included among the large agencies even though it reported fewer than 45 systems because of its unique personnel recordkeeping responsibilities and the size of the systems for which it is responsible. (The list of agencies in Appendix III is annotated to indicate the 21 major recordkeeping agencies.)
5/ The Government Printing Office costs have somewhat arbitrarily been allocated among the larger and smaller agency categories proportionate to the number of notices of systems of records published as of December 31, 1975; 86% to larger agencies, 14% to smaller agencies. No effort was made to allocate costs and Justice Department litigation and Civil Service Commission training are included in larger agency costs. None of these figures, however, is so large as to distort the results.

Source: OMB 1977b, p 23 and OMB 1977a, p 5

4.3.2.3.2 Analysis of the results

The anlysis of the cost survey covering 85 Federal agencies [1] permits a number of interesting observations to be made: [2]

- The publication requirements of the Privacy Act are by far the largest proportion of the one-time conversion costs ($13.5 million or 8%). This corresponds on average to about $2,000 per system. The expense of preparing and publishing the appropriate rules is included in these costs. $4.4 million, or 12% of the total operating costs, were estimated for the operating costs of the publication requirements.

- Data protection training costs (for internal measures such as attending courses of the Civil Service Commission) formed the second largest proportion of the conversion costs ($6.8 million or 23.6%).

- The general administration costs (including the various reporting requirements) were the third largest proportion of the conversion costs at 12.7% and represented 11% of the operating costs.

- The largest proportion of the operating costs was formed by the granting of information to data subjects (granting individuals access) ($10.7 million or 29.2%).

1) Cf. table 4.11 taken from OMB 1977a, appendix III, pp 1-2.

2) Cf. OMB 1977a, pp 4-8

Tab. 4.11: List of 85 Federal agencies which had published rules and notices of systems of records as of July 12, 1976

Council on Wage and Price Stability
National Security Council
Office of Management and Budget
Office of Special Representative for Trade Negotiations
Office of Telecommunications Policy
Inter-American Foundation
Overseas Private Investment Corporation
Agency of International Development
*Department of Agriculture
*Department of Commerce
*Department of Defense
*Canal Zone Government
*Department of Health, Education, and Welfare
*Department of the Interior
*Department of Justice
*Department of Labor
*Central Intelligence Agency
*Department of State
*Department of the Treasury
Energy Research and Development Administration
Environmental Protection Agency
*Department of Transportation
*General Services Administration
*Department of Housing and Urban Development
National Aeronautics and Space Administration
*Veterans Administration
*ACTION
Administrative Conference of the U.S.
Commission on the Review of the National Policy Toward Gambling
Advisory Commission on Intergovernmental Relations
Advisory Committee on Federal Pay
Amderican Battle Monuments Commission
U.S. Arms Control and Disarmament Agency
Board for International Broadcasting
Civil Aeronautics Board
*U.S. Civil Service Commission
Commission on Fine Arts
U.S. Civil Rights Commission
Committee for Purchase from the Blind and Other Severely Handicapped
Commodity Futures Trading Commission
Community Services Administration
Consumer Product Safety Commission
Equal Employment Opportunity Commission
Farm Credit Administration
*Federal Communications Commission
Federal Deposit Insurance Corporation

Federal Election Commission
Federal Energy Administration
Federal Home Loan Bank Board
Federal Labor Relations Council and Federal Service Impasses Panel
Federal Maritime Commission
Federal Mediation and Conciliation Service
+Commission on Federal Paperwork
Federal Power Commission
Federal Reserve System
Federal Trade Commission
Foreign Claims Settlement Commission of the United States
International Boundary and Water Commission, United States and Mexico
United States International Trade Commission
Interstate Commerce Commission
Marine Mammal Commission
National Credit Union Administration
National Foundation on the Arts and the Humanities
National Labor Relations Board
National Commission on Supplies and Shortages
National Mediation Board
National Science Foundation
National Transportation Safety Board
Nuclear Regulatory Commission
Joint Board for the Enrollment of Actuaries
Occupational Safety and Health Review Commission
Pennsylvania Avenue Development Corporation
*United States Postal Service
Postal Rate Commission
Privacy Protection Study Commission
Railroad Retirement Board
Renegotiation Board
*Securities and Exchange Commission
Selective Service System
*Small Business Administration
+Commission on White House Fellows
Tennessee Valley Authority
United States Information Agency
United States Railway Association
Water Resources Council
Pension Benefit Guaranty Corporation
Export-Import Bank of the United States

*Major agencies
+Report not received

Source: OMB 1977a, Appendix III, pp. 1-2.

- However, the recording of disclosure of data (keeping records to account for disclosure) came to nearly the same amount at $9.4 million or 25.7%, and therefore this proportion was considerably higher than expected.

- On the other hand, the costs for additional data security measures were, contrary to expectations, only 7.4% ($2.1 million) of the conversion costs and indeed only 3.7% ($1.3 million) of the data protection operating costs. This is probably due to the fact that some agencies with well run systems had to take only minor additional security measures at merely marginal costs whilst other agencies, on the other hand, had not yet adequately met the data secuity requirements of the Privacy Act.

- The cost savings shown in the survey due to the reduction of personal data maintained by Federal agencies caused by date protection are not significant. This may be explained, on the one hand, by the difficulty of determining whether and to what extent systems were reduced or not set up at all due to the Privacy Act. On the other hand, the administration agencies concentrated at the start more on their publication obligations and less on the reduction of the amount of personal data maintained. [1)]

1) OMB 1977a, p 6; cf. also OMB 1976, p 12.

In the subsequent period (1975-1976), however, a slight net reduction by 34 million records occurred. This reduction is, however, to be estimated higher looked at relatively in view of the general trend to increase data volume, especially since in the same period the number of Federal agencies has increased by 11 and the number of personal data systems of the Federal Administration has increased by 30. [1] The same tendency is to be found for 1977. The partly considerable reductions in a few large agencies were somewhat more than compensated for by growth in the case of other agencies. [2]

Apparently it can be assumed that in this respect there is still a very high potential for further reductions of data maintained. Thus also Bert Lance, Director, Office of Management and Budget: [3]

> "While I believe the Act has served to improve the administration of personal record keeping, I question the Government's need to maintain more than 6,700 personal data systems containing almost 3.9 billion records. Therefore, I have initiated a project to reduce the number of personal data systems maintained by agencies, the number of individuals on whom records are maintained and the amount of information maintained on each individual." [4]

1) OMB 1977b, p 2.

2) OMB 1978, pp 2, 4 and 7.

3) OMB 1977b, p 111.

4) With regard to corresponding specific efforts by various agencies see Privacy Protection Study Commission 1977b, pp 51-55.

In addition to these overall results, a comparative analysis of the data protection cost estimates of the individual administration agencies is very instructive. The basis for this is table 4.12 in particular, which gives (broken down into the individual agencies concerned) the data protection cost figures for 21 "major record-keeping agencies" summarised in table 4.10. This shows (as also from table 4.13, 4.14 and 4.15) a quite exceptional concentration on a very small number of agencies both from the aspect of the number of personal data systems and volume of data maintained, and also from the aspect of data protection costs and in particular the amount of information requested by data subjects. In the following, only a few of the most striking elements are discussed:

- 48% of the total operating data protection costs of all connected agencies fall to the Department of Defense, which operates about one third of personal data systems. This is attributed to the geographical dispersion of the operations of the Department of Defense and to the characteristics of the data subject (i.e. military and civilian personnel, who know and can easily look after their rights on information), whereas other agencies have very centralised data banks, whose data subjects are less aware of the Privacy Act. [1)]

1) OMB 1977a, p 6.

Table 4.12 Cost of Implement the Privacy Act of 1974
Reported by the 21 Major Record-Keeping Agencies

Start-Up/ Operating	Agriculture	Commerce	Defense	Canal Zone	HEW	Interior
Publication	$185,198	$195,279	$7,500,966	$166,688	$1,186,388	$87,713
Requirements	$81,483	$14,121	$2,344,490	$5,616	$471,224	$34,646
Training	127,920	67,476	2,063,036	20,149	721,012	355,854
	52,205	10,263	1,965,177	901	423,413	52,871
Granting Access	11,634	11,876	132,697	50	329,626	3,294
	39,641	28,871	3,105,884	24,187	755,071	11,265
Correcting Records	1,577	10,728	100,679	0	37,821	1,035
	3,500	150	1,706,672	8,296	62,009	1,879
Security and Control	20,920	88,860	575,776	6,505	362,870	75,330
	9,103	12,192	338,034	696	486,711	18,045
Accounting for	1,975	4,058	228,426	0	180,241	2,262
Disclosures	10,507	688	5,863,300	1,183	524,170	10,922
New Data Collection	9,867	1,778	861,566	0	51,141	13,126
Procedures	7,249	1,000	1,243,525	19,026	71,897	3,870
All Other	10,980	133,373	984,888	2,588	1,480,360	67,990
	58,455	211,221	917,467	16,466	1,504,783	61,434
Reductions from Record	-960	-1,000	0	0	-4,708	-25
Systems	-40	-4,544	-21,663	0	-3,500	-50
Eliminated						
Collections	-100	0	0	0	-19	0
	-700	-5	-42,331	-320	-800	-20
TOTALS	$369,011	$512,428	$12,448,034	$195,980	$4,344,732	$606,579
	$261,403	$273,957	$17,420,555	$76,051	$4,294,978	$194,862

Start Up/ Operating	Justice	Labor	CIA	State	Treasury	DOT
Publication Requirements	$259,411 $14,331	$67,881 $14,145	$5,400 $1,400	$190,000 $16,000	$579,354 $295,180	$103,969 $105,028
Training	116,624 $19,078	68,873 17,906	14,000 2,000	37,000 6,400	891,415 141,983	225,165 38,496
Granting Access	13,673 $3,384,040	2,760 13,544	0 630,000	2,500 171,500	245,204 973,426	50,212 61,514
Correcting Records	5,529 $12,685	6,929 550	0 100	3,000 800	16,220 152,748	261,286 76,176
Security and Control	77,886 $30,237	52,980 18,512	500 400	5,250 0	49,392 142,878	196,670 90,418
Accounting for Disclosures	21,056 $335,170	394 6,132	400 4,800	0 650	117,688 690,805	47,686 152,431
New Data Collection Procedures	669 0	680 1,010	50 0	400 900	19,830 15,713	37,525 56,472
All Other	47,905 $260,044	1,571 5,060	0 10,600	31,000 45,100	87,438 81,969	150,587 152,019
Reductions from Record Systems Eliminated	0 0	0 0	0 0	0 0	(455) 0	(3,700) (5,658)
Collections	-1,438 -15,671	0 -28	0 0	0 -200	0 -3,602	0 -400
TOTALS	$541,315 $4,039,914	$202,068 $76,831	$20,350 $649,300	$269,150 $241,150	$2,006,086 $2,491,100	$1,069,400 $726,496

Start-Up/ Operating	GSA	HUD	VA	ACTION	CSC	FCC
Publication	$349,300	$129,793	$624,793	$51,305	184,103	$75,485
Requirements	$170,200	$1,951	$178,744	$6,000	$101,565	$19,444
Training	292,100	80,649	728,128	9,632	226,607	9,026
	43,200	10,692	202,031	10,942	21,699	1,742
Granting Access	12,000	5,408	6,029	246	53,343	76
	26,200	7,278	884,231	25,947	329,366	6,402
Correcting Records	1,100	61	5,200	0	18,525	711
	5,200	183	9,258	0	32,657	834
Security and Control	131,200	41,331	98,024	5,805	131,657	2,641
	25,700	74	31,697	130	40,255	500
Accounting and Disclosures	15,500	1,280	1,221	51	4,864	7
	13,200	1,305	1,531,789	2,022	4,158	629
New Data Collection Procedures	22,300	316	59	0	85,050	7,787
	11,300	243	34,137	0	18,050	0
All other	105,600	25,114	52,827	0	36,409	0
	85,200	65,461	53,388	1,318	33,914	350
Reductions from Records Systems Eliminated	-12,300	0	0	0	0	0
	-300	-192	-300	0	-1,919	0
Collection	0	0	0	0	-20	0
	0	-244	-22,446	0	-164	-50
TOTALS	$916,800	$283,960	$1,516,281	$67,039	$740,538	$95,733
	$379,900	$86,751	$2,902,529	$46,359	$579,581	$29,851

Start Up/ Operating	Postal Service	SEC	SBA	TOTAL
Publication	108,044	8,851	110,000	12,621,421
Requirements	15,825	1,469	500	4,151,362
Training	261,592	25,135	0	6,341,393
	108,585	11,812	0	3,141,396
Granting Access	0	325	0	880,953
	21,350	1,420	0	10,501,137
Correcting Records	0	2,000	0	472,401
	16,150	800	0	2,090,647
Security and Control	14,157	358	0	1,938,112
	4,750	800	0	1,215,132
Accounting for Disclosures	3,315	3,045	0	633,877
	154,020	11,552	0	9,319,433
New Data Collection Procedures	0	4,800	0	1,116,944
	0	6,540	0	1,490,932
All Other	200	14,686	0	3,233,516
	37,215	21,901	11,500	3,634,871
Reductions from Records Systems Eliminated	0	0	0	-23,148
	0	0	0	-38,166
Collection	0	0	0	-1,577
	-3,264	0	0	-90,245
TOTALS	$387,308	$59,200	$110,000	$27,213,492
	$354,631	$56,300	$12,000	$35,452,499

Source: OMB 1977a, appendix III, pp 1-2

Table 4.13

Summary of Changes in Personal Recordkeeping by Agency

Agency	No. of Systems		No. of Individuals' Records (in millions)	
	1976	1977	1976	1977
Dept. of Defense	2,219	2,150	321.3	296.7
Dept. of HEW	693	714	1,313.0	1,345.1
Dept. of the Treasury	910	571	990.1	1,006.1
Dept. of the Interior	274	261	15.0	15.3
Dept. of Transportation	263	265	25.0	27.4
Dept. of Agriculture	235	234	28.5	31.9
Dept. of Justice	175	184	181.5	188.4
Canal Zone Government/ Panama Canal Company	133	133	2.5	2.4
Dept. of Energy*	-	112	-	7.2
Dept. of Labor	97	100	23.3	28.5
Securities & Exchange Comm.	99	99	2.7	2.7
Dept. of Commerce	95	99	446.8	432.2
Small Business Admin.	80	85	2.6	2.6
General Services Admin.	91	77	3.4	1.6
Postal Service	71	74	107.7	97.6
Fed. Communications Comm.	69	70	9.2	9.2
ACTION	61	61	.9	.8
Central Intelligence Agency	57	58	.1**	.2**
Dept. of Housing & Urban Dev.	58	53	27.2	23.1
Veterans Administration	52	52	156.3	159.2
Subtotals	5,732	5,452	3,657.1	3,678.2
Remaining agencies	1,021	972	332.7	337.3
Grand Totals	6,753	6,424	3,989.8	4,015.5

* The Department of Energy, created during 1977, adopted systems of records from the Energy Research and Development Administration, Federal Energy Administration, Federal Power Commission and parts of the Department of the Interior.

** The number of individuals in many CIA systems is classified.

Source: OMB 1978, p 9

Table 4.14

REQUESTS FOR ACCESS TO RECORDS

Agency Name	Total Received	Granted in Full or Part	Denied	Other[1]
Office of Technology Assessment	NR[2]	NR	NR	
Copyright Office	0	0	0	
Council on Environmental Quality	0	0	0	
Council on Wage & Price Stability	0	0	0	
National Security Council	NR	NR	NR	
Office of Management and Budget	11	0	0	11
Office of Special Representative for Trade Negotiations	0	0	0	
Office of Telecommunications Policy	NR	NR	NR	
Inter-American Foundation	1	0	1	
Overseas Private Investment Corp.	0	0	0	
Agency for International Develop.	NR	NR	NR	
Department of Agriculture	NR	NR	NR	
Department of Commerce	4,679	4,620	59	
Department of Defense	258,471	257,108	32	
Panama Canal Co./Canal Zone Gov't.	697	692	5	
Dept. of Health, Education & Welfare	149,277	127,498	124	
Department of the Interior	494	491	3	
Department of Justice	37,618	19,145	336	
Department of Labor	2,023	2,017	6	
Central Intelligence Agency	3,621	714	124	
Department of State	1,093	NR	NR	
Department of the Treasury	2,780	2,544	178	
Department of Energy	90	56	14	
Environmental Protection Agency	NR	NR	NR	
Department of Transportation	17,210	17,203	7	
General Services Administration	5,290	5,286	4	
Dept. of Housing & Urban Develop.	100	96	4	
Nat'l Aeronautics & Space Admin.	42	41	1	
Veterans Administration	922,811	907,308[3]	2,210	
ACTION	170	152	19	
Adminis. Conference of the U.S.	NR	NR	NR	
Advisory Committee on Federal Pay	NR	NR	NR	
Adv. Council on Historic Preservation	NR	NR	NR	
American Battle Monuments Commission	0	0	0	
U.S. Arms Control & Disarmament Agency	5	5	5	
Board for International Broadcasting	NR	NR	NR	
Civil Aeronautics Board	NR	NR	NR	
U. S. Civil Service Commission	2,352	2,329	23	
Commission of Fine Arts	2	1	1	
U.S. Commission on Civil Rights	46	19	27	
Cttee for Purchase from the Blind & Other Severely Handicapped	0	0	0	
Commodity Futures Trading Commission	4	0	0	4

Agency Name	Total Received	Granted in Full or Part	Denied	Other[1/]
Community Services Administration	35	32	3	
Consumer Product Safety Commission	NR	NR	NR	
Equal Employment Opportunity Comm.	8	2	2	2
Farm Credit Administration	1	0	0	1
Federal Communications Comm.	1	1	0	
Federal Deposit Insurance Corp.	19	18	0	1
Federal Election Commission	8	8		
Federal Home Loan Bank Board	NR	NR	NR	
Federal Home Loan Mortgage Corp.	NR	NR	NR	
Federal Labor Relations Council and Service Impasses Panel	0	0	0	
Federal Maritime Commission	NR	NR	NR	
Federal Mediation & Conciliation Service	0	0	0	
Federal Reserve System	51	50	1	
Federal Trade Commission	302	298	0	4
Foreign Claims Settlement Comm.	0	0	0	
Harry S. Truman Scholarship Found.	0	0	0	
Japan-U.S. Friendship Commission	0	0	0	
Advisory Comm. on Intergovernmental Relations	NR	NR	NR	
International Boundary and Water Commission - U.S. and Mexico	0	0	0	
International Trade Commission	0	0	0	
Interstate Commerce Commission	1	1	0	
Marine Mammal Commission	0	0	0	
Nat'l Advisory Council on Economic Opportunity	NR	NR	NR	
Nat'l Capital Planning Commission	50	50	0	
Nat'l Center for Quality & Productivity of Working Life	NR	NR	NR	
Nat'l Credit Union Administration	23	23	0	
Nat'l Foundation on the Arts and the Humanities	1	1	0	
National Labor Relations Board	112	112	0	
National Science Foundation	"Few"	NR	NR	
Nat'l Transportation Safety Board	0	0	0	
Nat'l Transportation Policy Study Commission	NR	NR	NR	
Nuclear Regulatory Commission	125	124		
Joint Board for Enrollment of Actuaries	15	NR	NR	
Occupational Safety & Health Review Commission	0	0	0	
Penn. Avenue Development Corp.	0	0	0	
Postal Service	NR	NR	NR	
Postal Rate Commission	0	0	0	
Railroad Retirement Board	NR	NR	NR	
Renegotiation Board	0	0	0	

Agency Name	Total Received	Granted in Full or Part	Denied	Other[1/]
Securities & Exchange Commission	54	20	1	33
Selective Service System	7,200	7,199	1	
Small Business Administration	182	172	12	
President's Commission on Personnel Interchange	NR	NR	NR	
President's Commission on White House Fellowships	NR	NR	NR	
Tennessee Valley Authority	27	27	0	
Internat'l Communication Agency	60	NR	NR	
U. S. Railway Association	NR	NR	NR	
Water Resources Council	NR	NR	NR	
Pension Benefit Guaranty Corporation	6	6	0	
Export-Import Bank	46	46	0	
TOTALS	1,417,214	1,355,515	3,203	

1/ "Other" includes requests withdrawn, cases where no record was found, requests still pending at the end of 1977, and requests returned for additional information, such as proof of identity and not continued by the requestor.

2/ NR = Not Reported

3/ Includes amendment requests.

Source: OMB 1978, pp 26-28

Tab. 4.15.: Summary Statistics on Request for Access to Records

Number of Total Requests Received	Number of Agencies	
> 100.000	3	5
10.000 - 100.000	2	
1.000 - 9.999	8	16
100 - 999	8	
20 - 99	11	70
1 - 19	13	
"Few"	1	
0	20	
Not reported	25	
Totals: 1.417.214	91	

Source: Calculations on the basis of table 4.14

- Costs for providing information arising in only six agencies (Departments of Treasury, Defense, Justice and of Health, Education and Welfare, the Veterans' Administration and the Central Intelligence Agency) accounted for 26.5% of the total operating data protection costs of all agencies and 93% of the total current information costs. [1] An even higher concentration accrued in 1977: more than 97% of the information requests were in respect of only five agencies (Departments of Defense, Justice, Transportation, Health, Education and Welfare, and the Veterans' Association). [2]

  This high concentration of information requests is, apart from the number and size of the affected systems and the volume of the data maintained, in particular conditioned by the sensitivity and the general significance of the data for its subjects. These agencies have thus a clientele, a sort of "natural constituency" which is not only numerous but also very active in making requests for information. In the case of the Department of Defense, these are for instance the military and civilian personnel, while the Federal law enforcement agencies count criminals among their "information clients". [3]

1) OMB 1977a, p 7.

2) OMB 1978, p 25.

3) See Comptroller General 1978b, cover page: "The most dominant category of requests identified by many of the agencies was individuals who have been or are subjects of Federal Investigations by the agencies. Some of these requesters were also identified by agencies as being criminals.

- The number of amendment requests, on the other hand, is relatively small and is concentrated on only a few agencies. These requests were in the main complied with (see table 4.16).

4.3.2.3.3 Conclusions

The following conclusions which can be drawn from the experience of the Federal Administration with the Privacy Act, and particularly from the cost survey of the Office of Management and Budget (OMB), apply basically also to private industry:

- Prior estimates of data protection costs can hardly be more than speculative and should be assessed with appropriate caution. Because of considerable methodological problems, even subsequent cost calculations remain more or less accurate estimates.

- The authorities did not come across insurmountable difficulties in the application of the Privacy Act. There were in general relatively small costs. In a few agencies (21) there were quite remarkable data protection costs amounting on average to $1.3 million for conversion, and $1.7 million operating costs, per agency. Considering the special characteristics (scope, contents) of the data bases in question, even those costs appear rather as relatively trifling, and in any case as reasonable. The majority of the authorities (64) recorded insignificant costs, averaging $35,000 for conversion and $18,000 for operating costs per agency.

Tab. 4.16: Summary Statistics on Requests for Amendments 1977 (Selection)

Agencies	Number of Requests for Amendments				
	Received	Granted in full	Granted in part	Denied	Pending
Department of Defense	15.048	14.939	43	64	2
Department of Health, Education and Welfare	7.295				
(Public Health Service)	102	98		4	
Veterans Administration	3.780				
Department of Transpar-tation	514	505			
Civil Service Commission	135	75			
Department of State	42	38			
General Services Administration	28	16			
Department of Justice (mostly FBI investiga-tive records)	197	8	58	131	
13 other agencies	926				
12 further agencies	no requests				

Source: OMB 1978, p. 308.

For all agencies (with consideration of the applicability of the findings to the private sector) it must be emphasised that the obligations of publication, which basically do not arise in the private sector, account for 46% of total conversion costs and 12% of the total operating costs of all agencies.

- The information and amendment requests do not appear to be the formidable problem that they are often made out to be. [1] (Misuse is virtually not recorded.) Seventy agencies received less than 100, i.e. a negligible number of such requests; sixteen authorities received a more or less substantial number of information requests and only 5 an extremely substantial number, without this appearing to be unreasonable in the specific cases in question.

  The relatively minute number of amendment requests can in practice be disregarded as a cost factor, the more so since these requests are predominantly complied with, which suggests that the positive effect of the improvement in quality of the data base prevails even from the point of view of the agencies.

1) See for instance the speculations by Golding 1974.

It is very likely that American data protection regulations for the private sector have or will have basically the same rather limited effects on costs. Experience, not only with the Fair Credit Reporting Act, points in this direction. [1] Any comment coming from private industry and suggesting high data protection costs is, apart from lobbying, mainly attributable to an inaccurate assessment in various aspects. [2]

1) See e.g. Whieldon 1979, p 56:

> "William O.Bailey, president of Aetna Casualty & Surety Co., Hartford, and a member of the Federal Privacy Protection Study Commission has found it hard to identify any explicit costs for his company in providing privacy protection of the kind that will be reflected in the draft bill that the Carter Administration will soon send to the Congress. (Among other things, that bill would grant individuals the right to see and correct insurance records and would compel insurors to inform individuals about adverse decisions.) That company, with annual revenues of $2.599 billion, simply incorporated nearly all the privacy provisions into changes that it was planning to make over a year or so. As a result, the cost was relatively small and even difficult to pinpoint."

2) See on this Whieldon 1978, p 56:

> "Another expert who believes that the cost of conforming to privacy legislation and regulations may be exaggerated is Dr. Lance Hoffman, associate professor in the Department of Electrical Engineering and Computer Science at George Washington University, Washington, DC. 'A lot of the additional cost isn't really associated with privacy itself but, rather, is the cost of putting procedures in place where none existed before. Those procedures might already be set up in a well-managed shop.'
>
> Hoffman, who also heads the Committee on the Right to Privacy in the American Federation of Information Processing Societies (AFIPS), insists that privacy considerations have been responsible for only a small amount of extra overhead cost.

As for the danger of obstacles and increased costs caused by different national data protection regulations, there are several realistic rather soothing comments from within the American industry, which regard such problems as normal conditions of doing business internationally. [1)]

(continuation of footnote 1 overleaf)

> Supporting Hoffman, D. Willis Ware says there's more than one reason that managers are concerned about privacy laws and regulations. 'It's clear that no one will be able to respond to privacy requirements unless he's completed the security job first, buttoning up the computer room, understanding how people there behave and putting controls on the system. What you find is that a lot of people talking about the cost of privacy are including in their estimates the cost of security. Security safeguards should be funded on their own merits, I believe.'
>
> Another reason, he contends, that concern may be exaggerated is that 'company managers haven't studied the details of proposed legislation and haven't thought through carefully what they'll be required to do. They're shooting from the hip.'"
>
> Cf. furthermore in this connection Whieldon 1978, p 58:
>
> "As Richard P. Cooley, a counsel for the Travelers Insurance Col., Harford, observes 'Access is the problem, not record keeping and record protection.'"
>
> To this the further comment has to be added that experience has already shown that even the right of access is not the formidably expensive problem it is often thought to be.

1) Barna 1978, p 37:

> "According to the Citibank spokesman, 'Any bank that operates multinationally is confronted with a lot of these kinds of issues... We will encounter varying degrees of operational difficulty, but that's unavoidable if we want to do business in a number of countries.' ... 'From everthing we've looked at, we can't see any particular problems', (Lynn) Brown (Director of data communications research and engineering for the $1.5 billion company) says."

4.3.3 Sweden

Experience under the Swedish data legislation is, in cost terms, of special importance for two reasons. Firstly, the Swedish Data Act has been in effect since 1973 and is thus the oldest data protection legislation at national level. It can therefore be described as positive experience. Secondly, the Swedish data protection model, along with the primarily self-control-oriented German Data Protection Law, and with the still more liberal British tendency for simple professional codes of conduct, serves sometimes as the archetype for restrictive bureaucratic data protection. In the international debate, data protection licensing systems like the Swedish are regarded (especially from American comments) as unwieldy, over-bureaucratic and (for the private organisations concerned) as unnecessarily expensive. In reality the Data Inspection Board (hereinafter referred to as the DIB) is certainly, on the contrary, quite unbureaucratic and efficient. [1)]

4.3.3.1 Licensing fees

The DIB levies licence fees on holders of data files but they are in most cases extremely low. Thus for the simplified licences (1972-1978 : 14,869 cases) a minimal

1) The following comments concerning Sweden are based in the main on extensive discussions which were carried out within the framework of various conversations with members of the DIB (especially the Director General Jan Freese and the Administrative Director Rabbe Wrede) and also with leading representatives of the Federation of Swedish Industries.
See also e.g. Freese 1978 and Westman 1978.

lump sum of only Sw. Kr. 200 (less than £25) is levied per data file, and less if several applications are dealt with together. Otherwise the DIB levies charges on the basis of a rate of Sw. Kr. 175 per man hour (1973-1978: 5,333 cases of regular licences and 1,023 cases of modifications). Higher fees (up to now not more than Sw. Kr. 20,000) are due only in the case of extensive and complex systems in the public sector.

In any case the DIB's fees, especially for the private sector, evidently offer no stumbling block.

It can be said in passing that where lumpsum fees for simplified licences do not apply, the DIB raise such cost-based fees with reluctance.

Its corresponding efforts vis-a-vis the government, especially with the Ministry of Justice, have certainly not yet had the hoped-for success. The DIB is aware of the fact that fees based on hourly rates can lead to unfair and unequal treatment. So when the processing of a non-typical case arising for the first time requires a great amount of work, it is faced with correspondingly high fees, while a subsequent similar case can be processed at a considerably lower cost as the preparatory work has already been done.

Moreover the flexible and extremely pragmatic approach of the DIB has the effect of keeping down costs to a large degree, as it reduces the (potentially considerable) conversion costs to a minimum.

STATISTICS OF THE ACTIVITIES OF THE DATA INSPECTION BOARD

Table 4.17 (date: 1.03.1979)

ACTIVITIES \ YEAR	1973		1974		1975		1976		1977		1978		Total	
	T	U	T	U	T	U	T	U	T	U	T	U	T	U
LICENCES														
11 Preliminary Inspections	-	-	20	-	6	-	6	3	7	2	3	2	42	7
12 Regular Licences	18	-	2494	198	925	11	488	9	793	300	615	53	5333	571
121 Simplified Licences	2	-	10266	68	1117	15	1162	6	1145	23	1117	138	14869	250
13 Reporting of Public Applications	135	5	55	1	9	-	14	-	17	2	6	-	236	8
14 Modifications	-	-	28	-	115	4	150	2	448	13	282	34	1023	53
15 Automatic Credit Information	-	-	3	1	-	-	1	-	2	-	-	-	6	1
16 Manual Credit Information	-	-	529	3	7	-	3	-	1	-	1	-	541	3
17 Automatic Debt Collection	-	-	1	-	-	-	2	1	-	-	-	-	3	1
18 Manual Debt Collection	-	-	214	16	51	9	22	2	23	-	29	13	339	40
19 Other Decisions	1	-	23	-	78	-	83	-	16	1	26	5	227	6
CONTROLS														
21 Data Protection Complaints	8	-	67	-	46	-	63	2	45	4	48	8	277	14
22 Credit Information Complaints	-	-	14	-	27	-	44	2	80	11	118	18	283	31
23 Debt Collection Complaints	-	-	16	-	33	1	33	-	65	19	44	19	191	39
24 Data Protection Control Initiatives	-	-	2	-	3	-	6	1	18	4	13	4	42	9
25 Credit Information Control Initiatives	-	-	-	-	1	-	-	-	1	-	2	-	4	-
26 Debt Collection Control Initiatives	-	-	-	-	1	-	5	2	3	-	2	-	11	2
28 Inspections	1	-	21	-	63	2	53	4	83	12	53	11	274	29
29 Other Decisions	3	-	58	-	13	1	26	7	26	4	32	12	158	24
INTERNAL ADMINISTRATION ETC.														
71 Budget Decisions	16	-	13	-	18	1	12	-	14	1	10	-	83	2
72 Personnel Decisions	4	-	14	-	6	-	-	-	3	-	-	-	27	-
79 Other Administrative Decisions	-	-	4	-	2	-	4	-	4	-	4	1	18	1
81 Opinions, General	18	-	42	-	48	-	35	-	47	-	49	2	239	2
82 Opinions re Complaints	-	-	6	-	18	-	12	-	7	1	5	1	48	2
91 Other Opinions	14	-	63	1	25	-	16	1	8	2	10	3	136	7
TOTAL	220	5	13953	288	2612	44	2240	42	2856	399	2529	324	24410	1102

T = Totals of Activities
U = Unsettled Cases

Source: Data Inspection Board

4.3.3.2 Requests for access

The danger of the occurrence of excessive costs through extensive notifications and giving of information is already reduced from the start in Sweden. The Swedish Data Act has no obligations for the general (automatic) notification of data subjects e.g. on initial storage. In the case of Sweden, dispensing with such an obligation was possible without reckonable loss of data protection control by the individual, as the licensing system of the DIB exercises centrally a fundamental and continuous oversight on the automatic personal data files to which the individual applying through the DIB can refer.

4.3.3.2.1 Volume of the requests for access

Although keepers of personal data files must without charge give to the data subject once within 12 months information on the relevant data, the number of information requests is by no means excessive. In fact the total of all such requests for Sweden as a whole for the first five years since the data legislation came into force is estimated to be only about 50,000. [1)]

In this the public sector is more affected than the private sector. The National Statistics Authority constitutes the most prominent case. After a campaign in the press it was deluged with about 15,000 requests for

1) Bayer 1979, p3. According to the DIB a slowly rising trend is recorded.

information. This case is, however, regarded by the DIB as most exceptional, but surely, in view of the large number of comprehensive personal data files of the Authority, not disproportionate.

Another case of wholesale information requests (about 10,000) concerned the Swedish company of Readers Digest. Publications of the press had been against the use by Readers Digest of an address record of the whole Swedish population for advertising purposes.

These cases are, however, quite exceptional in their extent and it appears impossible that DP applications involving personal data bring about a large number of requests. In extreme cases moreover the DIB may, in accordance with art. 10, para. 4 of the Data Act, grant exemption from the obligation on information. It can also concede extended information periods. Special authority for the levying of information fees, in accordance with art. 10, para. 2 of the Data Act, offers a further possibility to clear such extreme cases.

The generally small number of information requests, especially in the private sector, is probably attributable (apart from a general co-operative climate of trust of the open Swedish society) to the general fact that the population has confidence in control through the licensing system exercised by the DIB. Moreover big private data file keepers especially have pursued an active data policy of creating or maintaining confidence.

Thus firms have kept trade unions informed; published appropriate information in company news sheets and, as a matter of routine, and without the prompting of information requests, apprised external interested parties (bank customers, insurance policy holders, etc). The traditional fear of irregular exploitation of data protection information rights is not borne out in Swedish experience.

4.3.3.2.2 Costs of granting access

According to the assessments of the DIB, the organisations granting access are involved in costs at a statistical average of barely Sw. Kr. 1.- for each instance. This extremely low average figure is, in the main, explained by the fact that big private undertakings especially (banks, insurance, etc), within an active policy of data protection, inform the data subjects (own personnel, customers, etc) from time to time as a matter of routine, by using automatic procedures or by taking advantage of regular personal and postal contact.

4.3.3.2.3 Access fees

According to art. 10, para. 2 of the Data Act there is normally no fee for the information. In special cases, however, the DIB can allow the levying of access fees - based on the sum of the direct costs of granting access.

Accordingly, the DIB approves the levying of information charges especially in cases which, on request from data subjects, information is given which normally is given

only on payment. Hence the DIB allows credit information bureaux, for example, to charge about Sw. Kr. 20 to 25 for data protection information.

It is conceivable that the DIB approve even considerably higher information charges in special cases. It should be stated that, especially in the private sector in the relatively few cases in which information is sought more than once in 12 months, the levying of a charge is generally waived. This is probably in the main as the small information costs arising are not worth the collection expenses. Usually information costs are regarded as public relations costs - particularly by the firms who, as a routine, give out information which has not been asked for.

4.3.3.3 Data security measures

Even from the aspect of data security measures for data protection, such costs can at most be regarded as marginal. The DIB sees itself here as a partner, who on the basis of accumulated special data security know-how makes firms and administrations aware of their own security needs and indicates cost favourable solutions.

In the experience of the DIB, reviews of security measures in cases, already in hand, of general security needs, e.g. in the banking sector, generally call for no or few additional measures. These often lie in the orbit of small organisational changes which in practice cause no additional costs. When in individual cases more or less

considerable security measures are needed, as a general rule the affected organisations accept that such measures are probably only to a small degree directly for data protection and not for other needs. The Swedish National Statistics Authority, for instance, introduced additional security measures at a cost of about Sw. Kr. 1,000,000, on the advice of the DIB in recognition of data protection as well as various other needs.

Above all, the fact that the DIB has so far had no kind of complaint of excessive data security requirements shows most clearly that data security expense for data protection is not really a problem. The lack of controversy in this matter can probably then be taken as an indication that data security costs purely for data protection are small.

4.3.3.4 Opportunity costs

The opportunity costs of the Swedish Data Act, i.e. the loss of benefit by virtue of the law as explained, is generally not assessible, but shows up in a highly anecdotal way in individual cases. A large Swedish service bureau was obliged, through a decision of the DIB, to stop the use of a data file covering the whole population for direct advertising, which had up to then generated an annual business turnover of about Sw. Kr. 1,000,000 with a high profit margin. In the estimation of the DIB, this activity has been since its inception a misuse in the private sector. The decision of the DIB is seen rather as a correction of an irregular practice. There may well be other similar sensational cases.

4.3.3.5 Positive effects of the Data Act

The DIB sets great store, not only by the generally small data protection costs and by the fundamentally conflict-free co-operation and its special value to the organisation, but by the assertion that private firms by the advice of the DIB in carrying out their data duties bring about, in part, appreciable positive effects and special economies.

The licensing system compels the firm to analyse as a whole the data banks and information systems, which over the years may have grown in a more or less unco-ordinated form. In this way, through the know-how which has increased in the meantime, it is often possible so to advise the organisation that its systems work more effectively, reliably and cheaply. The positive effects are especially the avoidance and the use of obsolete data and the multiple recording and processing of data within a firm, and the general reduction of irrational uncontrolled growth of data banks and information systems.

The model example of the DIB is that of a large department store chain, covering the whole country, which through direct advertising distributed bonus savings certificates. Within the framework of a data processing system established in the early 1960's, all former customers since 1959 were recorded, and directly approached three times per annum. Coincidentally with the processing of the authority, in accordance with the

Data Act, it was pointed out to the firm that details of former customers can be stored only up to three years. The DIB gave an adjustment period of 18 months. After only five months, however, the firm announced its completion. In the estimation of the firm annually about Sw. Kr. 500,000 is now saved, as not only were the storage needs quite considerably reduced through the deletion of old customer details, but a correspondingly smaller number of the public were approached three times annually by direct advertising. An analysis of customer behaviour had shown that only a small proportion of the very old customers entered into new agreements. The bonus savings business, which hitherto had made a loss of about Sw. Kr. 250,000 had in the meantime been sold to a bank and should now for the first time make a profit of Sw. Kr. 250,000.

Furthermore, the guidance from the DIB often results in increased accessibility and generally less complexity of information systems. There have already been cases in which the DIB was able to point to existing information, research etc which obviated expensive duplication of work. So generally the application of data protection regulations and the advisory assistance of the DIB often lead to the start of a comprehensive coherent internal control of information on company level.

4.3.3.6 International distortion of competition

The Data Act has understandably also effects internationally. Up to now there have been relatively

few cases in which the DIB has imposed restrictive decisions in respect of international data processing.[1)]

- The DIB refused the Swedish Siemens permission to pass on personal data to the German parent company.
- The district administration office of Jonkoping was not allowed to send to England a magnetic tape holding the identity and addresses of its population. With the help of this tape, patients' plastic identity cards were to have been provided.
- In another case the publishers Albert Bonnier were not allowed to send to England a magnetic tape, which was to serve as the basis for a printing of a register of taxpayers.
- In this connection the case concerning the large American credit information bureau Dunn & Bradstreet was probably one of the most serious. Dunn and Bradstreet owned 100% of one of the ten leading Swedish credit information bureaux, but had to dispose of it, as it was decided that in view of the extremely sensitive nature of credit information, a credit information bureau operating in Sweden should not be in foreign hands.

These and other cases are however individual instances of international restrictions from which no fundamental structural distortion of international competition, for reasons of data protection, can be inferred. Any future international data protection conventions, etc. will probably lead to fewer restrictive decisions.

1) See Vinge 1975, pp 57-58.

Above all in practice there is no reason from the cost aspect (which is here the main consideration) in the case of the Swedish Data Act for distortions of international competition arising from increased data protection costs, because, as pointed out, such costs are completely irrelevant.

Jan Freese, Director General of the DIB, stands on principle against what he sees as a less than strong argument on the question of distortion, through data protection considerations, in international competition. He points out that not only has there been distortion of competition internationally in related field in many forms, but that these are intensively exploited by firms. For example, the intensive international postal advertising business of Holland, England and Spain is mainly attributable to differences in national postal charges, i.e. to international distortion of competition. Similar and even more disturbing distortions are recorded, in part through quite large differences of charges for the use of data transmission networks.

4.3.3.7 International harmonisation of data protection

Apart from the fact that suitable international harmonisation of data protection would be accompanied in part by considerable general simplification (e.g. international action or national data protection licenses), from the Swedish viewpoint, as there are no more than marginal data protection costs, there can be no expectation of further sizeable cost reductions by such harmonisation measures.

4.3.3.8 General viewpoint of the Swedish Federation of Industries

The Swedish Federation of Industries (Sveriges Industriförbund) looks at the question of data protection costs, which internationally and (before the passing of the Swedish Data Act) also in Sweden has been regarded by private industry as very problematic, rather as a minor problem. Because data protection costs in Sweden have been marginal, there have been no efforts so far in assessing or even estimating them. Since the existence of the Swedish Data Act, i.e. since 1973, protection costs have never been a matter for discussion, and the Federation of Industries in particular has had no occasion to occupy itself with the cost aspects of data protection. Data protection costs appear negligible from the viewpoint of Swedish private enterprise, especially when compared with the costs relating to Government bureaucracy. This is true also for the (generally small) number of requests for information.

In a very enlightened and far-sighted way, the Swedish Federation of Industries sees data protection and the small cost it causes as a social correlative to the continually increasing use of data processing. To this extent data protection is looked upon as means of avoiding social conflict. If the Federation of Industries speaks out, on the other hand, in favour of an early harmonisation of data protection and laments the delay so far, it is not because of cost considerations or fears about distortion of competition caused by data protection, but because of the general need for uncomplicated and foreseeable international business conditions.

4.3.4 Federal Republic of Germany

4.3.4.1 Estimation of costs before the coming into force of the Federal Data Protection Law

In relation to the extraordinary flood of publications dealing generally with data protection which were produced in Germany before the passing and coming into effect of the Federal Data Protection Act, the very small number of systematic and positive contributions on the problems of data protection costs is surprising.

Without discussing those contributions in details here[1] it can be stated generally that the Germany data protection debate has basically taken the same course as in other countries, especially Great Britain and the USA. Thus various partial estimates and projections of costs were encountered, which were made by private industry as part of public enquiries launched by the Federal Government or the Federal Parliament.[2]

Drawn up on the basis of the most diverse possibilities for data protection regulations, interpreted in an arbitrary or even exaggerated number, cost estimates with an extraordinary large scatter resulted, sometimes entering the realms of fantasy:

1) For details on the German debate on data protection costs see Hogrebe 1979, pp 482-511.

2) See especially Deutscher Bundestag, Innenausschuss 1976a, 1976b, 1976c and for example Capital 1976 p 61; Süddeutsche Zeitung 1977, p 36; Wirtschaftswoche 1976, pp 12-17 etc.

- German insurance companies for example reckoned with DM 50,000,000 of additional personnel expenses alone.[1)]
- A credit information organisation covering the Federal Republic foresaw additional data protection costs of DM 40,000,000 on a total annual expenditure of DM 35,000,000 to 40,000,000 previously.[2)]
- The data protection costs arising for the whole economy were estimated, depending on the source, at "a few billion Marks" or up to "about 20 billion Marks".[3)]
- Even for data protection costs expressed in percentages, there was a big spread somewhere between 1% and 30% of the total data processing costs of the organisation in question.[4)]

One of the few systematic cost studies came to the result that by making certain assumptions additonal data protection costs on average do not exceed about 1% of the data processing costs of the affected firms. The official advisor of the Federal Ministry of the Interior on the Federal Data Protection Law, who had asked for the study, accepted this result as his own estimate.[5)] This estimate

1) Süddeutsche Zeitung 1977, p 36.

2) Süddeutsche Zeitung 1977, p 36.

3) See Capital 1976, p 61.

4) See for similar examples of percentage estimating Sabirowsky 1977; Futh 1976, p 237.

5) See Angermann/Schmidt/Thome 1976, p 50 and following this Auernhammer, in Computer-Zeitung 31.3. 1976, p 2; a similar tendency is shown by Hogrebe 1979, p 503.

of costs appeared all the more realistic because estimates derived from private industry were available at a very early stage according to which the small additional data protection and data security costs were more than covered by savings effected by suitable measures at least in large computer installations.[1)]

4.3.4.2 Cost-related experience with the Federal Data Protection Law

The observer of the German data protection scene after the passing of the Federal Data Protection Law must see that the catastrophes prophesied by some in respect of data protection costs have obviously not materialised.

Indeed the law (once proclaimed as the law of the century) has led in the meantime to an impressively feverish, much inflated doubt-ridden data protection community complaining about the difficulties and burden of applying the law. However, substantiated complaints of excessive data protection costs have not appeared. One gets the impression that this is due on the one hand to the pressure of the private sector and its representatives applied during the law-making process, sometimes heavily and certainly successfully, in favour of a data protection law sympathetic to users. On the other hand, it can probably be assumed that the data protection costs arising in fact generally remain well below earlier extreme estimates. In this connection it does not matter whether some of the original

1) See the practical experience of Obelode/Windfuhr 1974, p 236.

cost estimates, following the logic of the lobbyists, were more or less deliberatly exaggerated, or whether they arose from false assumptions or inadequate analysis of the actual data protection expense. And it seems revealing that, apart from a few itemised estimates, there are no systematic representative data cost calculations (or even estimates) similar to the survey of the Office of Management and Budget.[1)]

Consequently it is proposed to evaluate the cost intensity of the Federal Data Protection Law in the following paragraphs mainly by qualitative considerations under different aspects, bearing in mind the inadequate data available and the limiations of the study. The general starting point is the fundamental fact that the various, and in some cases very strict and extensive, obligations and limitations of earlier data protection proposals either do not appear, or only in such a hollow form that, already on the passing of the Act, interested experts on data protection called for an amendment. In fact the Federal Data Protection Law is so studded with general provisions, which to a large degree make it possible for users to evade expensive or even inconvenient

1) Various statements on the theme of data costs protection are confined to the repetition of old estimates made before the enactment or the coming into force of the law, in their own abstract speculations on cost or only in summarising data protection measure generally affecting cost etc., or by repeating the USA-developed pseudo-accurate approaches to determining optimum stragegies on data protection and security. See in general Pougien 1977; Bode/Drews 1977; Leib 1978; Nagel 1979b.

data protection obligations, that experts state: "The Federal Data Protection Law is as full of holes as a Swiss cheese".[1)]

Furthermore, whole branches of industry interpret certain data protection regulations so broadly, e.g.with reference to initial automatic notifications, that there is already talk of effectively by-passing the Data Protection Law.

Taken all in all, despite all complaints of users about some aspects of the law, the Federal Data Protection Law basically cannot be called burdensome or particularly costly. One of the best illustrations of this is the fact that the credit trade today willingly accepts the "omnibus law", bitterly opposed earlier, and votes now against the introduction of a data protection law with application to specific fields and adapted to the special conditions of particular trades.[2)]

4.3.4.2.1 Data protection commissioners and data protection training

According to estimates, there are company data protection commissioners in about 12,000 German firms. Because of special professional requirements (knowledge of data processing, organisation, data protection law, etc.), the high hierarchical ranking, with responsibility directly to top management, and the consequent special qualification required for data protection commissioners, sometimes heavy costs in respect of data protection personnel are incured. It

1) See Spiegel 1979, p 52.

2) See Rödl 1979, p 10.

is evident, however, that the great majority of data protection commissioners appointed in the private sector do not work full-time in this function.[1] Apart from the fact that full-time data protection commissioners generally attend to other tasks, the proportion of full-time data protection commissioners among the total number (especially those in smaller and medium-sized firms) lies considerably below 15%.

To this extent the full-time data protection commissioner is quite the exception. Additional tasks lie especially in the following area:[2]

- protection of the company's important internal data
- general data security
- training
- coordination of DP activities among other companies
- internal audits, etc.

Practically no data protection commissioners have been newly recruited. They are recruited by and large internally from the fields of data processing and organisation (the greater part), accounting, law, personnel, auditing, purchasing or marketing.[3]

1) According to a survey by Jamin 1978, p 66 there are fewer than 33%. According to another survey which covered 100 of the 500 biggest German firms, only 15% of the appointed date protection commissioners carry out this function on a full-time basis; see Online-ADL-Nachrichten No. 12, 1977, p 995.

2) Jamin 1978, p 66.

3) Jamin 1978, p 66; Spiegel 1979, p 52.

It is often even the head of data processing and organisation, or the head of personnel who additionally takes on the function of data protection commissioner. The resulting conflict of interests, contrary to the fundamental idea of the data protection law, is especially criticized by the public supervisory authorities. Furthermore, groups of firms take advantage of the possibility of appointing one suitable data protection commissioner for all the firms in the group.[1)]

In this case, as in that of appointing an external data protection commissioner, the data protection personnel costs for the individual firms are considerably reduced, and in any case, it seems unrealistic in the light of prevailing practice to count the full salary of a highly qualified full-time employee as data protection personnel costs of the individual company. One estimate, for example, assesses the burden for one-time conversion measures at one to three man months, and the permanent workload at only one to three man days per month.[2)]

The other personnel costs, which arise in part from the initial and continuous training and briefing of the data protection commissioner himself (seminar and congress visits, association dues, literature, etc.) and to some extent through the general data protection training of other employees handling personal data, could especially after the initial phase, be classed as generally marginal, too.

1) 40% of the 100 data protection commissioners in the enquiry alredy mentioned carried out this function for several associated sister companies. See Online-ADL-Nachrichten No. 12, 1977, p 995.

2) Poths 1977, p 24.

4.3.4.2.2 Obligation to notify

The obligation to notify data subjects automatically when data concerning them is first recorded or transmitted (art. 26, para. 1 or art. 34, para. 1 - Federal Data Protection Law) appears in fact virtually not to exist in practice, in any case the obligation to notify can in practice be ignored as a cost factor. In the great majority of instances of storing or transmitting there are direct connections between the storing, transmitting or receiving office and the data subject, so that the notification is not necessary, as the data subject gets knowledge of the storing or transmitting in another way. Because of the very broad interpretation, even in some areas in which this knowledge cannot be assumed without further considerations (e.g. the area of the address vending and direct advertising), the obligation to notify has in practice been set aside in a dubious way.

Furthermore it should not be lost sight of that even with due observation of the obligation to notify, provided "other knowledge" is sufficient, virtually no additional costs arise if the contact with the data subject can be established directly or indirectly via third parties within the framework of routine procedures.

This is, however, almost always the case, or achievable with a little organisational creativity. To this extent the problem of notification, even for credit information agencies and address vendors etc., shows itself at least from the legal aspect as a by no means over-burdensome one of changeover.[1)]

1) See Hogrebe 1979, pp 507-508.

4.3.4.2.3 Requests for access

4.3.4.2.3.1 Volume and costs of requests for access

On the matter of the rather easily answerable question about the volume of requests for access so far, no representative figures are available. The most diverse opinions, however, are largely in agreement that "the big rush of data subjects has not materialised" and that "only in exceptional cases has use so far been made of the right of access in business practice".[1)]

Even the biggest companies with intensive personal data files (Insurance, Banks, Mail Order, etc.) have apparently recorded virtually no requests for access.

While there is some increase among credit information organisations etc. the question of volume, and with it also the matter of information costs in practice, has nowhere given rise to cost problems of any practical importance. Up to now it seems generally to be a "non-problem".

4.3.4.2.3.2 Access fees

Against this, and to a certain degree qualified by the missing rush of requests for access, the question of access fees levyable following the Federal Data Protection Law is being discussed quite intensively. According to the Federal Data Protection Act (art. 26, para. 3; art. 34, para. 3), private agencies can "charge a fee for the information which may not exceed the costs directly attributable to the provision of information".

1) See e.g. Online-ADL-Nachrichten No. 3, 1978, p 145; Datenschutz-Berater 1978b, p 149.

In the provision the legislator is aiming not only at financial compensation, but also at deterring grumblers, persistent questioners and frivolous requests for information. It is not surprising therefore that, especially in areas in which the law was received with special scepticism and in which great fears existed about the number of enquiries to be expected, relatively very high enquiry-deterring fees were fixed to protect against the mistrusting citizen and his endless requests. Thus, especially in such areas as credit information, charges of DM 25 and more were discussed. Such prohibitive fees were strongly criticised. Because of the considerable negative publicity, and particularly because information fees in the public sector were mostly between DM 4 and DM 20, so far in the private sector also, no charges exceeding DM 20 are apparently being made.

In this connection the Federal Data Protection Charges Order of 22.12.1977 [1] is especially worthy of mention. According to this, within the area of Federal Administration the access fee amounts to DM 10 per unit as a matter of principle. Oral or simple written information, however, can be given out without cost. Even such a charge as DM 10 is, however, regarded by data protection experts and, among others, the Federal Data Protection Commissioners as prohibitive.

1) Bundesgesetzblatt I, 77, p 3153.

With due note of the small number of information enquiries, the Federal Data Protection Commissioner advocates a general renunciation of all charges and payments for information to the data subject.[1)]

Significantly, the Federal Interior Minister in a recommendation of summer 1979 has in the meantime urged the highest federal authorities to rescind all access fees. Furthermore a large number of private firms are refraining from exacting payment. Apart from public relations considerations, the main reason is probably the expenditure which the establishment, calculation and collection of such fees would cause.[2)]

The inappropriateness on many grounds is shown by the German experience of access fees. The very small number of requests for access shows that the deterrent function of the fees is superfluous.[3)] Moreover, from the point of view of legal policy, it seems fundamentally extremely dubious to burden or even hamper the citizen with charges in the legitimate exercise of his data protection rights, which are based on the constitutionally guaranteed law on personal rights: charges which were conscientiously conceived with a

1) Bundesbeauftragter für den Datenschutz 1979, pp 51-52 and Bull 1978, p 575.

2) See e.g. Gola 1978, p. 4; and Datenschutz-Berater 1978b, p. 149.

3) It appears to be undisputed that in the case of the German Data Protection Law the small volume of requests for access is not just a consequence of the existing control of charges, but a lack of knowledge among the population and a very limited interest in such information.

view to deterring the isolated, wrongful or even merely inconvenient exercise of rights. (It seems more appropriate to abolish motor cars from the evidence yearly of thousands of wounded and dead from traffic accidents.) If access fees must be retained for other reasons, such fees should therefore have a fixed upper limit of certainly not more than DM 10, and preferably below that.

It can, however, be repeated that there is no need to calculate variable charges related to direct costs. More strictly it can be said that only a (small) lump sum unit charge (if any) makes sense. It is unnecessary here to go into the various conceptual absurdities and practical difficulties which are connected with what at first sight might seem to be a plausible idea, i.e. the concept that the access fee should not exceed the direct cost arising from the giving of information.[1)]

1) The idea of access fees covering the direct information costs is, in data protection, a gross misconception. With correct business accounting, such a charge leads usually to merely small minimal charges, originally probably not intended by the legislator: see Hogrebe 1979, pp 508-510. The inclusion of the personnel expenses (for the permanent staff involved) might be inconsistent with the business concept of direct costs. This is generally not appreciated: see e.g. Ehrich/ Kirchherr/Pusch 1978, p 82, Böhm 1977, p 79 and Ausschuss für Wirtschaftliche Verwaltung in Wirtschaft und öffentlicher Hand (AWV) 1977, pp 29-30. Also Kargl/ Reinermann/Schmidt/Thome 1979, p 16.

   On the other hand in certain situations quite heavy and, in effect, unfair cost fluctuations arise, which can lead to horrendous charge rates. So computing costs even for a costly enquiry cannot be brought to account per charge since they are normally invariably fixed or lump sum costs, if it involves a firm's own (i.e. purchased, leased or rented) computer installation. The same processing through a computer bureau would, however, be variable direct costs for the firm, possibly in the form of very high charges. Generally the direct costs depend to a large degree on the structure and efficiency of organisation and procedures: see Böhm 1977, p 80 and Gola/Hümmerich/Kerstan 1977, p 25. It can be mentioned that there is no certainty of the necessary predictability of the access fee with the charge calculation depending on variable expenditure.

The cost of calculating and collecting small access fees will probably exceed the revenue, so that the argument of compensation (at least in part) does not apply and only the deterrent motive remains.

It should finally be stated that the feat of excessive requests for information implies a pathological attitude which is not necessarily found in those making requests for information. The real problems appear to lie on the level of an understanding of modern democracy, of the concept of an open and transparent society, i.e. more in the attitude of the holder of the information. Only in quite exceptional individual cases of wrongful exercise of information rights should exemption (either administratively through the data protection supervisory authority, as in Sweden, or judicially) be given to the organisation concerned.

General limitation of the right of access, by fees or frequency etc., appear to be unsuitable in principle and unnecessary in practice.

4.3.4.2.4 Data security measures

No coherent information exists even on the costs of data security measures. Generally it is assumed that there is a special burden of cost for (technical and organisational) security of data. This is probably only relative to the very small costs of notifying, or requests for access, and of part-time data protection commissioners, who generally have litle work to do on data protection.

In absolute numbers, however, data security costs can in practice be ignored. Indeed the ten-item list in the annex to article 6 of the Federal Data Protection Law concerning technical and organisational data security measures appear very impressive and involved. It should not be overlooked, however, that it is not a catalogue or measures but of aims. Practice in data security is, however, firstly determined by the double qualification of article 6, para. 1, to the effect that security measures are to be taken only in as much as they are "necessary" and "their cost is in suitable relation to the sort of protection which is being striven for". Secondly, the interpretation of "necessary" and "suitable relation" is made by the data processing organisations themselves, a practice which has hitherto continued almost without check by supervisory authorities and other third parties. It is not surprising that there are no complaints about intolerable or even high data security expenditure.

As for suitable security measures taken under the data protection law, these cannot properly be regarded as purely data protection costs, because they benefit the organisation which processes the data and have been taken (or should have been) taken for other needs and obligations. This is today widely recognised in the German data protection debate and is indeed not seriously disputed by any organisation. Other reasons for effecting technical and organisational security measures include:[1)]

1) See also among many other Kraus 1978, especially pp 70-82; Ehrich 1978, pp 191; Fiselius 1977, pp 71-72; Risch 1978, pp 199-204; Nagel 1975, pp 92-93; Nagel 1979a, pp 24-40.

- protection of hardware and software from damage
- protection of data against industrial espionage, sabotage, and computer crimes, etc.
- general principles of orderly data processing
- principles for the keeping of personal files
- requirements of regulations on the acquisition and transmission of data.

One of the most striking examples so far is that of computer bureaux. The bigger ones in particular stress that they have had to take no, or in terms of cost only minor, additional security measures following the Federal Data Protection Law, since their security was already adequate.[1] They point out convincingly that excellent data security is a pre-requisite for their business, as otherwise customers would not entrust their data for processing. However, some knowledgeable people, in strict confidence, refer to cases where bureaux did take security measures to meet the Federal Data Protection Law. These insiders considered such measures as long overdue correction of old omissions and, emphatically, not as data protection expenditure. Significantly, bureaux emphasize their high level of data protection.

1) See e.g. the manager of the Federation of German Computer Bureaux (VDRZ) Lange-Hellwig, in: Computerwoche, 26.11.1976, p 5.

See also Singer 1978a, p 42; "For data security for a long time much has already been done in every bank in its own interest. It can be mainained that the Federal Data Protection Law asks for nothing that is not otherwise in existence or planned".

To sum up, it can generally be said that experience so far of the German Federal Data Protection Law, especially in the private sector, has shown that even in the initial period, in the area of security measure for data protection, no serious costs have arisen.[1)]

4.3.4.2.5 Summary and general considerations

To summarize, it can be said that the German Federal Data Protection Law has caused, particularly in the private sector, no excessive burdensome data protection costs.[2)] On the contrary, real data protection costs in the great majority of cases can be described as marginal.

1) Cf. a private communication from the Chairman of the Gesellschaft für Datenschutz und Datensicherheit Hans Gliss of 3 August 1979, p 2: "The question is always important as to whether the security measures would have had to be taken even without the German Federal Data Protection Law, in this or a weaker form because of existing risks. We believe that you will come to the conclusion that only relatively little cost can be directly attributed to the German Federal Data Protection Law."

   See also Betriebswirtschaftliches Institut für Organisation und Automation (BIFOA) 1978: "The principle of appropriateness enunciated in art. 6 of the German Federal Data Protection Law... can in borderline cases be met exclusively through organisational meaures ,... Organisational measures (arise) primarily from the firms themselves, their prices are not fixed, are difficult to calculate, and are rarely identified.

2) See e.g. Poths 1978, p 87, who concludes that costs for the introduction of data protection in the smaller and middle-sized firms in the machine construction industry (10-500 workers) amount to less than DM 30,000 to DM 70,000. It is generally assumed that larger firms have relatively smaller data protection costs than small and medium-sized ones.

This conclusion is the more noteworthy as it refers to experience of the law during the introductory and reorganisation phase; running costs of a stabilised data protection regime will be much less.

No cases of applications being suspended entirely because of data protection have appeared. Lost opportunities for earnings (opportunity costs) cannot therefore be ascertained, if there have been any.

No serious losses from difficulties and costs have been reported which could be attributed to inefficient data processing for the sake of data protection. Even the treatment of individual legally autonomous firms within a group as independent units so that data flows between them are confirmed as flows between third parties, has not (because of the generally liberal stipulations of the Federal Data Protection Law) apparently led to a noticeable reduction in personal data flows and processing between associated firms.[1)]

1) See e.g. Breker 1978a and 1978b for insurance companies which might be seriously affected, who, by way of reference to all-embracing "justifiable interests" (i.e. especially "every economic interest", as e.g. rationalisation, check on customer potential, advertising, risk reduction, lowering of costs, profitability) "reduce the special problem of data protection within big groups to a non-problem".

On the other hand, the positive effects of data protection must not be ignored. Apart from improved public relations and other unmeasured but important effects (reduction of error rates, updating etc. of data records), there are cost-reducing rationalisation effects which must not be underestimated, and which at least compensate for the real data protection costs. Rationalising effects in data processing and general organisation cannot be analysed further here, but references are given.[1)]

In this connection, it is sometimes argued that such positive effects of rationalisation cannot be attributed to data protection, as in this respect data protection is not causal, but only a "stimulus for hitherto unnoticed opportunities", and that it would therefore be wrong to take this rationalisation factor into account quantitatively within a general theory of data protection costs.[2)]

That may appear reasonable at first. But if a data protection measure initiates or brings about rationalisation whose costs are booked as data protection expenditure, then this expenditure must be properly reduced by the rationalisation profit achieved. Alternatively, the rationalisation profit can be regarded as caused by a general rationalistaion measure, in which case the costs of the rationalisation measure logically are also no longer bookable as data

1) See e.g. Datenschutz-Berater 1977, p 75-76 and Datenschutz-Berater 1978a, pp 36-38. The above-mentioned literature on the orderliness of data protection etc. is in this respect of importance.

2) See Poths 1978, p 88.

protection expenditure. The procedure is then shown as a beneficial rationalisation measure with an implicit cost-free data protection side-effect. Both methods yield the same (reduced) data protection cost.

In the not too distant future, probably one of the most important positive effects of data protection for business is that observation and implementation of data protection, especially in larger firms, is a step in the direction of the rational and effective general management of information. Such management of business information (perhaps integrating the functions of data processing and administration) would on the one hand treat information as a resource contributing to general business productivity, and on the other hand would include the dynamic aspects of all information processing and movement in the firm.

This step towards company information management is not an automatic consequence of data protection. However, the implementation of data protection creates certain conceptual, instrumental and organisational pre-requisites in this direction, which can be effected forthwith in the larger firms. This applies particularly to the German conception of data protection, which relies on central professional data protection commissioners reporting directly to top management, with far-reaching functions in all fields, and access to vital instruments of data protection management and control, such as registers, etc. relating to the resource of personal data.

Finally, experience with the Federal Data Protection Law raises the question whether, how far, and under what conditions a general system of registration, but especially a general licensing system, is as efficient, or more efficient, than the German decentralised system of internal self-control with limited, mainly occasional, control through regional supervisory authorities. The question can only be broached here, and is probably difficult to answer even in principle, as a meaningful answer would have to include an assessment of the data protection levels actually achieved in individual cases. This question remains, however, as German data practice so far, and probably in the future, is stamped with deep-seated vagueness because of the (perhaps unavoidable) fuzziness of a seemingly precise omnibus law loaded woolly with provisions.[1)]

This uncertainty in the data protection obligations of the individual DP user must increase his costs, unless it is balanced by a correspondingly tolerant interpretation of the law in practice. In this situation, appropriate unbureaucratic licensing procedures would make data protection obligations and tasks for the firm clear, predictable and quantifiable (all of which is important in this area).

1) Even today the following failings of the Federal Data Protection Law are criticised - vague drafting, contradictory recommendations, unclear concepts, different definitions for the same facts and even difficulties in defining such basic terms as data bank, concern, third party; see Jamin 1978, p 66.

4.4 Costs of data protection: general conclusions

4.4.1 Overestimation of data protection costs

A summary of the findings of the analysis of the various estimates and experiences of the four selected countries is given below. If some categorical comments are made on the cost of data protection, no general and definite judgement is intended; this is a simplified presentation.

If therefore it is stated that data protection costs are on the whole negligible or marginal, it should not be assumed that data protection controls could not be devised which, generally or in sectors, could give rise to heavy data protection costs. Clearly every new data protection law or other regulation poses the serious problem of how to bring about the desired effect on data protection with maximum efficiency, i.e. with minimal expenditure. But one can refute the dogmatic judgement which maintains at the national level that the costs of data protection are too high, and leads (through hints that at the international level there is a threat of distortion of free competition by data protection costs) to pressure on national decision-making committees. However, a rational basis for a European (and possibly more comprehensive) policy of harmonisation of data protection should be produced, based (among other things) on economic realities.

Categorical findings are not claimed here, because of the general statements made above, that comments, especially on data protection costs, are at best estimated guesses, in most cases merely speculations which tend to be too high, especially if they are made by potentially affected users and their representatives in the broadest sense.

Partly this is due to lobbying, but has, as e.g. the prior estimates of the Office for Management and Budget show, other objective grounds. Moreover, as again the example of the Office for Management and Budget shows, statements on data protection costs, based on practical experience, are not precise cost figures, but are rather based mainly on estimates which tend also to be set too high through inattention to certain cost reducing factors, imprecise cost calculations etc. In any case, the assertion of the unreliability of current statements on data protection costs, and of the connected, far-reaching and generally extreme over-estimation of real data protection costs is the central finding of the present study.

Solely on the grounds of the unreliability and incompleteness of the present empirical information, separate meaningful statements relating to the various special sectors, organisations and groups (public administrations, private business, computer bureaux, citizens etc.) are not possible within this study.

With due regard to the reservations made at the beginning of this section as to the general validity of the results of this study and in the light of the general findings, basic reliability and general dependability of statements is claimed as far as "real existing data protection" is concerned. The clear convergence of the findings of the examination of the various assessments and experiences in respect of data protection costs in four countries (and beyond) bears this out.[1)]

The further consideration, that various interests at national level would oppose all possible planned data protection controls which would clearly be more cost-intensive than the present regulations in the four countries, strengthens this conclusion with, moreover, due regard to future data cost controls (e.g. in UK and USA).

4.4.2 Notification

Automatic notification of the data subject of the fact of his inclusion in a personal data system (and possibly of the content of his record), in the sense of an unrequested automatic notification by the organisation which stores the data (as distinct from notification at the request of the data subject) can in principle be extremely costly, of course; as

1) Other countries, especially France, Austria, Denmark, Norway, Canada were included in the preliminary study, but there were no findings contrary to those given in this summary.

e.g. if periodic, say annual, apprising of all recorded people was required by individual direct mailing. In observed practice, however, apprising, especially in the private sector, plays almost no role from a cost viewpoint.[1)]

That may lie in the fact that the legislator,. in view of the probably heavy costs, and under pressure from interested circles, goes to the opposite extreme and in a far-reaching way dispenses with notification obligations. The Swedish data protection law does not provide any obligation to notify without request: this failure in the Swedish example is partly compensated for through central registration with the Data Inspection Board and cost-free right of access. In the German data protection law, the notification obligations are so generally stipulated and loosely phrased that private data processing organisations, with few exceptions, have, through loose interpretation, been able to evade them completely so far. With suitable arrangements (e.g. notification on the occasion of routine direct business contact with the data subject, or through business partners, etc.) far-reaching notification obligations are conceivable, which need not be at all costly.

1) This does not apply to the same degree for the American Federal Administration and the special kind of general apprising of the public in the form of far-reaching publication obligations under the Privacy Act: correspondingly less costly procedures are in this respect also probably currently being worked out.

4.4.3 Requests for access

Apart from the notification obligations, legislators in general approach the rights of the data subject in a similarly careful, not to say suspicious, way, as far as information is concerned as to whether he is on record and the content, and the informing of third parties. Apart from fears that the data subject might learn too much about the affairs of organisation, there is a desire to minimise the volume of requests for information not only from more or less "difficult" people, but from the public in general, and as far as possible to pass on to the enquirers any costs arising, not least for the purpose of deterrent.

It must be stated emphatically that such fears and trends, compared with the reality of the generally almost negligible volume of information requests, appear to be completely exaggerated and unwarranted. Experience in four countries and beyond shows that the rights of access provided by data protection laws (and moreover within the framework of "freedom of information" legislation) are used by the data subject only to a limited degree, and that abuse does not occur at all in practice. Concentrations of information requests which have occurred have generally been based on special situations and particular legitimate reasons for the data subjects to request the information, and do not justify a general restrictive attitude.

The findings from the considerations given here show that, especially in the private sector, in general no information costs arise which are worth mentioning. It is, therefore, in practice unnecessary to deter information requests by information fees. On the other hand, a full cost-covering fee without levying prohibitive access fees seems unrealistic anyway. The levying of small fees (e.g. covering only direct costs) appears, however, on various grounds (danger of higher charges on grounds of broad interpretation by private offices, general accounting and collection costs exceeding the charge) to be rather illogical. It is, therefore, probably appropriate with very few exceptions to avoid any information fees. The "emergency brake" for exceptional circumstances where special costs or other burdens arise should be provided not in the form of access fees but in the form of administrative or judical decision on the individual case.

4.4.4 Data protection commissioners and other data protection personnel costs

The German Data Protection Law is at present the only one where a data protection commissioner provided with far-reaching duties and powers constitutes the central element of a data protection implementation and control structure, relying mainly on internal self-control. Nevertheless, it is noteworthy that the full-time data protection commissioner is the exception, and that generally, after a relatively short change-over period of intense activity

related to data protection, his permanent routine data protection load is quite small, i.e. that with an efficient procedure for the (usually) part-time data protection commissioner, the data protection personnel costs arising from him can be kept within bounds. This is of wider relevance, as various operational functions are concentrated in the person of this commissioner which probably have to be discharged in a more or less corresponding form in private organisations under other national data protection regulations. In the absence of adequate data, it is difficult to assess how far other personnel costs arise. Probably the main factors are the initial data protection training of the personnel involved in personal data during the change-over period, and to a smaller degree the permanent routine briefing, together with the notification of the data subjects and the processing of their information and correction requests. While in respect of the American Privacy Act there are suggestions of relatively high initial training costs in the public sector, there are in this connection no signs of specially high costs under the German or Swedish data protection laws.

In the general absence of a large volume of work on notification and information requests, corresponding small personnel costs, even with a possible future increase in work, can through efficient organisation and automation be reduced to an acceptable minimum for the treatment of special cases (corrections, blockings, deletions).

4.4.5 Registration and licensing fees

In the case of registration and licensing fees, such as those raised in Sweden and as those being considered in Britain, the problem is essentially not so much their absolute amount (practically of no importance) as rather the problem of their method of calculation. In this respect the concept being discussed to a certain extent in Britain of a fee covering the costs of a data protection authority does not seem to be very practicable due to various considerations. In this connection it is indicative that the Swedish Data Inspection Board which has experience in this matter is, on the contrary, tending towards minimising and finally completely abolishing such fees.

If fees can be raised at all, then they should in any case not exceed low and simply structured lump sums (per data file, application or such like).

4.4.6 Data security

The (technical and organisational) data security costs, which a priori to a great extent are regarded as a special, if not the decisive, element of data protection costs, obviously move into the background in practice as being marginal. This may be partly due to the fact that data processing agencies to a certain extent do not take their security obligations too seriously.

In the majority of cases, however, comprehensive data security measures are already being taken, either due to other safety requirements and various self-interests, so that relatively minimal additional measures due to data protection are necessary, or measures, which for other reasons were already overdue, are being taken with regard to data protection requirements, which can only be actually taken into account to the lowest degree as true data security measures due to data protection with regard to costs.

In practice this way of viewing matters is obviously accepted basically by the data processing agencies. In any case, the arising data security measures due to data protection are not, as far as can be seen, regarded as being considerable by those engaged in the field.

4.4.7 Opportunity costs

Apart from the fact that the application of the concept of opportunity costs in the sphere of data protection regulation does not seem to be unproblematical, no concrete opportunity costs were able to be identified. Their possible existence can, of course, not be fully excluded. In view of the relatively less restrictive effects in toto of the data protection legislation considered it can probably be assumed, however, that in general no dramatic opportunity costs (will) arise and that any diffusely occurring costs (will) remain theoretical.

4.4.8 Effects with regard to costs and other positive effects for the data processing agencies

The true data protection costs, which with correct costing tend to be low, can be still further reduced in terms of figures by various effects with regard to cost and other positive effects of data protection within the framework of a total estimate of the burden due to data protection in the case of personal data processing agencies. It is, of course, not to be neglected that a precise evaluation in terms of figures of these various positive effects (especially within the scope of this study) is not possible; however, there are sufficient signs to conclude that the net burden defined in this way of the data processing agencies due to data protection actually remains, in general, marginal in its effect.

In saying this, it is assumed that the various data protection obligations and requirements are met correctly and in accordance with the law, and at the same time, however, in an efficient manner. This implies, on the one hand, a clear internal data protection policy and an appropriate precise organisation of the data protection measures and, on the other hand, the widest possible automation in the sphere of data protection (data and

datafile register, automatic notifications and distribution of information, data security measures with regard to hardware and software etc.).[1)]

Such positive effects lie, on the one hand, in the sphere of increased efficiency in data processing operation, especially in data management (reduction and more efficient organisation of data, more up-to-date and more correct data etc.) and other functions (e.g. auditing), as well as general organisation. On the other hand, a seriously and efficiently operated internal data protection policy can give important impulses in the direction of economical and integrated general operations information management which goes beyond data protection and personal data on the one hand and data processing on the other hand. Data dictionary systems etc. can be, for example, valuable elements for an efficient operational data protection and at the same time essential bases for economical data administration.

Last but not least, public relations effects arise, especially in the sectors where this is of special importance and where at the same time there exists an

1) It must be clearly pointed out in this connection that data protection costs arising for a data processing agency also depend on the general organisational and technical efficiency of the agency. This also applies to information costs. This is also a further reason for opposing access fees to cover costs. There is the danger that inefficiency will be passed on to the data subjects without the agencies being subject to healthy rationalisation pressure with regard to the information given under the right of access.

especially delicate data protection problem, and through this potentially increased data protection costs. This concerns sectors, for example, such as: banks, credit information organisations, insurance companies, address vendors, direct advertising agencies, opinion research institutes, government statistics offices and also functions such as personnel files.

In all such areas, the confidence which the specific data subjects place in the correct handling of the data concerning them is more or less the basic foundation for every activity in the respective area. Therefore data protection which is optimal as far as possible and acceptable to the data subjects is becoming, on the one hand, an essential public relations argument and, on the other hand the basic prerequisite. This (in view of the increasing anxiety of the public with regard to their privacy[1]) is becoming so to an increasing degree,

1) See, as one of the most recent documents in this context the American opinion poll of Harris/Westin 1979. Cf. also Westin 1978, pp 14-16 as well as, in particular, the quotations taken from the poll in Zientara 1979, p 35:

> "It is not surprising, then, that 63% of the public agrees with the statement that 'If privacy is to be preserved, the use of computers must be sharply restricted in the future'....The message is loud and clear. If the institutions of this society expect to be able to continue to make widespread use of computers, the public must be convinced that the personal information stored in the computers is adequately protected from improper use."

irrespective of the presence of appropriate data protection legislation. Therefore the pertinent effort made by the (private and public) data processing agencies of these areas (and more and more beyond these) perhaps still represents itself as data protection costs but at any rate quite definitely not as "unnecessary additional costs due to data protection legislation". This basically demonstrates that in the final analysis it is actually a question of public relations costs or general business costs ("costs of being in business"). If regarded in a similar fashion, data protection costs would represent themselves to a substantial degree as costs of, or basic condition for, the conflict-free introduction and stable operation of modern, in particular automatic, information processing systems.

4.5 The issue of distortion of international competition caused by data protection costs

4.5.1 Definition of the issue

The consideration that national data protection regulations cause costs, that different national data protection regulations result in more or less considerable but different costs, and that finally, distortions of competition arise from this on the international level, seems basically to be quite plausible.

Such distortions of competition caused by data protection costs could mainly consist in that companies of various countries competing in international markets have unjustifiable cost advantages or disadvantages in competition due to differing burdens caused by data protection costs. Distortion could also be seen in that companies operating internationally must meet several data protection laws at the same time, so that for them accumulation of costs arises through the fact that they must take certain data protection measures several times or that they must at the same time take different, in some countries even conflicting, data protection measures.

Whilst this possibility of such distortions of competition applies basically to companies of every type, such distortions are especially feared for information-intensive companies, above all for large multinational companies with intensive internal communication. In particular in the sphere of the data processing industry, corresponding fears have been expressed with regard to internationally operating bureaux, including data transmission services (value-added networks etc.), and the software industry.

It must not be forgotten, however, that although fears with regard to distortions of competition at first appear quite plausible and therefore are expressed frequently by different interested parties, such fears are always formulated very generally and, as far as can be seen, can practically never be demonstrated in specific cases with some degree of detail.

4.5.2 General evaluation of the issue of competition

The results of this study seem to explain this deficiency (let it be noted, only with regard to questions of distortions of competition caused by data protection costs). As shown in the statements above, data protection costs considered in general are low, and in any case not large enough to affect the international competitiveness of companies. In quite individual, very special situations this assessment may, in certain circumstances, not apply to this degree of certainty, but such individual cases cannot affect the overall judgement.

It cannot and should not, let it be noted, be excluded that data protection regulations are conceivable which are very cost-intensive and therefore distorting with regard to international competition, and it cannot be excluded either that a country, in aiming at a specific problem, will pass such a law. The assessment given here refers basically only to "normal" national data protection legislation, i.e. in particular to the "omnibus legislation" as well as the already partly existing legislation concerning certain sectors (e.g. with regard to finance and credit systems, address vending and direct advertising, science and research).

However, it is also to be assumed that basically no country will pass an excessively cost-intensive data protection law since, on the one hand, there is no demand for such a law as the public in general is obviously satisfied with the data protection level attained (and, as shown, not cost-intensive) in, for example, Sweden and Germany; the innovations usually demanded appear to be inconsiderable so far. On the other hand, the internal national opposition to cost-intensive laws would already be so great that it would never come to such data protection laws and international distortions of competition. The influence of national associations of interested parties in the formulation of the existing various national data protection laws is already a central element of recent data protection history.

As a general result, it can be maintained that there are no international distortions of competition due to data protection costs, because of the lack of appreciable data protection costs. Even certain relatively unimportant extra burdens which accrue to companies operating internationally, in particular multinational companies, in certain circumstances due to the fact that they are faced with various, differently conceived data protection laws, in no way become concentrated into distortions of competition due to costs. Any international cost differences caused by data protection or extra burdens fade in comparison with other, quite virulent international cost differences as, for example, in the field of international telecommunication rates.

With the negation of distortions of competition caused by data protection costs, no judgement, of course, is made with regard to any existing distortions of international competition which do not arise through different data costs but directly through certain data protection regulations, in some circumstances motivated by protectionism.[1] If, however, certain data protection regulations result directly in effects impairing international competition, then these are not competition distortions caused by data protection costs which are being discussed here solely.

1) In this connection, for example, the statements of the Report of the Legal Committee of the European Parliament 1979, pp 6,22 with regard to the problems of data protectionism and distorted competition conditions are basically quite relevant. See also Pantages/Pipe 1977; Pantages 1977b; Schwappach 1978; Gassmann 1976.

In summarising, it can therefore be stated that data protection costs represent practically no critical element in the international sphere which decisively limits data protection aims. On the contrary, it seems that both nationally and internationally (assuming in each case an economically efficient formulation and carrying out of data protection regulations), a considerably higher data protection level is realisable before data protection costs become critical.

4.5.3 Evaluation from the point of view of the data subject

Apart from any differences in the access fees required in specific cases, the individual data subjects are not affected either as regards costs due to the differences in the national data protection laws. (Even in the purely national sphere there are differing access fees as well as substantial differences between existing various data protection laws concerning different sectors.)

It must, however, not be ignored that the individual is considerably hampered and practically prevented to a greater extent in the exercising of his data protection rights at international level than are internationally operating companies with various national bases and representatives. This, however, is again not really a cost problem, but a de facto difficulty which naturally has economic implications (costs for international data protection consultation, translation, communication costs etc.) as soon as the data subject seriously attempts to overcome these difficulties.

4.6 Cost-effective harmonisation measures of a European data protection policy

In view of the data protection costs which tend to be low, and through this the absence of distortions of international competition caused by data protection cost which are of any practical relevance, there is no need for a European harmonisation policy which is primarily directed towards the reduction of data protection costs and of corresponding distortions of competition. The necessity of an international and especially European data protection harmonisation policy arises from an economic standpoint rather from the necessity of a common data processing market generally free from distortions of competition due to data protection or, put in more common terms, from the necessity of a common data and information market.

The basic result of the study presented here concerning the question of data protection costs lies, however, in showing the relativity of the data protection issue, so that a European data protection harmonisation policy is made possible which does not just concentrate on the limited cost aspect, and anxiously strives for the removal of the international data protection cost differences, but also actively works for the uniform realisation of the legitimate aims of data protection on international level, taking into account at the same time the overriding aspects of the information market and industrial policy aspects.

It must be noted that this does not imply a trivialisation of the data protection cost issues. On the one hand, the problem and the task in general still remain, i.e. to realise the data protection aimed at with the highest possible efficiency (but without the data protection cost considerations which have been put into proper relationship here determining the decision about the data protection level to be aimed at). On the other hand, the study and adequate taking into consideration of the cost aspects lead to significant conclusions for the actual formulation and practical realisation of data protection.

Accordingly, various elements of a data protection harmonisation policy are now listed in summarised form as they arise as the result of this data protection cost study.

4.6.1 Cost-relevant elements of a data protection harmonisation policy

4.6.1.1 Principles

In view of the basic triviality of data protection costs, the ambitious concept of the European Parliament of a "guideline for the harmonisation of data protection law at the highest level for the citizens of the Community"[1] seems to be realisable as far as expense is concerned, if the principle of efficiency is observed. Besides the uniformity and simplicity of such data protection

1) Europäisches Parlament, Rechtsausschuss 1979, p 7.

guidelines and corresponding national data protection regulations, their durability and in particular their calculability in the sense of foreseeability of their requirements are important. An essential contribution of a Community guideline would therefore be the creation of stable and foreseeable business conditions in regard to data protection in the European data and information market.

The provision of an adequate transition and conversion period for each harmonisation guideline is fundamentally important for a decisive minimisation of the (one-time) data protection costs.

4.6.1.2 Registration and licensing

In view of the considerable uncertainty in the application of national data protection requirements which the German system of data protection self-monitoring has caused in business, whereas the Swedish licensing model is obviously regarded by business as being an instrument creating precise and clear regulations for the individual case, the introduction of an essentially uniform registration and licensing obligation of personal data files or data processing applications at European level seems to be inevitable in the long run.[1] For the individual data processing agency such official approval would take on the function

1) Cf. also the relevant Recommendation No.1 of Europäisches Parlament, Rechtsausschuss p 9.

of a data protection certificate which, with appropriate international harmonisation, especially with regard to public agencies, corresponding companies and individual persons abroad, documents and guarantees the correct observance of data protection.[1)]

Apart from the fact that a licensing requirement is, of course, also an essential contribution to the general raising of the data protection level obtained in practice, further economic aspects advocate a data protection licensing system which, as the Swedish example shows, does not have to be excessively expensive at all. In general terms, a licensing system increases data protection efficiency insofar as it enables pragmatic solutions to be achieved for various individual aspects of data protection without unsuitable concessions with regard to the data protection level attained.

Adequate registration and licensing of personal data files and data processing applications thus enables the publicity requirements, in particular in the field of notifications and granting of information, to be kept at a practical level, since the corresponding registers which are officially kept and are generally accessible and published in one form or another (directly or indirectly) already cover a basic requirement of

1) It seems significant that traditionally very pragmatic British voices have been raised in support of a licensing system; see British Computer Society/Computing Services Association/Data Processing Association 1978. See also European Computing Services Association 1978 where in particular the concept of a data protection certificate is mentioned.

publicity. In particular, however, the special efficiency of a licensing system is founded on the confidence which it generates among the public in regard to the data protection level attained. Through this, substantial friction losses in the field of data protection are avoided to a great extent. Corresponding confidence in the observance of data protection reduces, for example, the occurrence of information requests, with all the potential subsequent problems connected with them.

For the reasons stated above, registration and licensing should be made free of charge or for a nominal lump-sum fee.

4.6.1.3 National data protection authorities

The setting up of national data protection authorities (in certain circumstances with a regionalised structure) is, on the one hand, the logical complement to a data protection registration and licensing system and, on the other hand, is necessary for the efficient implementation of national data protection regulations and international harmonising guidelines. [1] In addition to practical decisions on individual cases, valuable know-how and means are set up at the same time at a central point, through which substantial contributions can be made, not

1) See also the Recommendations no.10 ff of the European Parliament with regard to the setting up of national independent data protection bodies and their functions, Europäisches Parlament, Rechstausschuss 1979, pp 10, 11, 28, 29, 31.

only to the adequate further development of data protection, but also to the development of more comprehensive concepts concerning data and information policies and of relevant social objectives.

4.6.1.4 Notification

Any community guidelines concerning the (free of charge) notifications with regard to storage, processing, distribution etc. of personal data should be based substantially on the possibilities of automated (direct or indirect) notification procedures. If general notification in the form of publications or virtual notifications in the form of data registers etc. of the data protection authority, which are kept open to general access, are not regarded as sufficient, it should be carefully checked to what extent the obligation of periodic repeated notification of the data subjects is suitable. An efficient general data protection structure on the basis of a licensing system administered by a data protection authority, and also the utilisation of efficient notification procedures, permit the data subjects to be repeatedly notified not only on the occasion of the first storage, processing, transfer etc. of personal data, but also at certain periods or on certain occasions in areas where this appears to be suitable for the interest of data protection that is not only theoretical. [1)]

1) Recommendation no.4 of the European Parliament, which only aims at single notification in the case of initial storage, probably does not go far enough. See Europäisches Parlament Rechtsausschuss, 1979, pp 9 & 28.

4.6.1.5 Granting of access

Even from the aspects of costs, it seems proper not to impede the right of data subjects to data protection information either by fees or by time limitations or other limitations. [1] On the contrary, the national data protection authorities, both at national level and in co-operation at international level, should persistently support data subjects in the exercise of their rights to information and notification, and other associated rights based on the principle of registration and licensing. In this connection, an essential objective is to reduce the implicit and partly considerable private administrative burden which arises for the individual in pursuance of his data protection rights, especially in the national sphers, so that it does not become a barrier which degrades these rights substantially to theoretical positions.

Apart from certain saving regulations (especially as regards some sectors), only administrative or legal decisions concerning individual cases (as an "emergency brake" so to speak) should be able to limit the right of the data subject to information and notification which is basically not burdened by either fees or time or other limitations.

1) See also Recommendation no.3 of the European Parliament, which does not, however, exclude a time limitation, but otherwise favours complete freedom from fees and costs for the exercising of data protection rights by data subjects. Europäisches Parlament Rechtsausschuss, 1979, pp 10 & 30.

In the international sphere, however, due to economic considerations, channeling of such requests by individual data subjects via the co-operating national data protection authorities would probably occur.

4.6.1.6 Data security

In the sphere of data security, one can reasonably expect from Community guidelines only more or less precise objectives (similar to the list in the appendix to para. 6 of the German Federal Data Protection Law). Further putting into specific terms of this data security objective, and in particular the periodic informing in this respect of the data processing agencies, should be left basically to the co-operating national data protection authorities.

4.6.1.7 Data protection commissioners and data protection liability

The question of personal and substantial data protection liability is potentially a competition-distorting element. At this point it is merely remarked that effective carrying out of data protection regulations presupposes, on the one hand, personal liability (also subject to criminal law) and on the other hand, substantial liability both for material (financial) and immaterial (moral) damages which in certain circumstances should be essentially independent of negligence (strict liability). Whilst it also seems appropriate to identify a specific person responsible comprehensively for data protection legal requirements

(for example, corresponding to the German company data protection commissioner), the specific data processing agency should in the final analysis be fully liable itself, in particular with respect to the civil liability law.

International harmonisation is especially necessary with regard to immaterial (moral) damages. [1)]

4.6.2 Costs of data protection harmonisation

The costs arising from data protection harmonisation carried out at European level cannot reliably be estimated in the abstract. They are probably, however (if harmonisation takes place with regard to content roughly within the framework outlined here), not heavy. This applies especially to the additional burdens arising for personal data processing agencies; and this is probably because practically an international consensus implying nine (and more) governments with respect to data protection harmonisation will hardly be realised which leads to high data protection burdens. In addition, it would also be the aim of international data protection harmonisation to limit, if not reduce, the data protection costs existing in the international sphere.

With regard to the costs arising through the international data protection harmonisation mechanism to be established, no reliable estimates can be made at the

1) With regard to the questions of liability, see also Recommendation no.3 of the Europäisches Parlament Rechtsausschuss, 1979, pp 9 & 28.

present stage either. To the extent, however, that, in particular, the conversion and carrying out of any international data protection harmonisation guidelines etc. will be transferred mainly to the specific appropriate national bodies (preferably central national data protection authorities), no appreciable additional costs should occur. This applies especially if the national data protection authorities carry out such a guideline in self-organising practical co-operation, and on a Community basis for example merely secretarial and clearing functions, or even only observation functions, are attended to.

4.7 Possible main points of emphasis of future research orientated towards economic and other related aspects of data protection

4.7.1 Accompanying research for the preparation and implementation of European data protection guidelines

In addition to the aspects which were investigated or mentioned in this part of the study, there are many economic and related aspects which must be taken into consideration within the framework of the preparation and implementation of European guidelines for data protection harmonisation. This applies in particular if special data protection guidelines for specific sectors of the economy or data processing applications are concerned, and in general to the problems of international data flows.

Accompanying research orientated towards economic aspects would in this connection have basically the double objective of, on the one hand, investigating the economic effects of planned guidelines which may be inadequate when it comes to their practical application as regards costs or otherwise and, on the other hand, of showing the possibilities of efficient implementation and subsequent application of appropriate data protection regulations. The practical experience, for example, gained in the USA and Canada with various data protection regulations and other regulations concerning information in the various sectors of the economy at state and federal level (e.g. in the field of finance and credit information) can be taken as starting points and subjects of such investigations.

With regard to transborder data flows, an exact analysis of the relevant practices (e.g. in the framework of specialised networks: SWIFT, SITA... or of internal networks of internationally operating organisations) and also of the first practical results of relevant regulations (especially in Sweden) would be indispensable.

In this context the following issues appear specifically to need further investigation:

- practical implications and costs of the public data protection supervisory authorities (European Community, Scandinavia, Austria, Canada), and estimation of the corresponding implications and costs of European data protection harmonisation (including financing schemes)
- elaboration of a body of European data protection statistics covering on a coherent basis the practical implications and costs etc. due to the various national data protection regulations (private sector)
- practical economic implications (cost etc.) of international data protection regulations in specific sectors of industry (address vendors/direct mail, banking and insurance, credit reporting etc., computer bureaux and data bank vendors etc.) with special regard to American sectoral data protection regulations
- study of the harmonisation issue on the level of state data protection regulations within and between the USA

and Canada (with special regard to economic aspects)

- the issue of de facto distortions of international competition due to data protection
- practical implications and problems of international data protection regulations with regard to internal communications of multinational companies and groups (particularly in the areas of clients, marketing, financial and personnel data)
- function of data protection as an integral part of efficient data resource management at company level
- experience regarding the practical implications and costs of various international freedom of information regulations (Sweden, USA, Canada etc.)
- practical and economic aspects of the data protection issue with regard to new electronic information and communication technologies
- data protection, personal profiles, automatic decision-making, administrative and technical control technologies.

4.7.2 Economic aspects of data protection of legal persons

A second possible main point of emphasis of research orientated towards economic aspects is, in this connection, the problem of the protection of the data of or about legal persons. In this case, taking into account the realities of the practical field and of the European interest in harmonisation, it would be necessary to investigate the type, method, operational and economic effect of such data protection of legal

persons. It is to be assumed that these problems will considerably increase in importance in the coming years.

4.7.3 Legal framework of a European common data and information market

A third possible main point of emphasis (which widens the problems of data protection) of future research is finally the extremely important question of the necessity with regard to industrial policy of creating an enlarged common legal framework concerning data and information at European level for the building up of a real common data processing market. It is to be noted that, in view of the continuing build-up of national and European public data transmission networks and generally accessible data banks (kept by private or public entities), and also the future diverse information services to be based on these, the preparation of an integrated European data and information market is already urgent at the present time. A basic consideration is that the lack of adequate institutional framework concerning data and information both at national and European level will delay and obstruct the development of this sector of the economy which is extremely important for the economic efficiency and independence of Europe.

The exceptional importance which legal regulations concerning data and information can have for the development of decisive sectors of the service industries, and especially the information industry, can be clearly shown for instance by the statement that

without bank secrecy (a legal regulation concerning information) the entire banking and financing industry as we know it would not be conceivable. The mature and far-seeing acceptance of the idea of legally guaranteed data protection by Swedish industry as a necessity and prerequisite for the socially acceptable and economical introduction and utilisation of modern information technologies points in this direction as well.

In this connection it should therefore be investigated to what extent, beyond data protection regulations, further common European legal regulations concerning data and information are neccessary. In this case, the following problem areas of future research in the field of electronic information industry can be named in the form of keywords:

- Data and information liability or guarantee regarding permanent availability, quality etc. of data bank services and such like
- Proprietory rights with respect to electronic data and information as well as services and products based on these
- Rights of access and use by individuals and organisations of data banks, data networks, application software, interpretational know-how etc.
- Private and public organisation of infrastructures in the area of information technology, information resources, information industries etc.

- Legal issues of authentification and evidence with respect to electronic data etc.
- Private and governmental rights of access and inspection with respect to data banks etc.(e.g. as legal evidence, checking of data and programs for automatic decision-making, publication of cryptographic transmission codes etc.)

Adequate research into these and related fields is also of special importance for the Community, since through this an important contribution is made to the determination of positions concerning industrial policy which the Community is occupying in discussion and competition with the USA as the dominating information industry.

4.8 Bibliography

[1] Abele, Paul R.:
Die Kosten der Informationsverarbeitung in Kreditinstituten.
In: IBM Nachrichten 26(1976) H.226 S.42-47

[2] American Federation of Information Proceeding Societies (AFIPS):
System Review Manual on Security.
Montvale, N.J.: AFIPS Press, 1974, 109 pp.

[3] Anderson, Margaret L.B.:
The Forthcoming data protection legislation: A Talk by Paul Sieghart.
In: Computer and Law Vol. 9(1976) pp.5-6

[4] Anderson Company:
Computer Security Reguirements: An Investigation of Computer Security Costs.
(Rep. No.ESD-TR-77-24 for Command and Management Systems, Electr.Systems Div.,Hanscom Air Force Base, MA).
Fort Washington, PA 1976
January, 70 pp.

[5] Angermann, Adolf; Schmidt, Werner; Thome, Rainer:
Untersuchung über die Kostenwirkung eines Bundesdatenschutzgesetzes (in der Fassung des Entwurfs vom 10.12.1975).
Heidelberg 1976
(Unveröffentliches Manuskript) 51 S.

[6] Angermann, Adolf; Thome, Rainer:
Ansätze für eine Kosten-Nutzen-Analyse des Datenschutzes.
In: data report (1973) H.4 S.18-22

[7] Auernhammer, Herbert:
Die Konzeption des Entwurfs des Bundesdatenschutzgesetzes unter besonderer Berücksichtigung des betrieblichen Datenschutzbeauftragten.
Dortmund 1974
In: Der Datenschutzbeauftragte: Gesetzliche Anforderungen und Erfahrungen in der Praxis, S. 17-31

[8] Auernhammer, Herbert:
Probleme der Datenschutzgebung, auch unter Wirtschaftlichkeitsaspekten. Referat auf dem Internationalen kkongreß für Datenverarbeitung.
Berlin 1976
(Manuskript)

[9] Avison, D.E.; Crowe, T.:
Computers and Privacy.
In: Computer Bulletin, March 1976, pp. 8-13

[10] Barna, Becky:
Information Management: A New Threat to Multinationals.
In: Computer Decisions, August 1978, pp. 34-38

[11] Bayerl, Alfons:
Bericht über den Besuch beim schwedischen Datenüberwachungsamt, 23. und 24. Januar 1979.
Europ. Parlament, Rechtsausschuß, Unterausschuß "DV und Persönlichkeitsrecht", Dokument PE 56.958/Anl. 1, 30.1.1979, 6 S.

[12] Benjamin, Alan A.:
Privacy, Security and Responsibility.
In: Transnational Data Regulation, Conference Proceedings, Brussels, February 1978, Uxbridge: Online Confer. Ltd., 1978a, pp.1-8

[13] Benjamin, Alan A.:
The Impact of Privacy and Security Regulations upon Installation Performance.
In: SEAS (ed.): Proceedings Spring Technical Meeting 1978: Performance of Computer Installations. Berne, 1978b, pp. 133-141

[14] Berg, John L. (Ed.):
Exploring Privacy and Data Security Costs: A Summary of a Workshop, February 20, 1975, Gaithersburg, Maryland.
National Bureau of Standards, Washington, D.C., Tech. Note 876. Washington, D.C.: U.S. Government Printing Office, VI,28pp

[15] Bergmann, Lutz; Möhrle, Roland:
Datensicherung in Rechenzentren: Leitfaden für Wirtschaft und öffentliche Verwaltung.
DKT-Schriftenreihe, Band 1.
Datakontext-Verlag, Köln, 1979, 54 S.

[16] Betriebswirtschaftliches Institut für Organisation und Automation (BIFOA) an der Universität zu Köln:
Maßnahmen zur Datensicherung und zum Datenschutz: Probleme und Kosten der Implementierung.
Informationsforum, 16.2.79,
Tagungsunterlagen, Köln, BIFOA 1979

[17] Bing, Jon:
Transborder Data Flows: Some Legal Issues and Possible Effects on Business Practices.
In: Transnational Data Regulation, Conference Proceedings, Brussels, February 1978,
Uxbridge: Online Confer. Ltd., 1978,pp.15-27

[18] Bode, Albrecht; Drews, Hans-Ludwig:
Die Auswirkungen des Bundesdatenschutzgesetzes in der Industrie.
In: Siemens-Zeitschrift, Vol. 51, Heft 5, Mai 1977, S. 370-375

[19] Böhm, Kurt:
Kostenimplikationen von Datenschutzregelungen.
In: Dierstein, Rüdiger; Fiedler, Herbert; Schulz, Arno (Hg.): Datenschutz und Datensicherung. Köln 1976, S. 216-226

[20] Böhm, Kurt:
Datenschutz für medizinische Daten: Gesetzliche Bestimmungen und ihre Kosten.
In: Datenschutz und Datensicherung (1977) H.2 S.78-81

[21] Brack, Werner:
Sicherheitsfragen in der Datenverarbeitung.
In: Datascope (1977) H.25 S.10-16

[22] Breker, Klaus:
Auswirkungen des BDSG auf den Konzern, insbesondere den Versicherungskonzern.
In: Datenschutz-Berater (1978a) H.4 S.56-62

[23] Breker, Klaus:
Problematischer Datenschutz im Konzern.
In: Online adl-Nachrichten (1978b) H.9 S.680-682

[24] Brennan, Edward J.:
Statement of Edward J. Brennan, Jr., Vice President and General Manager, TRW Information Services, Long Beach, Cal., before the Privacy Protection Study Commission.
Washington, August 4, 1976, 17 pp.

[25] British Computer Society, Privacy Committee:
Submission of Evidence to the Committee on Privacy (Younger Committee).
March 1971, 25 pp.

[26] British Computer Society:
Submission of Evidence to the Data Protection Committee (Lindop Committee).
October 1976, 31pp + appendices

[27] British Computer Society; Computing Services Association; Data Processing Management Association:
Privacy, Security and Computers: A Joint Statement Europ. Parl., Legal Affairs Committee, Sub-Committee 'Data Processing and Individual Rights', Public Hearing, Brussels, 6 Feb. 1978.
Working Dokument No. 8, PE 52.105, 16 Jan. 1978, 3 pp.

[28] Brossmann, Michael:
Ordnungsmäßigkeit der DV: Neue Prüfmethoden notwendig.
In: Der Arbeitgeber 30(1978) H.10 S.498-499

[29] Browne, Peter S.:
Computer Security - A Survey.
In: AFIPS Conference Proceedings, Vol. 45, National Computer Conference, New York, June 7-10, 1976, pp. 53-63

[30] Brussard, B. K.:
The Price of Privacy.
In: Frielink, A. B. (ed.): Economics of Informatics: Proceedings of the IBI-ICC Symposium, Mainz 16-20 Sept. 1974. Amsterdam 1975, pp. 53-62

[31] Brussard, B. K.:
The Price of Privacy.
In: US Senate: Privacy and Protection of Personal Information in Europe. Committee on Government Operations, March 1975. US government Printing Office. Wash. 1975a pp.112-118

[32] Bull, Hans Peter:
Das Bundesdatenschutzgesetz in der ersten Phase seiner Verwirklichung.
In: Online adl-Nachrichten (1978) H.7/8 S.572-575

[33] Bundesbeauftragter für den Datenschutz:
Erster Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, Bonn 1979, 71 S.

[34] Callies; Bresson:
Elements pour une methode d'evaluation des couts entraines par l'exercice du droit d'acces aux fichiers.
In: Commission Informatique et Libertes 1975b, annexe G, pp. 421-425

[35] Canadian Bar Association:
Comments on the Green Paper on Legislation on Public Access to Gouvernment Documents and Recommendations for a Model Bill on Freedom of Information in Canada.
Ottawa April 4, 1978, 31 pp.

[36] Canadian Human Rights Commission:
Annual Report of the Privacy Commissioner 1978.
Minister of Supply and Services, Ottawa 1979, 16 pp. + appendices

[37] Capital:
Datenschutz scheitert an den Kosten: Kein Recht mehr auf Privatleben.
In: Capital (1976) H.1 S.61-63

[38] Cary, Frank T.:
IBM's Guidelines to Employee Privacy (An Interview).
In: Harvard Business Review, Vol. 54, No. 5, Sept./Oct. 1976, pp. 82-90

[39] Chamoux, Jean-Pierre:
The Economics of International Telecommunications.
In: Telecommunications, May 1979, pp. 79-82

[40] Chastain, Dennis R.:
Security vs. Performance.
In: Datamation Vol. 19(1973) No.11 pp.110-116

[41] Civil Service Department:
Disclosure of Official Information: A Report on Overseas Practice.
London: Her Majesty's Stationary Office, 1979, V, 54 pp. + Appendices: 150 pp.

[42] Commission Informatique et Libertes:
Rapport de la Commission Informatique et Libertes, tome 1.
Paris 1975a
106 pp

[43] Commission Informatique et Libertes:
Rapport de la Commission Informatique et Libertes, Annexes, tome 2.
Paris 1975b
446 pp

[44] Committee on Data Protection:
Report of the Committee on Data Protection.
Chairman: Sir Norman Lindop.
Her Majesty's Stationary Office, Cmnd.7341, December 1978, XXIV, 460 pp.

[45] Committee on Data Protection:
Summary of the Findings of the Cost Study Consultants.
In: Committee on Data Protection: Report of the Committee on Data Protection. Her Majesty's Stationary Office, Cmnd. 7341, Dec 1978, pp.443-448

[46] Committee on Privacy:
Report of the Committee on Privacy. Chairman: Sir Kenneth Younger.
Her Majesty's Stationary Office, Cmnd. 5012, London, July 1972, XI, 350 pp.

[47] Comptroller General of the United States:
Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment. Report to the Congress.
Washington: U.S. General Accounting Office, April 28, 1978a, V, 48 pp.

[48] Comptroller General of the United States:
Data on Privacy Act and Freedom of Information Act Provided by Federal Law Enforcement Agencies.
Washington: U.S. General Accounting Office, June 16, 1978b, Report and Appendices

[49] Comptroller General of the United States:
Government Field Offices Should Better Implement the Freedom of information Act.
Washington: U.S. General Accounting Office, July 25, 1978c, VIII, 47 pp.

[50] Comptroller General of the United States:
Impact of the Freedom of Information and Privacy Acts on Law Enforcement Agencies.
Washington: U.S. General Accounting Office, November 15, 1978d, II, 36 pp.

[51] Computer Talk:
Lawyers say they cannot handle privacy legislation.
In: Computer Talk 27.6.1979, p. 5

[52] Computerzeitung:
Der Mittel-Weg: Dr. Auernhammer im CZ-Interview: Datenschutz kostet ein Prozent.
In: Computer Zeitung (1976) H.6 S.1,2,4,7

[53] Computing:
Privacy could force prices up.
In: Computing Europe Vol. (1977) No.2 pp.1

[54] Computing Services Association:
Technical Guidelines on Privacy: Suggested Technical Guidelines for Organisations in Preparation for On-Coming Privacy Legislation in the United Kingdom.
September 1977, 30 pp.

[55] Data Processing Digest:
Modeling Computer Privacy Costs, by Robert C. Goldstein, Installation Management Review, Vol. 7, Nos. 1-4, 1978, pp. 7-14. (Review).
In: Data Processing Digest Vol. (1979) No.8 p.11

[56] Datainspektionen:
Guidelines for the Data Inspectorate's Inspection Procedures in Accordance with the Data Law.
Stockholm, 6.7.1978, 12 pp.

[57] Datenschutz-Berater:
Rationalisierungseffekte durch das BDSG.
In: Datenschutz-Berater (1977) H.5 S.75-76

[58] Datenschutz-Berater:
Ausbau der Dateiinventur zu einer rechnergestützten Dokumentation: Rationalisierungseffekte durch das BDSG.
In: Datenschutz-Berater (1978a) H.3 S.36-38

[59] Datenschutz-Berater:
Grundsätze ordnungsmässiger Speicherbuchführung (GoS) im Bundessteuerblatt veröffentlicht.
In: Datenschutz-Berater (1978b) H.10 S.154-155

[60] Datenschutz-Berater:
Kosten- und Leistungsverrechnung bei der Datenverarbeitung.
In: Datenschutz-Berater (1979a) H.6 S.14-15

[61] Datenschutz-Berater:
Informationsforum des BIFOA, Universität Köln, Maßnahmen zur Datensicherung und zum Datenschutz Probleme und Kosten der Implementierung?.
In: Datenschutz-Berater (1979b) H.8 S.10

[62] Delbetänkande av datalagstiftingskomitten (DALK):
Personregister Datorer Integritet.
Stockholm 1978
(English Summary pp. 337-363)

[63] Deutscher Bundestag:
Bericht und Antrag des Innenausschusses (4. Ausschuß) zu dem von der Bundesregierung eingebrachten Entwurf eines Gesetzes zum Schutze vor Mißbrauch personenbez. Daten bei der Datenverarbeitung.
Bundesdatenschutzgesetz - Drucksache 7/1027.
Drucksache 7/5277. 2.6.1976

[64] Deutscher Bundestag, Innenausschuß (724-2453):
Stellungnahmen zu den Fragen für die öffentliche Anhörung zum Entwurf eines Bundesdatenschutzgesetzes.
Ausschußdrucksache 7/137, Drucksache 7/127, 26.3.1976a

[65] Deutscher Bundestag, Innenausschuß (724-2450):
Protokoll der 104. Sitzung des Innenausschusses und der 83. Sitzung des Ausschusses für Wirtschaft, durchgeführt am 31.3.1976 als öffentliche Anhörung zu Fragen der Datenschutz-Gesetzgebung.
Bonn 1976b

[66] Deutscher Bundestag, Innenausschuß (724-2453):
Unkorrigiertes stenographisches Protokoll der öffentlichen Anhörung des Innenausschusses zum Entwurf eines Bundesdatenschutzgesetzes am 31.3.1976.
Ausschußdrucksache 7/139, 6.4.1976c

[67] Dierstein, R.:
BDSG. Novellierung. nein aber .....
In: Der Arbeitgeber 31(1979) H.2 S.76-77

[68] Dierstein, Rüdiger; Fiedler, Herbert; Schulz, A. (Hg.):
Datenschutz und Datensicherung. Fachtagung 1976 der ÖGI und der GI.
Köln 1976

[69] Domestic Council Committee on the Right of Privacy and The Council of State Gouvernments (Ed.):
Privacy: A Summary of a Seminar of Privacy: December 15-17, 1974, Washington, D.C.
Lexington, Kentucky, The Council of State Gouvernements, 1975, VII + 64 pp.

[70] Donovan, J.F.:
Problems of privacy.
In: Diebold Research Program-Europe, Data Exchange, May-June 1977, pp. 18-20

[71] Douglas, A.S.:
The U.K. privacy white paper 1975, In: AFIPS: Conference Proceedings 1976 National Computer Conference, June 7-10, 1976, New York City, N.Y.
Montvale, N.Y.: AFIPS Press, 1976, pp. 33-38

[72] Duschanek, Alfred (Ed.):
Datenschutzgesetz 1978. Kommentar.
Österreichischer Wirtschaftsverlag. Wien
1979, 148 pp.

[73] Ehrich, Hermann:
Datensicherung mit vertretbaren Aufwand.
In: Datenschutz und Datensicherung (1978) H.4
S.190-193

[74] Ehrich, Hermann; Kirchherr, Roland; Pusch,
Eberhard:
Datenschutz bei Sparkassen: Ein praktischer
leitfaden zur Anwendung der Datenschutz-
gesetze in der Sparkassenorganisation.
Deutscher Sparkassenverlag, Stuttgart, 1978,
206 S.

[75] Ehrlich, Götz:
Datenschutz-Testat: Neue Aufgaben für
Wirtschaftsprüfer?.
In: Der Arbeitgeber 30(1978) H.5 S.191

[76] Ellison, J.R.:
Privacy Legislation: Feasibility and Costs.
Manchester: National Computing Centre,
February 1977, 5 pp.

[77] Europäisches Parlament, Rechtsausschuß,
Unterausschuß Datenverarbeitung und
Persönlichkeitsrecht:
Vollständiger Wortlaut des Hearings über
Datenverarbeitung und Persönlichkeitsrechte.
Brüssel, 6.2.1978.
Europäisches Parlament, Generaldirektion
Ausschüsse und interparlamentarische
Delegationen. Dokument PE 52.496, 288 S.

[78] Europäisches Parlament, Rechtsausschuß:
Bericht über den Schutz der Rechte des
Einzelnen angesichts der fortschreitenden
technischen Entwicklung auf dem Gebiet der
Datenverarbeitung. Berichterstatter: Alfons
Bayerl.
4. Mai 1979, Dokument 100/79 Europäisches
Parlament, PE 56.386, 88 S.

[79] European Computing Services Association (ECSA):
Privacy, Data Protection, Security and Computers. Statement by the European Computing Services Association (ECSA) to the Council of Europe, 1978, 9 pp.

[80] Farr, M.A.L.; Chadwick, B.; Wong, K.K.:
Security for Computer Systems. 2nd Impression.
Manchester/London 1973

[81] Fischer, Hans-Jürgen:
BDSG und die Revisions-Abteilung. In:
DSB-Kongress '78, 8.-10.5.1978, Düsseldorf.
Kongress-Dokumentation.
München: CSMI, 1978, 10 pp.

[82] Fiselius, Günter:
Datenschutz und Bundesrechnungshof (BRH).
In: Datenschutz und Datensicherung (1977) H.2
S.70-72

[83] Fishlock, David:
Protecting privacy could double computer cost.
In: Financial Times 29.3. 1977, p. 9

[84] Fishman, William L.:
International Data Flow: Personal Privacy and Some Other Matters.
Fourth International Conference on Computer Communication, Kyoto, Japan, September 26-29, 1978, 28 pp.

[85] Focus on France.
In: Transnational Data Report Vol. 1(1978) No.1 pp.1-8

[86] Focus on Germany.
In: Transnational Data Report Vol. 1(1978) No.2 pp.1-2, 15-21

[87] Focus on Norway and Sweden.
In: Transnational Data Report Vol. 1(1978) No.3 pp.1-6, 14-16

[88] Focus on Denmark.
In: Transnational Data Report Vol. 1(1978) No.4 pp.1f,4f,8,12

[89] Focus on United Kingdom.
In: Transnational Data Report Vol. 1(1979) No.8 pp.1-4,10-14

[90] Freese, Jan:
The Swedish Data Act.
In: Review Briefings Eurocomp78, online-conference, London 1978, 8 pp.

[91] Freiling, Claus:
Zur Stellung des Datenschutzbeauftragten in der Unternehmung.
In: Zeitschrift für Organisation (1977) H.8 S.449-453

[92] Futh, Horst:
Ein einfaches Verfahren zur Abschätzung von Kosten und Risiken der Datenschutz- und Datensicherungsmaßnahmen.
In: Dierstein, Rüdiger; Fiedler, Herbert; Schulz, Arno (Hg.): Datenschutz und Datensicherung. Köln 1976, S. 227-238

[93] Gabler:
Dr. Gablers Wirtschafts-Lexikon, Kurzausgabe.
Frankfurt 1972

[94] Gassmann, Hans-Peter:
Probleme bei internationalen Datenflüssen und Gemeinsamkeiten des Datenschutzes in Europa.
In: Dierstein, Rüdiger; Fiedler, Herbert; Schulz, Arno (Hg.): Datenschutz und Datensicherung. Köln 1976, S. 11-26

[95] Gliss, Hans:
Mitteilung des Vorstandsvorsitzenden der Gesellschaft für Datenschutz und Datensicherung an Edmund F.M. Hogrebe, 3. August 1979, 2 S.

[96] Gola, Peter:
Ein Datenschutz-Test.
In: Datenschutznachrichten (1978a) H.2 S.2-5

[97] Gola, Peter:
Die Benachrichtigungspflicht ist mit Kosten verbunden.
In: Computer Zeitung (1978b) H.7 S.43

[98] Gola, Peter; Hümmerich, Klaus; Kerstan, Uwe:
Datenschutzrecht: Erläuterte Rechtsvorschriften und Materialien zum Datenschutz.
Teil 1: Das Bundesdatenschutzgesetz, Verfassungsrechtlicher Datenschutz, Internationaler Datenschutz.
Berlin 1977
J. Schweitzer Verlag, 120 S.

[99] Gola, Peter; Hümmerich, Klaus; Kerstan, Uwe:
Datenschutzrecht: Erläuterte Rechtsvorschriften und Materialien zum Datenschutz.
Teil 2: Einzelvorschriften des Bundes zum Datenschutz.
Berlin 1979
J. Schweitzer Verlag, XIII, 250 S.

[100] Golding, Edwin I.:
The Administrative Burdens of Privacy Legislation.
In: Renninger, Clark (ed.): Approaches to Privacy and Security in Computer Systems. NBS Special Publication 404. Washington, US Department of Commerce, NBS, Sept. 1974 p.66

[101] Goldstein, Robert C.:
The Cost of Privacy: Operational and Financial Implications of Databank-Privacy Regulation.
Brighton, Mass: Honeywell Information Systems Inc. 1975a, 150 pp.

[102] Goldstein, Robert C.:
The Cost of Computer Privacy and Security.
In: Honeywell Information Systems (ed.): Computer Security and Privacy Symposium.
Waltham, Mass, August 1975b, pp. 13-19

[103] Goldstein, Robert C.:
The Costs of Privacy.
In: Datamation Vol. 21(1975c) No.10 pp.65-69

[104] Goldstein, Robert C.:
Modeling Computer Privacy Costs.
In: Installation Management Review, Vol. 7, Nos. 1-4, 1978, pp. 7-14

[105] Goldstein, Robert C.; Nolan, Richard:
Personal Privacy Versus the Corporate Computer.
In: Harvard Business Review March-April 1975, Vol. 53, No. 2, pp. 62-70

[106] Goldstein, Robert C.; Seward, Henry H.:
A Computer Model to Determine Low Cost Techniques to Comply with the Privacy Act of 1974. User's Guide. NB SIR 76-985.
U.S. Department of Commerce, National Bureau of Standards, February 1976, III, 52 pp. (NTIS PB-250.755)

[107] Goldstein, Robert C.; Seward, Henry H.; Nolan, Richard L.:
A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Reguirements.
NBSTN-906.
U.S. Department of Commerce, National Bureau of Standards, June 1976, VII, 64 pp. (NTIS PB-254.048)

[108] Green, Roger:
Privacy could force prices up.
In: Computing Europe No. 2, 13.1.1977, p. 1

[109] Hanusch, Horst:
Zur wohlfahrtsökonomischen Theorie der finanzwirtschaftlichen Entscheidung.
In: Recktenwald 1970, S. 41-86

[110] Hanusch, Horst:
Theorie des öffentlichen Gutes: Allokative und distributive Aspekte.
Göttingen 1972

[111] Harris, Louis and Associates, Inc.; Westin, Alan F.:
The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy, Conducted for Sentry Insurance, 1979, 104 pp.

[112] Hebditch, David:
Will Data Flow be Stemmed?.
In: Telecommunications, May 1979, pp. 75-82

[113] Hennings, James Michael:
Toward an Understanding of Cost-effective Access Control in Data Base Systems.
Ohio State University, Master's thesis, 1976, 138 pp.

[114] Hogrebe, Edmund F. M.:
Verwaltungsautomation und Datenschutz in Frankreich.
In: EDV und Recht Bd. 9. Berlin, 1976, 649 S.

[115] Hogrebe, Edmund F. M.:
Second Look at Implementing the German Data Protection Act.
In: Transnational Data Report Vol. 1(1978) No.3 pp.9-12

[116] Hogrebe, Edmund F. M.:
Wirtschaftliche Aspekte des Datenschutzes.
In: GMD (Hg.): Auswirkungen des Datenschutzes. Eine Studie zum Datenschutz.
München/Wien, 1979, S. 482-511

[117] Home Office:
Computers and Privacy. (White Paper).
Her Majesty's Stationary Office, Cmnd. 6353, London, December 1975a, 13 pp.

[118] Home Office:
Computers: Safeguards for Privacy (Report).
Her Majesty's Stationary Office, Cmnd. 6354,
London, December 1975b, 48 pp.

[119] Honeywell Information Systems (ed.):
Computer Security and Privacy Symposium:
Proceedings, April 29-30, 1975, The Inn Mc
Cormick Ranch, Scottsdale, Arizona.
Waltham Mass.: Honeywell Information Systems,
August 1975, 121 pp.

[120] Hund, Jürgen:
Änderung des Bundesdatenschutzgesetzes.
In: Datenverarbeitung in Steuer, Wirtschaft
und Recht (1976) H.5 S.146-150

[121] IBM (ed.):
Elements and Economics of Information Privacy
and Security.
In: IBM (ed.): Data Security and Data
Processing. Vol. 3, Part 2, Study Results:
State of Illinois, White Plains N. Y. 1974,
pp. 23-244

[122] Institute of Data Processing:
Evidence to the Data Protection Committee.
September 1976, 8 pp.

[123] Jamin, Klaus:
Umfrage zum Datenschutzbeauftragten: Aufgaben
erfüllt.
In: Bit, Mai 1978, S. 64-68

[124] Janssens, Carol Jean:
Privacy Legislation and its Implication
Toward the Computer Industry.
Naval Postgraduate School, Monterey, Cal.,
Master's thesis, June 1977, 51 pp.

[125] Joinet, Louis; Bancilhon, Francois:
Rapport sur la Commission Suedoise
d'Inspection des Donnees (Datainspection).
Stockholm, 20-23.3. 1979.
Commission Nationale de l'Informatique et des
Libertes, Paris, 1979, 17 pp.

[126] Kargl, Herbert; Reinermann, Heinrich; Schmidt, Werner; Thome, Rainer:
Probleme des Bundesdatenschutzgesetzes aus betriebswirtschaftlicher Sicht.
In: Datenschutz und Datensicherung (1979) H.1 S.9-16

[127] Kenny, J.J.:
The White Paper.
In: Computer Bulletin March 1976, pp. 7, 16

[128] King, John Leslie; Schrems, Edward L.:
Cost-Benefit Analysis in Information Systems Development and Operation.
In: Computing Surveys, Vol. 10, No. 1, March 1978, pp. 19-34

[129] Kirchner, Jake:
Users Still Not Safeguarding Privacy.
In: Computerworld, August 6, 1979, p. 32

[130] Klempner, I.M.:
Secrecy; or the Cost of Withholding Information.
In: Proceedings of the American Society for Information Science, Vol. 10, 1973, pp. 111-113

[131] Knabben, Walter:
Datenhaftung: Der Datenunfall und seine zivilrechtlichen Folgen.
Köln: Data Kontext-Verlag, 1979, 42 S.

[132] Kraus, Wolfgang:
Datensicherungsmaßnahmen nach dem BDSG. Die Realisierung der Datensicherungsmaßnahmen des Bundesdatenschutzgesetzes unter besonderer Berücksichtigung der Problematik des Personalwesens.
Köln: Data Kontext-Verlag, 1978, 222 pp.

[133] Lamb, John:
Extra costs warning from top privacy man Lindop.
In: Computer Talk 22.11.1978, p. 1

[134] Langhorne, Rossiter W.:
Private enterprise concerns about data protection and transborder data regulations.
In: Online Conferences (ed.): Data Regulation: European and Third World Realities. Uxbridge, 1978, pp. 135-157

[135] Larsen, Kent S. (Ed.):
Privacy a Public Concern: Document based on the proceedings of a Seminar on Privacy sponsored by The Domestic Council Committee on the Right of Privacy and The Council of State Governments.
Washington: U.S. Government Printing Office, 1976, VI, 183 pp.

[136] Layard, Richard (ed.):
Cost-Benefit Analysis: Selected Readings.
Harmondsworth, Middlesex 1972

[137] Leib, Hans - Jürgen:
Kosten des Datenschutzes.
In: Öffentliche Verwaltung und Datenverarbeitung - Online - ADL-Nachrichten (1978) H.9 S.3-7

[138] Liedtke, Cornelius:
Theorie der öffentlichen Güter und optimale Struktur einer Föderation.
Berlin 1972

[139] Lobel, Jerome:
The Cost of Computer Privacy. AFIPS Conference Proceedings Vol. 44, National Computer Conference, May 19-22, 1975, Anaheim California.
Montvale, N.J.: AFIPS Press 1975, pp. 935-940

[140] Mellerowicz, Konrad:
Kosten und Kostenrechnung, Bd. 2: Verfahren, Teil 2: Kalkulation und Auswertung der Kostenrechnung und Betriebsabrechnung.
4. Aufl. Berlin 1968

[141] Mellerowicz, Konrad:
Kosten und Kostenrechnung, Band 1: Theorie der Kosten.
5. Aufl. Berlin; New York 1973

[142] Mellerowicz, Konrad:
Kosten und Kostenrechnung, Band 2: Verfahren, Teil 1: Allgemeine Fragen der Kostenrechnung und Betriebsabrechnung.
Berlin; New York 1974

[143] Mishan, E.J.:
Cost-Benefit Analysis.
London 1975

[144] Musgrave, Richard; Musgrave, Peggy; Kullmer, Lore:
Die öffentlichen Finanzen in Theorie und Praxis, Bd. 1.
Tübingen 1975

[145] Myers, Edith:
Costs, Codes, People and the Constitution: Those Who Cope with Privacy Talk it Over in Phoenix Symposium.
In: Datamation May 1976, pp. 180-182

[146] Myers, Edith:
Security: The Only Means to Privacy.
In: Datamation May 1977, pp. 240-242

[147] Myers, Edith:
Security: A Game of Catch Up.
In: Datamation May 1979a, pp. 76-79

[148] Myers, Edith:
Privacy Guidelines.
In: Datamation 1979b, pp. 79-81

[149] Nagel, Kurt:
Neugestaltung der handels- und steuerrechtlichen Buchführungsvorschriften.
In: Nagel, K. (Ed.): DV Aktuell 1976.
Stuttgart: Science Research Associates, 1975, pp. 92-99

[150] Nagel, Kurt:
Bestimmungsfaktoren für eine Wirtschaftlichkeitsanalyse bei Datensicherungssystemen.
In: Datenverarbeitung in Steuer, Wirtschaft und Recht (1976a) H.10 S.309-315

[151] Nagel, Kurt:
Wirtschaftsanalyse bei Datensicherungssystemen.
In: IBM-Nachrichten 26(1976b) H.232 S.295-299

[152] Nagel, Kurt:
EDV-Revision.
In: Informatik-Spektrum 1(1978) H.2 S.73-80

[153] Nagel, Kurt:
Was sollte der Datenschutzbeauftragte über die Ordnungsmäßigkeit wissen.
In: Gesellschaft für Datenschutz und Datensicherung (Hg.): Datenschutzfachtagung DAFTA '78, Tagungsband. Köln 1979a, S.24-40

[154] Nagel, Kurt:
Methoden zur Bestimmung der Kosten von Datenschutz und Datensicherheit.
In: Datenschutzkongreß '79, Berlin, 11.-13. Juni 1979. Dokumentation, I/4, 1979b, 18 pp. + Exhibits

[155] National Study Group on the Security of Computer-based Systems:
Where Next for Computer Security?.
In: Report Manchester: National Computing Centre, 1974, 180 pp.

[156] Niblett, G.B.F.:
Digital Information and the Privacy Problem.
OECD Informatics Studies, No. 2, Paris 1971

[157] Nielsen, Norman R.:
Computers, Security and the Audit Function.
In: AFIPS Conference Proceedings. Vol. 44,
National Computer Conference, May 19-22 1975,
Anaheim, California.
Montvale N.J.: AFIPS Press, 1975, pp. 947-954

[158] Nielsen, Norman R.; Ruder, Brian:
Computer System Integrity Safeguards.
In: Information Processing 77, (Proceedings
of IFIP Congress 77, Toronto, August 8-12,
1977), 1977, pp. 337-342

[159] Nielson, Norman R.; Ruder, Brian; Brandin,
David H.:
Effective Safeguards for Computer System
Integrity.
In: AFIPS Conference Proceedings, Vol. 45,
National Computer Conference, New York, June
7-10, 1976, pp. 75-84

[160] Niesing, Hartmut; Uphoff, Helmut:
Kosten-Nutzen-Betrachtungen als Grundlage der
Auswahl von Alternativen - dargestellt am
Beispiel aus der Datenerfassung.
In: Öffentliche Verwaltung und
Datenverarbeitung 2(1972) S.468-476

[161] Obelode, Günter; Windfuhr, Manfred:
Datenschutz und Datensicherung (5): Methoden
zum Datenschutz und zur Datensicherung -
vorgestellt an einem praktischen Beispiel.
In: IBM Nachrichten (1974) H.221 S.232-236

[162] Österreichische Gesellschaft für Politik
(Ed.):
Der Bürger in der Informationsgesellschaft:
Materialien zum Datenschutz in Österreich.
Österreichische Gesellschaft für Politik.
Wien 1974, 42 S.

[163] Office of Management and Budget:
Privacy Act Implementation: Guidelines and Responsibilities.
In: Federal Register, Vol. 40, No. 132, Part III, Washington 1975, pp. 28.948-28.978

[164] Office of Management and Budget, Executive Office of the President:
First Annual Report of the President: Federal Personal Data Systems Subject to the Privacy Act of 1974, Calendar Year 1975. Two Volumes. July 20, 1976.
Washington: U.S. Government Printing Office, 1976, 18 pp. + Appendices

[165] Office of Management and Budget, Executive Office of the President:
Costs of Implementing the Privacy Act of 1974 (Public Law 93-579, 5 U.S.C. 552 a), March 1977a, 8 pp. + Appendices I-III.
(Report sent to Abraham A. Ribicoff, Chairman, Committee on Governmental Affairs, U.S. Senate accompanied by a letter dated March 7, 1977 from Bert Lance, Director, OMB.)

[166] Office of Management and Budget, Executive Office of the President:
Second Annual Report of the President: Federal Personal Data Systems Subject to the Privacy Act of 1974, Calendar Year 1976. June 30, 1977.
Washington: U.S. Government Printing Office, 1977b, 23 pp. + Appendices

[167] Office of Management and Budget, Executive Office of the President:
Third Annual Report of the President: Federal Personal Data Systems Subject to the Privacy Act of 1974, Calender Year 1977. July 20, 1978.
Washington: U.S. Government Printing Office, 1978, 39 pp. + Appendices

[168] Ombudsman Committee on Privacy, Association for Computing Machinery, Los Angeles.
Chapter:
Privacy, Security in the Information Processing Industry.
New York 1976
Association for Computing Machinery, 1976, XX, 187 pp.

[169] Online Conferences Ltd. (Ed.):
Data Regulation European and Third World Realities. Conference Proceedings, New York, November 1978.
Uxbridge, England: Online Ltd., 1978, VIII, 233 pp.

[170] Ordemann, Hans-Joachim:
Grenzüberschreitender Datentransport: Internationales Datenschutzübereinkommen.
In: Öffentliche Verwaltung und Datenverarbeitung (1977) H.6 S.3-7

[171] Organisation for Economic Co-operation and Development (Ed.):
Transborder Data Flows and the Protection of Privacy. Proceedings of a Symposium held in Vienna, Austria, 20.-23. September 1977.
Information, Computer, Communications Policy Series No. 1.
Paris: OECD, 1979a, 335 pp.

[172] Organisation for Economic Co-operation and Development (Ed.):
The Usage of International Data Networks in Europa. (Study commissioned from Logica Ltd., London). Information, Computer, Communications Policy Series No. 2.
Paris: OECD, 1979b, 287 pp.

[173] Ostermann, J.:
Das Konzept der gemeinsamen kommunalen Datenverarbeitung.
In: Bürotechnik (1978) H.3 S.34-35

[174] PACTEL (PA Computers and Telecommunications): The Data Protection Committee, Cost Sub-Committee, Consultancy Report. July 1977, 2+102+37 pp.
(Unpublished Cost study, commissioned by the British Committee on Data Protection; summarised in: Committee on Data Protection: Report, HMSO, Cmnd 7341, Dec. 1978, pp. 443-448)

[175] Pantages, Angeline:
The Price of Protection.
In: Datamation. March 1976, pp. 141-144

[176] Pantages, Angeline:
Is the World Building Data Barriers.
In: Datamation. December 1977, No. 12, pp. 90-103

[177] Pantages, Angeline; Pipe, G. Russel:
A New Headache for International DP.
In: Datamation. June 1977, Vol. 23, No. 6, pp. 115-123

[178] Parker, Donn B.:
A New Approach to the Cost of Computer Security.
In: Computer Security and Privacy Symposium: Proceedings, April, 29-30, 1975, The Inn McCormick Ranch, Scottsdale, Arizona. Waltham, Mass. Honeywell IS. Aug. 1975, pp. 87-90

[179] Parker, Donn B.:
Computer Abuse Perpetrators and Vulnerability of Computer Systems.
Proceedings Computer Security 1976 Conference, Amsterdam, November 1976, IAG/IFIP Application Information Processing Group

[180] Parker, Donn B.; Nycum, Susan; Oüra, S. Stephen:
Computer Abuse. Report prepared for National Science Foundation. (NTIS: PB 231-320/AS). Menlo Park, Cal.: Stanford Research Institute, 1973, 131 pp.

[181] Pipe, G. Russel:
An Assessment of Views on Transnational Data Regulation.
In: Online Ltd (Ed.): Transnational Data Regulation, Conference Proceedings, Brussels, 7-9 February 1978, 9 pp.

[182] Pipe, G. Russel:
Transnational Data Regulation: Widespread Impacts Expected.
In: Telecommunications, May 1979, pp. 71-72

[183] Poths, Willi:
Datenschutz als Teilzeitaufgabe: Probleme und Möglichkeiten in kleineren und mittleren Unternehmen.
In: Datenschutz und Datensicherung (1977) H.1 S.22-24

[184] Poths, Willi:
Kosten des BDSG in kleineren und mittleren Unternehmen.
In: Datenschutz und Datensicherung (1978) H.2 S.86-88

[185] Pougin, Erwin:
Betriebswirtschaftliche Auswirkungen des Bundesdatenschutzgesetzes.
In: Die Betriebswirtschaft 37(1977) H.4 S.523-532

[186] PRC Information Sciences Company:
The Effect of Privacy Laws on Information Management. Part I: Legal Aspects, V, 93 pp. Part II: Record Management Philosophy, V, 47 pp. Part III: Systems Audit and Implementation, 60pp.
McLean, Va/Los Angelos, Cal., March 1976

[187] Prest, A.R.; Turvey, R.:
Cost-Benefit-Analysis: A Survey.
In: Economic Journal, Vol. 75, 1965, pp. 685-705

[188] Privacy Protection Study Commission:
Report of the Privacy Protection Study Commission Personal Privacy in an Information Society. July 1977.
Washington: U.S. Government Printing Office, 1977a, XII, 654 pp.

[189] Privacy Protection Study Commission:
Report of the Privacy Protection Study Commission. Appendix 4: The Privacy Act of 1974: An Assessment. July 1977.
Washington: U.S. Government Printing Office, 1977b, 173 pp.

[190] Recktenwald, Horst Claus:
Eine Theorie der Staatswirtschaft.
In: Jahrbuch für Nationalökonomie und Statistik, Nr. 175, 1963, S. 76-89

[191] Recktenwald, Horst Claus:
Effizienz und innere Sicherheit: Unteilbare Güter: Gesetz, Ordnung, Polizei.
In: Recktenwald, Horst Claus (Hg.):
Nutzen-Kosten-Analyse und Programmbudget.
Tübingen 1970, S. 249-266

[192] Recktenwald, Horst Claus (Hg.):
Nutzen-Kosten-Analyse und Programmbudget: Entscheidung und Planung.
Tübingen 1970

[193] Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education & Welfare. July 1973.
Washington: U.S. Government Printing Office, DHEW Publication No. (OS) 73-97, 1973, XXXV, 346 pp.

[194] Renninger, Clark R. (Ed.):
Approaches to Privacy and Security in Computer Systems. Proceedings of a Conference Held at the National Bureau of Standards, March 4-5, 1974. NBS Special Publication 404. Washington: U.S. Department of Commerce, National Bureau of Standards, September 1974, 72 pp.

[195] Renninger, Clark R.; Branstad, Dennis K. (Ed.):
Government Looks at Privacy and Security in Computer Systems. A Summary of a Conference Held at the National Bureau of Standards, Gaithersburg, Ma., November 19-20, 1973. NBS Technical Note 809. Washington: U.S. Department of Commerce, National Bureau of Standard, February 1974, VII, 37 pp.

[196] Rihaczek, Karl:
Angemessene Datensicherung.
In: Datenschutz und Datensicherung (1977) H.1 S.39-41

[197] Risch, Roland:
Die Überwachung der ordnungsgemässen Anwendung von DV-Programmen.
In: Datenschutz-Berater (1978) H.12 S.199-204

[198] Rödl, Helmut:
BDSG: Auswirkungen auf Handelsauskunfteien.
In: Datenschutzkongreß '79, Berlin, 11.-13. Juni 1979. Dokumentation, III/3, 1979, 11 S.

[199] Sabirowsky, Klaus:
Was der Datenschutz kosten wird.
In: Frankfurter Allgemeine Zeitung, 30.7.1977

[200] Samet, P.A.:
Notes for a discussion on security.
In: Proceedings SEAS Anniversary Meeting 1976, Berlin, pp. 297-299

[201] Schneider, Jochen:
Notwendigkeit, Nutzen und Wirtschaftlichkeit von Datensicherungsmaßnahmen im Rahmen rechtlicher Gestaltung des Datenschutzes. Referat auf dem Internationalen Kongreß für Datenverarbeitung, Berlin 1976a. (Manuskript)

[202] Schneider, Jochen:
Thesen zum Workshop B 1 (Notwendigkeit, Nutzen und Wirtschaftlichkeit von Datensicherungsmaßnahmen im Rahmen rechtlicher Gestaltung des Datenschutzes). Thesenpapier. Internationaler Kongreß für Datenverarbeitung. Berlin 1976b. (Manuskript)

[203] Schomerus, Rudolf:
Datenschutz im grenzüberschreitenden Datenverkehr.
In: Gesellschaft für Datenschutz und Datensicherung (Hg.): Datenschutzfachtagung DAFTA '77. 22.-23.11.1977, Köln 1978, S.69-80

[204] Schwappach, Jürgen:
Internationale Datenflüsse im Bereich der Industrie.
In: Datenschutz und Datensicherung (1978) H.1 S.21-24

[205] Seidel, Ulrich; Bechmann, Ulrich:
Der Datenschutz aus der Sicht des Anwenders.
In: Öffentliche Verwaltung und Datenverarbeitung (1975) H.8 S.369-373

[206] Sieghart, Paul:
Privacy and Computers.
London: Latimer New Dimensions, 1976, VIII, 228 pp.

[207] Simitis, Spiros:
Bundesdatenschutzgesetz: Ende der Diskussion oder Neubeginn.
In: Neue Juristische Wochenschrift 30(1977) H.17 S.729-737

[208] Singer, P.:
Maßnahmen zur BDSG. Sicherheit und Ordnungsmäßigkeit in einer Bank.
In: Datenschutz und Datensicherung (1978a) H.3 S.151-156

[209] Singer, Peter:
Die Organisation des Datenschutzes in einer Bank.
In: Datenschutz und Datensicherung (1978b) H.1 S.39-44

[210] Society for Worldwide Interbank Financial Telecommunication:
Responsibility and Liability.
SWIFT Special Newsletter, Brussels, April 1979, 4 pp.

[211] Spafford, John L.:
Statement by John L. Spafford, President of Associated Credit Bureaus, Inc., Houston, Texas, before the Privacy Protection Study Commission.
Washington, August 4, 1976, 59 pp.

[212] Spiegel:
Datenschutz: Wie Schweizer Käse.
In: Spiegel, 20.8.1979, S. 52

[213] Stadler, Norbert:
Datensicherung durch Organisation: Voraussetzung des Datenschutzes.
Freiburg 1975

[214] Subcommittee on Consumer Credit:
Fair Credit Reporting Act 1973: Hearings before the Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs, United States Senate. October 1, 2, 3, 4 and 5 1973.
Washington 1973
U.S. Government Printing Office , VI 993 pp.

[215] Süddeutsche Zeitung:
Datenschutzgesetz wird zum Kostenfaktor.
In: Süddeutsche Zeitung, Nr. 65,
19.-20.3.1977, S. 36

[216] Sugden, Robert; Williams, Alan:
The Principles of Practical Cost-Benefit Analysis.
Oxford: Oxford University Press, 1978, XII, 275 pp.

[217] Taylor, F.E.:
The protection of confidential computerised information using cost-effective countermeasures.
In: Proceedings of the European Computing Congress 1974. Uxbrigde 1974, pp.1007-1022

[218] Treasury, Board:
Preliminary Assessment of the Implementation of Part IV of the Canadian Human Rights Act: An Overview.
Ottawa, December 1978, 30 pp.

[219] Turn, Rein:
Privacy Transformations for Databank Systems.
In: AFIPS Conference Proceedings, June 4-8, 1973, Vol. 42, 1973, pp. 589-601

[220] Turn, Rein:
Toward Data Security Engineering.
Santa Monica, California: Rand Corporation, January 1974a, 25 pp.

[221] Turn, Rein:
Privacy and Security in Personal Information Databank Systems. Prepared for the National Science Foundation.
Santa Monica: Rand Corporation, March 1974b, XVII, 104 pp.

[222] Turn, Rein:
Security Problems in Computer Communication Systems.
In: Computer Communication Review 5(1975a) H.1 S.35-44

[223] Turn, Rein:
Cost Implications of Privacy Protection in Databank Systems.
In: Database, Journal of ACM September 1975b, pp. 3-9

[224] Turn, Rein:
Data Security: Costs and Constraints.
In: Policy Issues in Data Protection and Privacy: Concepts and Perspectives.
Proceedings OECD Seminar, 24-26 June 1974.
OECD Informatics Studies No. 10, 1976a, pp. 243-265

[225] Turn, Rein:
Classification of Personal Information for Privacy Protection Purpose.
In: AFIPS Conference Proceedings, Vol. 45, National Computer Conference, New York, June 7-10, 1976b, pp. 301-307

[226] Turn, Rein:
Implementation of Privacy Protection Requirements.
In: Information Processing 77, (Proceedings of IFIP Congress 77, Toronto, August 8-12, 1977), Amsterdam, etc., 1977, pp.957-962

[227] Turn, Rein:
Implementation of Privacy and Security Requirements in Transnational Data Processing Systems.
In: Transnational Data Regulation, Confer. Proceedings, Brussels, Febr. 1978. Uxbridge: Online Conferences Ltd., 1978,pp.113-132

[228] Turn, Rein:
Privacy-Protection Costs in Record-Keeping Systems.
In: Information Privacy Vol. 1(1979) No.7 pp.298-302

[229] Turn, Rein; Shapiro, Norman Z.:
Privacy and Security in Databank Systems: Measures of Effectiveness, Costs, and Protector-Intruder Interactions.
In: AFIPS Conference Proceedings December 5-7, 1972, Vol. 41 Part I, 1972, pp. 435-444

[230] Turn, Rein; Shapiro, Norman Z.; Juncosa, Mario L.:
Privacy and Security in Centralized vs. Decentralized Databank Systems.
Santa Monica, California: The Rand Corporation, 1976, pp. 17-29

[231] U.S. Department of Commerce, National Bureau of Standards:
Guidelines for Automatic Data Processing Physical Security and Risk Management.
Federal Information Processing Standards Publication No. 31, June 1974, 92 pp.

[232] U.S. Senate, Committee on Government Operations:
Privacy and Protection of Personal Information in Europe: Privacy Developments in Europe and Their Implications for United States Policy.
March 1975, U.S. Government Printing Office Washington, 1975, VII 436 pp.

[233] Verband Deutscher Rechenzentren:
Datenschutz-Kompass '78.
Hannover: VDRZ, 2. Auflage, 1978, 113 S.

[234] Verfassungsausschuß:
Bericht des Verfassungsausschusses über die Regierungsvorlage: Bundesgesetz über den Schutz personenbezogener Daten.
1024 der Beilagen zu den stenographischen Protokollen des Nationalrates XIV. GP, Wien, 5.10.1978, 22 pp.

[235] Vinge, P. G.:
Experiences of the Swedish Data Act.
Stockholm, Federation of the Swedish Industries, 1975, 64 pp.

[236] Voss, Heinz-Rudolf:
BDSG-Auswirkungen auf Kreditsicherungs-organisationen.
In: Datenschutzkongreß '79, Berlin, 11.-13. Juni 1979. Dokumentation, III/4, 1979, 17 S.

[237] Ware, Willis H.:
Handling Personal Data.
In: Datamation Vol. 23(1977) No.10 pp.83-87

[238] Weihe; Blesgen:
Kostenmässige Auswirkung des Bundesdatenschutzgesetzes für die Wirtschaft.
In: Der Betrieb (1977) S.433

[239] Westin, Alan F.:
Good marks but some areas of doubt.
In: Business Week, May 14, 1979, pp. 14-16

[240] Westman, Gustaf Adolf:
Computers, Privacy and Legislation in Sweden.
In: Information Gate Keepers (Ed.): TDF '78: Conference on Transnational Data Flows, Washington, May 16-18, 1978, 6 pp.

[241] Whieldon, David:
How much will "Privacy" cost?.
In: Computer Decisions, August 1979, pp. 54-62

[242] Wilson, John H.:
Costs, Budgeting, and Economics of Information Processing.
In: Annual Review of Information Science and Technology, Vol. 7, 1972, pp. 39-67

[243] Wirtschaftswoche:
Datenschutz: Krach um ISA.
In: Wirtschaftswoche (1979) H.31 S.16-20

[244] Wirtschaftswoche:
Datenschutzgesetz: Vorsicht, der Computer hört mit.
In: Wirtschaftswoche (1976) H.9 S.12-17

[245] Wissmann, Karl-Heinz:
Ordnungsmäßigkeit des Datenschutzes: Beurteilungsgrundsätze.
In: Datenschutz und Datensicherung (1977) H.1 S.30-34

[246] Wissmann, Karl-Heinz:
Die Kosten des Datenschutzes und Grundsätze ordnungsmäßigen Datenschutzes (GoDS).
In: Datenschutz und Datensicherung (1978) H.2 S.81-85

[247] Wong, Kenneth K.:
Risk Analysis and Control.
Manchester: National Computing Centre Ltd. 1977a, VIII, 144 pp.

[248] Wong, Kenneth K.:
A new approach for risk analysis and control: The UK experience.
In: Bruce Gilchrist (Ed.): Information Processing 1977. Proceedings of IFIP Congress '77. Toronto, Aug. 8-12, 1977. Amsterdam 1977b, pp. 905-910

[249] Woodward, Franklin G.; Hoffmann, Lance J.:
Worst-Case Costs for Dynamic Data Element Security Decisions.
In: Proceedings of the Annual Conference of the ACM, November 1974, San Diego, Vol. II, pp. 380-753

[250] Wronka, Georg:
Beeinträchtigt Datenschutz die Werbung? Das Bundesdatenschutzgesetz und seine Auswirkungen auf die Direktwerbung.
In: Direkt-Marketing, 1977, Nr. 5

[251] Zientara, Marguerite:
Harris Poll Finds: Most Americans Feel DP Threatens Privacy.
In: Computerworld June 11, 1979, p. 35

[252] Zimmermann, Dieter:
Ist die Protokollierung nach dem EBDSG für den Datenschutz notwendig und geeignet?.
In: Öffentliche Verwaltung und Datenverarbeitung (1975) H.5 S.197-206

[253] Zimmermann, Gerhard:
Recht- und Ordnungsmäßigkeit der Datenverarbeitung. Lehrgangsunterlagen.
Gesellschaft für Mathematik und Datenverarbeitung. St. Augustin, 1976