NBS TECHNICAL NOTE 876

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

Exploring Privacy and Data Security Costs— A Summary of a Workshop

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards [1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, and the Office for Information Programs.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of a Center for Radiation Research, an Office of Measurement Services and the following divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Nuclear Sciences [2] — Applied Radiation [2] — Quantum Electronics [3] — Electromagnetics [3] — Time and Frequency [3] — Laboratory Astrophysics [3] — Cryogenics [3].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services to promote the use of available technology and to facilitate technological innovation in industry and Government; cooperates with public and private organizations leading to the development of technological standards (including mandatory safety standards), codes and methods of test; and provides technical advice and services to Government agencies upon request. The Institute consists of a Center for Building Technology and the following divisions and offices:

Engineering and Product Standards — Weights and Measures — Invention and Innovation — Product Evaluation Technology — Electronic Technology — Technical Analysis — Measurement Engineering — Structures, Materials, and Life Safety [4] — Building Environment [4] — Technical Evaluation and Application [4] — Fire Technology.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus within the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consists of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS and other agencies of the Federal Government; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.
[2] Part of the Center for Radiation Research.
[3] Located at Boulder, Colorado 80302.
[4] Part of the Center for Building Technology.

Exploring Privacy and Data Security Costs— A Summary of a Workshop

Edited by

John L. Berg

Systems and Software Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

A Report of the NBS Workshop
on Privacy and Data Security Costs
February 20, 1975
Gaithersburg, Maryland

Gary D. Bearden, Chairman

U.S. DEPARTMENT OF COMMERCE, Rogers C. B. Morton, *Secretary*

U.S. NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

Issued August 1975

Library of Congress Catalog Card Number: 75-600063

National Bureau of Standards Technical Note 876

Nat. Bur. Stand. (U.S.), Tech. Note 876, 35 pages (Aug. 1975)

CODEN: NBTNAE

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1975

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. C13.46:876). Price 85 cents. (Add 25 percent additional for other than U.S. mailing).

On February 20, 1975, nine informed EDP professionals were invited by the Systems and Software Division of the Institute for Computer Sciences and Technology to discuss the costs Federal agencies should anticipate in complying with the Privacy Act of 1974. The invitees came from Federal agencies, private industry, and academe and shared an interest in the three questions posed by the day's agenda:

1. What benefits or increased value will EDP managers or data base administrators gain from implementing privacy requirements?

2. What direct or hidden costs can be identified and what processes can be used to identify costs?

3. How should costs be allocated among those who receive privacy's benefits or face its obligations?

Working within the structure of an informal workshop under the chairmanship of Mr. Gary Bearden, U.S. Civil Service Commission, the participants engaged in an informative and lively discussion that produced a valuable interchange of ideas. The participants and their affiliations were:

Mr. Gary D. Bearden (Chairman)	*Director, Bureau of Manpower Information Systems U. S. Civil Service Commission*
Mr. Walter L. Anderson	*Associate Director, Financial and General Management Studies Division U. S. General Accounting Office*
Mr. Richard A. Eberhart	*Senior Policy Analysis Officer Domestic Business Policy Analysis Office of the Secretary U. S. Department of Commerce*
Mr. Earl P. Bassett, Jr.	*Vice President Federal Government Affairs 3M Company*
Mr. Robert Caravella	*Chief, Information System Center Federal Trade Commission*
Mr. Theodore G. Clemence	*Program Planning Officer Office of the Director Bureau of the Census*
Dr. Richard L. Nolan	*Associate Professor of Business Administration Harvard Business School*

Mr. Stan Halper	*Director of Operations, Auditing and EDP* *Coopers and Lybrand*
Mr. Larry Simonette	*Practice Director* *Data Processing and Software* *Peat, Marwick, Mitchell and Company*

The affiliations are listed for information only. The participants acted as individuals and presented their own views.

This publication summarizes the discussion at that workshop.

Editorial Philosophy

In preparing for publication a summary of a workshop such as this, the editor has a responsibility to the participants. He must present their comments clearly, accurately, and fairly. He must satisfy the participants' intent to share their experience with their colleagues. Therefore, the editor has a responsibility to present their discussion in a manner that invites reading and in a logical structure that clarifies their ideas.

At the same time an editor must recognize that the nature of a round table discussion leads to certain rhetorical devices that get lost on the way to the printed page. Speakers take positions not necessarily their own in order to act as devil's advocate. Speakers attempt to express ideas still forming in their minds and, consequently, articulate long rambling sentences that often have abrupt changes of thought in the middle and could only be understood in the context of that instant. Speakers challenge other speakers by asking questions based on assumptions the speaker may not necessarily hold. And humor often makes a point about a serious subject better than a pompous assertion would.

A topic under discussion frequently has two possible meanings and the partners to the dialogue may each use a different sense without realizing that they may have taken a position in the minds of listeners contrary to the one they intended. Correcting this misunderstanding may not take place for several minutes and result in the need for both discussants to retrace and reaffirm the declarations of their true positions.

Finally, speakers seek and deserve credit for the value of their ideas and the originality of its presentation.

We reconciled our stated editorial responsibilities with these difficulties in two ways.

First, we decided not to produce a verbatim transcript but, rather, to capture the sense of the discussion and to render spoken English into a form more suitable for the printed page. We preserved the context of each statement by making the organization of the summary follow the order of the agenda.

To increase the summary's readability, we collected and unified the discussion of different topics when they were intertwined during the discussion. We also reduced and clarified many of the statements while sticking to the speaker's intent.

Where no point was served by identifying the speaker, we simply reduced the discussion to a narrative description and identified it as such. In places where knowing the speaker's identity clarified the thought or established the speaker's position for use in understanding statements later on, we identified him. Although the editor participated in the discussion his role was to clarify other's points and to remain anonymous.

Just as many lighter comments livened the workshop itself, lighter comments are included in the summary to leaven it; particularly where they highlight the topic or assist in transitioning to another topic.

The second way we reconciled our responsibilities was to submit the summary in draft form to the participants for their verification of the accuracy of our capturing the speaker's intent.

The editor hopes that the participants accept the diligence shown in preparing their views for publication as his expression of gratitude for an enjoyable, informative, and useful session and his pleasure that each of them found the session profitable, too.

John L. Berg
Systems Architecture Section
Systems and Software Division
Institute for Computer Sciences
and Technology

TABLE OF CONTENTS

EXPLORING PRIVACY AND DATA SECURITY COSTS--A SUMMARY OF A WORKSHOP

John L. Berg, Editor

On February 20, 1975, the ICST hosted a one-day round-table discussion on the economic aspects of privacy and data security costs. The workshop was chaired by Gary Bearden, U.S. Civil Service Commission. The participants were Walter L. Anderson, General Accounting Office; Richard A. Eberhart, Office of the Secretary, Department of Commerce; Earl P. Bassett, Jr., Vice President, 3M Company; Robert Caravella, Federal Trade Commission; Theodore Clemence, Bureau of Census; Richard L. Nolan, Harvard Business School; Stan Halper, Coopers and Lybrand; and Larry Simonette, Peat, Marwick, Mitchell and Company. The group discussed the benefits EDP managers or data base administrators might gain from the privacy requirements, the processes for identifying direct or hidden costs, and processes for allocating costs.

Key words: Computer security; data security; privacy; privacy costs; security costs.

1. WELCOMING REMARKS

Mr. Seymour Jeffery, Chief, Systems and Software Division, extended a welcome from the Institute for Computer Sciences and Technology as well as his personal welcome to the workshop participants. After noting Dr. Willis Ware's recent comment that no hard data exists on privacy costs, Mr. Jeffery stressed that the question facing ICST was one of deciding what technological questions NBS should address in the area of determining privacy implementation costs. He then gave a brief overview of ICST's work in computer security and the technical areas, such as personnel identification, encryption, and physical security, in which work was currently being done. Mr. Jeffery thanked the participants for their help and introduced Mr. Gary Bearden as Chairman of the workshop.

Mr. Bearden added his personal welcome to the panel. He then reviewed the agenda and made some administrative announcements. He informed the panel that the results of the workshop would be published by NBS and that early drafts would be circulated to the panel for their comments.

Mr. Bearden explained that his interest in the costs of the Privacy Act of 1974 results from his position as Director, Bureau of Manpower Information Systems at the U.S. Civil Service Commission.

Chairman: Virtually all of the many files at CSC are personal files. Data volumes reflect the level of activity at CSC. The number of data transactions reflect the Federal Government's 3 million active workers, 2-3 million applicants each year, and 1.3 million retirees. Data processi activity levels also involve the CSC responsibility for promulgating and enforcing the personnel regulations for all personnel departments in all

agencies throughout the country, and include policy on record-keeping practices.

CSC files have been generally available to the Federal employee except for investigatory files. These were not open until the day before the workshop. On that day the new Freedom of Information Act became effective. The CSC will continue to protect the sources of confidential data, but the new requirements permit individuals to see all the data in their files. The CSC will not be under disclosure or notification provisions of the Privacy Act until September 27, 1975, when the law becomes effective.

So far, the CSC has experienced a very low rate of inquiries from data subjects about their files. In spite of publicity, CSC had received a total of 10 new requests under the Freedom of Information Act to date. In the main, the disclosure requirements will have a cost figure reflecting the "demand curve" of inquiries and this suggests that costs could be separated into capital (one time) costs and operating (recurring) costs.

2. AGENDA ITEM: PRESENTATION OF INDIVIDUAL VIEWS

The Chairman suggested moving into the first part of the agenda, the presentation of individual views. (Dr. Richard Nolan had submitted for circulation limited to the panel a draft copy of his views in an article to be printed in the Harvard Business Review. That article has since been published[1/].)

Mr. Theodore Clemence, Bureau of Census, stated that his bureau had early statutory requirements for protecting individual records. Census has two broad record systems which have accumulated over the years from surveys and censuses of both corporations and individuals. The first system consists of the archival files which have accumulated since the first census in 1790 and now number about a billion records. These, for example, are used for proof of age in order to gain social security benefits when no birth certificate is available. The second are the operating files, which number several million each year. These are used to produce the various census reports.

The Privacy Act impacted the Bureau of Census lightly since the Bureau successfully conveyed to Congress the concept that the files of personal information are treated in a statistical or research manner rather than administrative. As such, they do not directly affect individuals nor are they the source of potential individual harm. The Bureau of Census operates under specific laws (Title 13 codified in 1954) which make census records immune from legal process; even from subpoena. The Bureau of Census, however, shares with other agencies common problems such as physical security and cost/benefit analyses of privacy requirements.

1/ *Robert C. Goldstein and Richard L. Nolan, Personal Privacy versus the Corporate Computer, Harvard Business Review, March-April 1975.*

The Bureau of Census has extensive experience to share with other Federal agencies in what it calls the Contract of Trust with the public. One specific area of experience is the telling of the data subject whether the information sought is required by law or not. The BoC can't survive without public trust. The most important link in building the confidentiality chain is the morale of the agency's own troops, what he called the human equation.

Mr. Larry Simonette, Peat, Marwick, Mitchell and Company, explained that this workshop on privacy was a new wrinkle to him since his previous concern and interest was in security, integrity and the confidentiality of data but that he had observed increasing interest in the privacy aspects. Consequently, he felt that an auditor's scope must be widened to include this subject. His company's emphasis has been on corporate and financial data. He expressed a personal interest in the task of answering "What is the cost of privacy?" He concluded that the first interest should be the capital costs. The accessing of data probably will determine the operating costs but he heard with interest Bearden's comment about how few people actually applied to see their file. Mr. Simonette felt he had some opinions to contribute to the panel but that his major interests have been in the questions of security, integrity, and confidentiality.

Mr. Earl P. Bassett, Jr., Vice President for Federal Government Affairs of the 3M Company, stated that he had two motives for joining the panel. First, an understandably selfish motive in developing ideas for selling 3M products which include information systems, computer output microfilm systems, and computer driven microfilm systems. The second motivation resulted from 3M's internal concerns about complying with the laws on privacy. As a multinational corporation, 3M has had to cope with many diverse laws, for example, the Swedish privacy law. At a recent meeting convened to discuss personal files, 3M found, to their surprise, that many files on the same individual were scattered geographically throughout the company and were under the control of many different people. These files have many different aspects; investigative, counseling, evaluations, etc. This problem is aggravated by the many different nationalities employed by 3M. 3M makes a point of employing individuals from the country in which the plant is located and must follow the laws and practices of the host country. Under the new trade bill, 3M will be branching into eastern bloc countries and lesser-developed nations and will follow their policy of hiring people locally. This will undoubtedly compound the problems of privacy with the necessary existence of widespread business files and ordinary business communications. One specific problem that has been suggested is a possible abuse of the Privacy Act provision permitting the worker to see his file. Abuse of this right may result in excessive lost production time. A ramification of the provision which allows the data subject to be accompanied by a representative may be that his union will require his permission to share access to the man's file. Another specific problem is the constraints on the transfer of personnel files as the individual himself is transferred geographically. The question was raised as to whether Mr. Bassett felt that privacy legislation affecting the private sector would come first

from the Federal or local government level. Mr. Bassett pointed out that 3M was already under privacy laws in some states.

Mr. Richard A. Eberhart, Domestic Business Policy Analyst with the Office of the Secretary of Commerce, stated that his office provided general guidance on the impact of policy decisions and statutes on business. Currently, they are investigating the manner in which selected private industries are addressing the rights of individual privacy, whether corrective legislation is necessary, and the cost impact on industry of such legislation. Their information gathering vehicle will be a questionnaire, now in its early stages, which will provide the base for projecting privacy impacts out to private industry. They will watch the cost to industry of any new law, particularly in view of our essentially inflationary times.

The Chairman noted for the information of the workshop members not from Federal agencies that a new requirement was forthcoming. Soon, economic impact statements will be required for new legislation or executive orders; particularly, if the impact is inflationary.

Mr. Robert Caravella, Federal Trade Commission, stated that he had project responsibility for the State of Illinois Project SAFE (Secure Automated Facilities Environment) which was a multi-discipline approach to the problem of protecting computer systems. SAFE involved technical, costs, training and, with the production in cooperation with NASIS of model legislation, even legal aspects. Currently, he is with the Federal Trade Commission where he is responsible for protecting the Commission's sensitive corporate information. The Commission has few personal files.

Mr. Caravella identified one of his major concerns as developing a logical outline of data security and privacy costs. He saw multiple options for subdividing the outline, for example, security versus privacy, levels of security, direct versus indirect costs. He expressed a hope that the workshop might be able to produce an outline of such a cost structure.

Mr. Stan Halper, Coopers and Lybrand, stated his major concern was the audit objective and was directed mainly to security of corporate data. He indicated his personal interests in design of data bases as it affects privacy (again, corporate not personal) and encryption. He has worked on assessing the costs of these features, particularly in the area of the Federal Credit Bureau Reporting Act, a forerunner of privacy legislation. He associated himself with Caravella's hope to construct a general outline of costs.

Dr. Richard Nolan, Harvard Business School, stated that Harvard had mounted an intensive research program six years ago in computer based systems. Three years ago, the decision that privacy issues should have a high priority resulted in a research project that culminated in a dissertation by Dr. Robert Goldstein, entitled "Cost of Privacy." The work represents an approach to estimating privacy costs through a computer model. The model was applied to certain industries and public

agencies for key applications. Dr. Nolan stated that their goal was to provide research guidance to the private and public sectors. In response to a question Dr. Nolan said that a working copy of a paper to appear in the March issue of the Harvard Business Review had been circulated to the panel. The research was sponsored by Honeywell Information Systems, Inc. and the Goldstein thesis will be published by them. Copies of the thesis are available from Harvard Business School and will be available from Honeywell.

Mr. Walter Anderson, General Accounting Office, described GAO's general responsibilities as being in auditing, but widened that to include financial accountability, management accountability, and program results. Mr. Anderson's responsibilities include Automatic Data Processing. He pointed to several topics as examples of their output. These included computer output to microfilm, standard codes and elements, efficiency in software documentation, comparison of Federal and private physical security, study of privacy cost impact, application of minicomputers, programming productivity, and software conversion.

Since GAO has responsibilities in auditing Government computer system procurement, GAO would like to have a standard accounting system that permits it to see where privacy was increasing costs. However, present standardization progress does not permit this. Consequently, the suggestion of outlining the privacy and security costs struck Mr. Anderson as good.

GAO's major concern is to identify accurately privacy costs and to avoid having other extraneous things thrown in under the privacy cost umbrella.

3. AGENDA DISCUSSION ITEM: WHAT BENEFITS OR INCREASED VALUE WILL EDP MANAGERS OR DATA BASE ADMINISTRATORS GAIN FROM IMPLEMENTING PRIVACY REQUIREMENTS?

Chairman: It seems that many of us on the panel have concerns about the cost involved with the implementing of the privacy legislation, but the first agenda item addresses the benefits resulting from implementing the Act. So I ask you to adjust your thinking for the moment to consider how agencies and, potentially, private industry gain from implementing the Act.

Now, I see the first benefit as the increased visibility computer data systems will have. Prior to the Act, each agency head had sole discretion on what systems would be implemented. Much redundancy undoubtedly has resulted from this lack of a single, central control of systems proliferation. With the new law, agencies must notify the Office of Management and Budget, Congress, and the public through published announcements of new or augmented computer data systems. Now, computer data systems proposals will get not only the desirable Governmental scrutiny, but even a new data element will get public scrutiny as well since the base concept of the privacy law is that there shall be no secret personal files.

Further, the public and Governmental bodies will have done three things. They will have prepared written descriptions of the proposed system's statutory basis. They will have determined whether the data being collected is mandatory or voluntary. They will have defined the actions to which the respondent is subject if he doesn't comply with either voluntary or mandatory requests.

All of these factors may well produce a significant benefit of reducing the costs associated with the oft mentioned mushrooming computer data systems.

Panel: That benefit is a by-product.

Chairman: Yes, a by-product of the Act but nonetheless a benefit.

Discussion: The question arose as to whether one could claim as a benefit being forced to do what one should have done before. The panel seemed to agree that many of the requirements in the privacy law were practices that were merely good information management practices. Savings resulted from reducing two areas: first, redundant data items and, second, unnecessary data items eliminated as a result of data subject complaint.

However, there is some benefit to the additional privacy provided by current inefficiencies. Some five or six years ago, people proposed the idea of eliminating inefficiencies by centralizing all Government data into one data bank but the idea generated so much public hostility that the idea had to be dropped. That suggests the basic point: the cost of providing privacy will be inversely proportional to the public's sense of agency fairness. Clearly, there would be no Privacy Act if the public had no uneasiness about Government data. And there would be no burden of new capital costs to shore up defects in present systems if proper practices had been previously followed. Further, the operating costs of educating the public about agency files will go down as public confidence in an agency's fairness increases.

Caravella: I believe four points can be made.

First, the benefits of reducing duplications apply to data as well as to entire systems. Many agencies seem to collect as much data as they can and worry later about the use of the data.

Second, in the State of Illinois, certain economies of scale were a benefit of centralization and the thrust was for centralization all along. But the criminal justice agencies were inhibited from centralization by the haziness of ground rules. Once concrete ground rules, as in the Privacy Act, were provided and there was no specific prohibition, those systems could go forward. For example, the State of Illinois developed a large, centralized data system. It contained primarily health and welfare records. Revenue and criminal justice agencies would not consolidate to that center for fear that the privacy of its data would not be protected in the centralized system. With the privacy law protecting the data, the centralization may now go forward.

Question: What reason for avoiding centralization will they come up with next?

Caravella: Probably that the manufacturer has not provided sufficiently secure software. But that leads to the third point.

Third, the manufacturers of computer and information systems have been reluctant to invest in the design and construction of security software and hardware. Now the Privacy Act gives requirements which may justify the necessary capitalization to provide the security features.

Panel: It also gives them an additional marketing argument. We have seen a lot of privacy companies jumping up in the last few months that used to be software or security companies.

Caravella: Fourth, the law will encourage the gathering of only necessary data with a consequent savings.

Question: The Privacy Act requires the collection to the extent possible of data directly from the data subject. Will that benefit the agency by increasing the public's image of the agency's data integrity and validity?

Panel: In other words, if an agency seeks credit information it should, to the extent possible, get that information from the data-subject and not from a credit bureau. Will that benefit the agency with respect to the integrity, reliability, validity and acceptability of the data by the public? That's probably a benefit to the public. Remember the individual has a parochial interest in that data. What checks and control do you have on the data he's giving you?

Halper: The Privacy Act has benefits and detriments. A particular concern is the impact it will have on the currently general trend towards a large centralized common shared data base. To some extent, the more constraints placed on the collection of data, the more overhead costs will increase and the more the drive will be towards centralizing these collection functions. But there is a distributive effect, too, in the desire to get the information back to the field. It appears that privacy considerations will be most felt there and become a major overhead cost. This might lead to the decision <u>not</u> to centralize and to lose the cost savings implicit in centralization. Some experience has been developed on this subject as a result of implementing the credit reporting legislation. A decision had to be made whether (a) to perform the processing (data validation) in a central location for the client credit bureaus, or (b) have each client do all of the processing and feed final data into the central data base. A choice for the whole industry, at that time, was not made. But the newspapers indicate a lack of confidence in some of the local credit bureau data bases and the high costs associated with them.

Question: Did particular regulations drive these cost requirements?

Halper: Yes, the credit law allows an individual to ask for all the ata on him. However, the data flow is to the local credit bureau from a central office which has received data from many different local credit bureaus. So the data was being updated through several possible points. The central agency set up good standards to control, as required, this updating but the standards would have increased the local credit bureau's costs two to three times.

Question: How does that process work?

Halper: Suppose you had made purchases in Pittsburgh and Duluth. Your transactions would reach both local credit bureaus who would update their files (whether manual or computer). The two may decide to centralize your file in one of the two places, but both should be handling your file in a consistent fashion. This requires standards for processing updates. Networks of data systems will have great difficulty implementing the Privacy Act without good standards. This standards process will be very expensive. This also raises the question of enforcing the standard and the cost of enforcing those standards.

A central force may dictate and force standards; it may even be able to afford the costs. But if independents also reside on the network, the costs involved will decide for them whether they will do the centralization standards. The other side of the coin would be that the central office would have to adopt the node's standards or procedures. Adopting incrementally all of the local standards by the central office will produce a very cumbersome system with very high overhead costs. The system may even become untenable.

Question: But when you have a law that sets liabilities on the holders of data that is not accurate, timely, relevant or has incomplete compliance with the requirements for disclosure accounting, don't you have the beginning of standards?

Halper: Yes, but how do you choose the level of that standard versus the cost of implementing that standard to the most common denominator? The benefit, then, is setting the common basis for standards to satisfy privacy.

Question: Will the Act help the EDP manager justify to his management the costs of doing more of what one could label as good information practices?

Panel: Some panel members doubted the success of this approach. The costs have to be justified on the basis of the data base effectiveness and one can assume that the quality of the data base had been commensurate with the managerially set and paid-for goals. If the impact is on the EDP manager and not his management, then such an approach doesn't offer much hope. However, it may accelerate data consolidation or improvements already underway.

Others felt that they had used the suggested argument on upper management to justify the spending of resources for analyzing the whole data flow in order to determine what privacy and security problems existed.

The EDP manager is the one most concerned and probably most responsibl for the existing state of security and privacy. Though he may not yet see it, a benefit exists in this necessity to review his entire processing flow with respect to its privacy controls.

Fear of direct personal liability or a refined sense of corporate responsibility under the law will result in new consideration of EDP controls.

In dividing the discussion into direct and indirect economic benefits, some panel members saw no direct economic benefits flowing from the Privacy Act. There are many indirect economic benefits and direct social or corporate benefits, but no direct economic benefits. EDP managers have acted as czars, and the Privacy Act will give them another sword to stifle applications they find inconvenient. Actually, the ultimate users should be the determiners of what uses the computerized information should be put to. But the tendency is for the user to become more sophisticated in seeing through such double talk.

It was not so clear to others that the EDP manager is such a czar. In some shops the user presents his case for a computer application to executive management who makes the decision; not the EDP managers. Some felt that while that may be the desired system, in fact it often wasn't.

Chairman: Taking as an argument point that there were no direct economic benefits, can the panel support that assertion?

Panel: Looking at the problem from the other standpoint, one of the purposes of the Act was to increase the integrity, validity, reliability and accuracy of personal data. If the Act does not fail, if it achieves that purpose, it also increases the value of the data base. But, that benefit is independent of privacy. Congress could have simply legislated increased integrity and that would have improved the data base. Congress could use similar punitive damage measures to improve data.

Chairman: Many things could be paraded under the title of privacy but a basic concept is that the Act may be a step towards defining propert rights to personal information. However one defines privacy, many things are connected by appearing together in the Act which we can call "privacy" without regard to proving they have a connection. We now do have a Privacy Act. Whatever benefits accrue to the collection of concepts connected under the Privacy Act (and, therefore, called "privacy") should be listed. What direct economic benefits can be assigned to this bill? The Privacy Study Commission can be expected to ask what benefits and wha costs. Agencies have to report annually the costs of privacy. Can we report to the Congress and the American people the benefits of the la

Nolan: The Act will be an immediate spur to introduce good information management practices if EDP centers have not done so already. So there is a one-time benefit. However, when the system is completed and running, there is a recurring operating overhead cost associated with privacy. This produces a direct social benefit but it produces no economic benefit. This overhead cost has to be applied to an intangible (albeit justified) social benefit and not a direct economic benefit to the paying company.

Basically, privacy is an encumbrance on the use of information. The problems of redundancy will eventually and inexorably be addressed with data base technology and standards even without the Privacy Act.

Bassett: Before leaving the subject of the one-time benefit, one should not lightly lump redundancy only under that one-time benefit. In a major company, planning is projected in five year plans. If redundancy exists and is allowed to remain, that cost is reflected in every one of the five years. Removing that redundancy means a savings over every year that the duplication might have existed.

Discussion: The proper name for the recurring benefit is cost avoidance rather than cost savings.

Question: Are we limiting the definition of a "direct economic benefit" so narrowly as to include only revenue, e.g. a fee charged for providing privacy information?

Panel: The panel generally agreed that the potential of revenue was very small, undoubtedly less than any costs. Further, the Privacy Act set certain limitations on the fees an agency may charge. For example, the current Act allows charging fees for copying records but not for the actual search for records.

Question: Should "direct economic benefit" be understood to mean only cost savings or cost avoidance?

Panel: The panel attempted to define "cost avoidance" and whether the discussion was limited to the current Privacy Act. The chairman suggested planning a major emphasis on the Privacy Act but allowing a reasonable extrapolation of the law into the private sector. The private sector now has the advantage of avoiding a "crash" cleaning up of their data files by anticipating that the law will eventually be extended to include them. However, industry knows generally their condition, now, and purely economic reasons are causing them to review their EDP practices. In a sense, the Privacy Act provides an economic benefit to private industry in that it buys time for more efficient and planned adoption of the privacy requirements.

A collection of good cost figures from actual operating cost in terms of capital costs and operating costs would prove very useful in assisting the development of future privacy laws.

Clemence: The individual subject of the data system has some refuge in the redundancies and omissions of current systems. Allowing the system accessor to use his judgment about the accuracy and relevance of the data coming from that system gives a desirable human control to the system. However, when all data is accurate or has a high confidence of accuracy, that refuge of personal judgment is gone.

Discussion: But the accuracy of the data has major impact on the privacy question. The wholesale upgrading of data integrity must have a direct economic benefit. The subject must have less concern if the data is accurate. Corporate data in use for decision-making must be accurate and that's an understandable economic value. The panel needs a good definition of direct and indirect economic benefits.

The example of a data subject asking to review the data about himself provided the opportunity to identify the cost of giving him a copy of his record. That cost might be allocated to the data validation function. Clearly, the increase in the validity of the subject's data has a direct economic benefit and may justify the data validation costs. However, the point was made that the cost of correct data should be "up front" and not assessed at the time a respondent corrects his own record.

Chairman: Does a direct economic benefit result from the increased validity, timeliness and relevance of data used in decision-making?

Nolan: It's difficult to associate that benefit with privacy. What the Privacy Act does is encumber the use of information. We're constraining the use of information. That has to be an overhead cost. That cost is borne by us because it is socially responsible to do so. Now, we seem to be justifying that expense by pointing to actions that should have been done all along. We seem to be listing by-products to help sell the legislation. We could probably list many direct benefits that would not have been done or would not have been done as quickly had there been no law and this could be used to argue that the law costs less than we thought because we have more benefits than just the social one intended: to protect privacy.

Question: Can a company president point to more than just the social benefits of complying with any future privacy legislation?

Nolan: Probably not many. Certainly many companies are now deciding to comply for purely economic reasons. The passage of the Privacy Act, on the other hand, is saying that that process is not moving fast enough. The legislature helps move that process along by passing laws that force us to pay the necessary costs. There are no direct economic benefits, only an overhead cost. But we've accepted that overhead cost as justified for social reasons.

Chairman: But won't that overhead cost have been there all along if we had been doing this thing right from the outset? How can we now claim that as a privacy cost?

Caravella: Why is it so important to breakout the benefits into direct and indirect?

Panel: Well, theoretically, direct benefits are more concrete and easily measurable. But that doesn't seem to be the case here.

Caravella: We can't even seem to agree on what is indirect or direct so why bother to separate them? We may be hung up on seeking economic benefits. The Privacy Act legislates social values and the economic benefits are no more than those for, say, food stamps. You don't say food stamps put a certain amount back in the GNP, but you still consider its social value. I think more important than the economic value is the perception the public has of the record keepers and their fairness. Census has a nice reputation of keeping private your information from others who requested your data. That has given people much more confidence in giving data to Census. Census knows that the economic value lies in the aggregated data which also provides privacy protection.

Question: Couldn't one argue that the Census has a more valuable data base because of its reputation for confidentiality?

Panel: Yes, but Census didn't have direct legislation that hammered Census over the head to provide that reputation. On the other hand, Census did have legislation that helped it protect that privacy.

Question: Can the panel learn anything by comparing the privacy legislation and its ramification to the environmental laws?

Bassett: I'm reminded of the taconite mining operation up in Minnesota which is dumping tailings into Lake Superior at the rate of some several hundred million tons per year. The environmentalists said that dumping was filling up Lake Superior. The mill employed 15,000 people. The latest ruling of the judge was that the mill had to install on-land disposal systems. The net worth of the facility was, I believe, $175,000,000 and the cost of the disposal was going to be $355,000,000. The facility would also have to be closed down for three years to install the new system. That means 15,000 people are going to be out of work. There is no question whether they should do it--the law says they will. Now there's fear, fear in the mind of the employee, fear in the mind of the company. But the company may decide simply to shut down the plant. That judicial decision was made in spite of the recognized economic impact.

Nolan: But that has two sides. True, there may be a net depression in that area over the next fifty years but no one is doing studies to see, say, how the fishing industry is going to grow each year. That kind of speculating gets you more and more into never-never land. We shouldn't fall into that trap.

Panel: You may want to say, "Mr. Congressman, privacy requirements are going to cost you millions of dollars for system encryption, data usage priorities, and levels of sensitivity." Those are the direct benefits of spending the money.

Nolan: There's some slippery stuff here, too, on the subject of distributive systems. A whole industry of mini-computer manufacturers is working aggressively on the basis of providing a network of mini-computers dispersed geographically. Now you're telling them that there are new rules. This may have a serious economic impact on them.

Halper: Consider also the question of packet transmission. How does one make up packets? Can they be mixtures of sensitive and unsensitive messages? Can two independent users of a common carrier mix their messages whatever their sensitivity? Does this imply levels of sensitivity? Can two unsensitive packets become sensitive if transmitted together? This raises the whole question of encryption overhead costs. The industry is just beginning to understand this.

Chairman: In a brief summary, the panel finds no quantifiable, direct economic benefits to the privacy legislation but there are indirect economic benefits and social benefits. The social benefits are, of course, the direct benefits intended by the privacy legislation.

Discussion: The poorer provider of credit information will eventually be driven out of business by purely economic forces.

However, the law will strengthen the impetus towards improving information management practices and better system structuring. It simply is an additional spur, but the impetus couldn't be measured.

Nolan: TRW's credit bureau implemented the Richardson report and their cost per transaction increased $2.00 (from $1.50 to 3.50). They were more socially responsible but, at that rate, they would be out of business in a few months.

Panel: No one else implemented those rules?

Nolan: No.

Panel: Then the legislation now puts them on fairer economic footing.

Nolan: The purpose of the legislation and its direct benefit is the providing of privacy. You don't pass privacy laws to encourage documentation or to develop standards.

Halper: For example, IRS rule 71-20 says that machine-readable records can also be accepted as records. That law includes a set of standards to assist the IRS auditor in finding information but the standards are simply what any good EDP shop would be doing. The taxpayer gets no direct benefit. The benefit goes to the IRS. That's why the law was passed. Some shops got an indirect benefit in that they were shaken up for the good due to documentation requirements. But the direct benefit was to make IRS's job easier.

Question: Are the economic benefits to the data-subject?

Discussion: Well, for example, more valid data may permit a data subject to get a loan where previously he couldn't. That's a direct economic benefit. The 1970 Fair Credit Act may have anticipated that kind of damage. However, the Privacy Act doesn't appear to have direct benefits. The law was drawn to prevent the loss of benefits through bad data and to provide the means for seeking redress.

Clemence: One always has the problem of deciding when to challenge the use of information. Again, the costs reflect the perception people have of the use of the information. For example, how many times have you been asked at checkout stands to corroborate your credit card with other information like your social security number or your drivers license. Now most people give that information freely because they see the benefit to themselves as greater than the possible abuse by the requestor. People are afraid of the universal identifier yet the average person is carrying around 17 numbers. Consider the inefficiency of that.

Question: With the provisions of the Privacy Act now in effect and the protection it gives by informing the public, will the public reduce its resistance to the building of large data bases, the centralization of computer systems, networking, and information sharing? The public now has assurances of knowing the usage of information being collected and can challenge it. I'm thinking of information as a property which has value and its aggregate use has great economic value. For example, as our resources become increasingly scarce, we'll need more planning and, therefore, better information. This may become more critical in the 80's than even the 70's. Will the truth in information laws allow us to seek the economic benefits of integrated systems without the resistance earlier given say, the national data bank of the 60's with the public's fear of abuse and the dossier society? Will they see the advantage of the potential long-range planning?

The panel held mixed views. Some felt that even if most of the requirements discussed were met, the public would still view such a centralization as a consolidation of power into one hand instead of many hands. There's protection in the pluralism of inefficient systems. Centralization could result in the protection of privacy by lumping individual information into statistical aggregates. It could also damage privacy by collecting units of public information into a dossier. Others felt that the law and the passage of time would remove the mystique of the data collecting as more citizens see the published notices of the data collections, see their uses, and develop a sense of controlling them.

Access to a single central file will give data subjects a sense of confidence that they know what the user of the data knows and can correct it. However, centralization could also connect previously unrelated information to deny the data subject previously obtainable benefits.

A major reason for the public's lack of confidence in the Government's ability to limit abuse of a central data base was the lack of technology to lend credence to any promise of protection for abuse. Will that technology be here in the next ten years that the law is in operation?

Certainly we have the opportunity to educate the public in the benefits of centralization and the fairness of the systems.

In terms of public fears, it seems that increased technology increases potential privacy abuses. The increased technology of transmitting data over communication lines or in computer networks risks new abuses though encryption may alleviate the potential harm.

Chairman: Still the question remains: will the Freedom of Information Act (which became effective February 19, 1975 and opened long shut investigatory files) and the Privacy Act assist in quieting fears about centralization by permitting the public to see what's in its file and to challenge it?

Panel: The Buckley Amendment which opened school files actually seems to have had the effect of leading to the purging of many files. Still, it does render the decisions of agency heads (particularly those that appear to involve subjective moral judgments) open to scrutiny. When a physician makes judgments that enter personnel files and, therefore, become public information, he must be more alert to his responsibilities under the doctor-patient relationship of confidentiality.

A recent privacy newsletter revealed that all medical insurance claims go to a central data base where they are open to other medical insurance companies and even to credit companies. This underscores the point that business needs data bases, particularly the insurance business. Business could not exist without them. The data bases are used for decision-making and the need for planning is increasing.

Question: Will the present laws affect today's fragmentation of data bases at all?

Panel: In the private sector, the economic benefits of centralization will determine the end of fragmentation. For example, the centralization of airline reservations into one data base is forced by the economic considerations of the cost savings compared to each airline having its own system. Insurance companies are another example.

A distinction needs to be made between the private sector and public sector. An enlightened data subject will understand that greater efficiencies in providing services will result in a lower cost of private sector services or, at least, reducing cost increases. The public, however, looks on Government as a public servant and the holder of data as public property. Its decisions about what the Government shall do is made in that light. The public has a very negative view of centralization and it will be a long time before public funds are provided for centralization. In the private sector the same negative feeling exists and it's not likely that the Privacy Act will overcome it. Centralization of data bases will require a positive push to offset this negative feeling and a period of education to enlighten the data subject could be set-back by one horror story like those we've seen.

What technology will contribute to this subject is not clear but should be significant if the last ten years is a measure. The legislation is timely in that it may spur this technology.

Question: How about the other side of the coin? Will the Privacy Act inhibit the building of data bases?

Panel: In the short run, it will inhibit data base development unless economic considerations override the inhibiting aspects. An aspect is the sharing of IRS records with other Federal agencies. The Census Bureau would have had significant cost increases if it could not get statistical data from IRS. Now two out of five businesses need not fill in Census surveys because of Census's ability to get data from IRS.

In the long run, the pressures of growing data base technology and computer networking through communication networks plus the increasing need and drive towards business efficiencies will force consideration of centralization and the privacy legislation will build the public confidence needed. This makes the law more supportive of data base progress.

Questions: Suppose the present Privacy Act were extended to treat publicly held corporate information in the same way that individual personal files are being treated. What would the impact be?

Panel: You mean if the corporation could see and challenge the data? Corporate data was originally covered in earlier versions of the Privacy Act. The question has too many ramifications to be considered here.

4. AGENDA DISCUSSION POINT: WHAT DIRECT OR HIDDEN COSTS CAN BE IDENTIFIED AND WHAT PROCESSES CAN BE USED TO IDENTIFY COSTS?

Chairman: I suspect that identifying the capital costs will be easier than identifying the recurring operating costs. The capital costs, or initial one-time cost for implementing privacy may be considered the start-up costs.

Anderson: I suggest we consider only those measures necessary to produce minimum compliance [rather than desirable or extended measures].

Chairman: With that in mind, let's consider direct capital costs first.

Halper: 5 U.S. Code §552a(e)(10), of the legislation states "Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records ..." With that as the hallmark of our discussion, I suggest we assume that the data base already exists, is complete, and has been paid for. What must then be done is to establish a system design and operating standards that meet the compliance level. That strikes me as a high cost item. Protection will have to be applied at two places; (1) to prevent data base tampering from those inside your shop, and (2) tampering from outside your shop. I see this as having four aspects:

1. Having the necessary physical and data security to limit access to only authorized internal personnel.

2. Insuring that maintenance can be performed on the system without endangering the data base.

3. Insuring that necessary update, correction, and purging functions can be performed safely.

4. Preventing outside or unauthorized tampering.

I see the major cost as "structuring" the system so that it has these protection features.

Clemence: Perhaps we should focus on existing systems and the cost of updating them rather than the design of new systems.

Discussion: Several existing systems deal with personal data but were not built with the capability of fetching up information about a specific individual. A serial search for a specific person could cost $1000. A distinction should be drawn between costs associated with increasing physical security and the cost of adding a new system capability of accessing individual data. Many Federal agencies are already improving the physical security for their own ends with resources as they become available, but adding new capabilities should be considered separately.

Chairman: The Privacy Act has three main features which, I'm sure, we'll all agree are simply good information management practice. These are:

1. Notification to the individual of the file's existence.

2. Disclosure of information to the individual and nondisclosure to others.

3. Access and control by the individual of the file content and exclusion of others.

What are the capital costs to implement these requirements?

Nolan: Perhaps it would be profitable if I describe our efforts at Harvard to analyze the costs of implementing the HEW regulations. First, we analyzed the regulations and prepared a list of discrete requirements. Then we estimated the resources necessary for each requirement. We used this to construct a model of the capital costs necessary to implement the regulations. We considered the usage regulations as the key element that influenced all the other factors. Our approach was to interpret the requirements and what we thought was a sensible implementation method. We then sought from practitioners in various fields an assessment of our interpretations and modified them appropriately. We identified these major cost components:

a. programming

b. computer processing increases

c. information storage increases

(1) off-line

(2) machine-readable

d. data communications (including mailings)

e. administration

f. capital equipment

Using this basis, we took each regulation and built a function of the resources it would require. We then went to selected Government agencies, insurance companies, credit bureaus, and a large company personnel file and collected data about the cost of each resource. This gave us the cost of the HEW privacy requirements for key applications.

Question: Did you observe the need anywhere for a complete redesign?

Nolan: Yes.

Question: Was your work limited to EDP systems?

Nolan: No. We included functions not normally associated with the EDP functions, such as postage expenses, and also manual data systems.

We found that the usage regulations were the key elements and that the others revolved around them. The second thing we found was that the requirement for notification of individuals had a major effect on costs. Just the postage could raise costs two or three magnitudes.

Halper: In data files that I have seen, there was not sufficient information retained so that implementing individual notification was practicable. The address was in the individual's personnel folder rather than on the file. Thus, two distinct sources would have to be correlated to notify the individual. The entire record would have to be redesigned to supply all the information solely from the computer source.

Nolan: In the credit bureau we investigated, the privacy conversion cost was a million dollars but the annual cost increase was twenty million dollars. However, our study indicated that with a redesign of the system, this cost increase could be significantly reduced. However, that meant turning a fairly straightforward and simple system into a more complex one.

Chairman: Did you also find that enhancing the computer system also required enchancing the supporting manual systems?

Nolan: Yes.

Halper: We found, for example, that in some systems it was cheaper to inform the individual upon every update rather than processing a special run to prepare a periodic statement of his record.

Chairman: Did you consider the cost of verifying the identity of the person requesting access to what he purports to be his record? In the CSC with 30 million records and remote offices handling mail requests, we are quite concerned about this problem.

Nolan: Perhaps the best way to answer that question is to explain that our approach forced us to make many interpretations and decisions that were arbitrary. This highlights the diversity of choices facing implementors.

Clemence: I have a concrete example of the costs of verifying the identity of the inquirer. At the Census we will give you a certified copy of your census form if you fill in the requisition form in such a way that we can be sure of your identity. That costs us about seven dollars. However, if we're not sure of your identity and have to take special steps to verify your identity, that costs us $30 to $50 which we absorb.

Chairman: At the Civil Service Commission we have considered various approaches to verifying the identity of the inquirer. We have many branch offices so we can request a personal appearance at an office. Or we may require mail requests to be notarized. But note that in selecting the method, we're deciding how much the requestor will pay to see his record.

Halper: Did the legislation consider how to identify new information being added to previous information? I mean a way to associate correctly new information with existing stored information pertinent to the same individual. For the moment I am considering the use of a password given the data-supplier to assure him that in the future only he can see the data previously supplied.

Discussion: For example, an individual may maliciously submit derogatory information about a second person by pretending to be the second person. Some "manual" or off-the-computer process must be utilized to identify individuals. Maybe agencies with many branch offices like the Social Security Administration can provide standard identification processes.

Under the Privacy Act the Federal manager has personal liability for improper disclosures. What mechanisms for personal identification must he build to be in compliance? There must be some guidelines for the certification of identity that would satisfy the judicial system that the Federal manager was in compliance with the law. Online terminals need a means to identify themselves, too. Many credit terminal operators are clerks with the power to do credit checks on virtually anyone once the terminal has identified itself to the computer. Some protection is available in that the charges for that credit check will eventually get back

to a manager who can discipline the clerk but it is, of course, too late to prevent loss of that information. A major question still remains: how to identify an inquirer seeking information from a personal data record allegedly his? Is this an oversight in the law?

The law requires that a record be kept of each non-routine disclosure of the personal record even if the disclosure is to the data subject, himself. These disclosure records must be kept for the life of the record or at least five years. This new accounting system is a major record-keeping system itself. It also represents a significant cost element but the cost is directly related to the rate at which inquiries will come in. Experience to date indicates a low inquiry rate.

Bassett: Can the costs become too high to be accepted by the taxpayer?

Chairman: The law limits the cost to the inquirer at the copying cost per page, which at CSC will probably be five cents per page.

Bassett: I meant the indirect costs to us all rather than the direct cost to the person seeking information. Couldn't the costs reach the point where they become unacceptable to taxpayers in general?

Chairman: I think the more common reaction will be to blame the familiar "Government inefficiencies."

Simonette: It may well turn out that the capital investment will be made in anticipation of large demands but the demands will actually be light. This would mean maintenance or operating costs disproportionate to the capital costs. Shouldn't the operating costs as based on anticipated demand be used to determine the expenditure of capital costs?

Discussion: The law has certain requirements. One can interpret what constitutes minimal compliance but one has to meet that minimum whatever the capital costs are. For example, the question of authenticating mailed-in requests through a notarized application form. The deterrents on the potential abuser are those associated with perjury. Some panel members felt that those were rather light. Additional protection would be offered by requiring supporting data from the inquirer, such as social security number, address, parents' names, etc. Additional protection also results from the need to give a known return address which is recorded in the disclosure record. While some suggested that the inquirer could be required to present himself to a police station to support this application, the consensus seemed to consider that excessive. Cost figures should reflect the law's obligation on agencies to establish offices where applicants can be identified and see their records. In most cases the system gains some protection by the need for the applicant to give his request to an agency staff member who actually conducts the search. This highlights the point that most disclosures are to agency personnel and constitute routine disclosures. Such disclosures are typically to certified personnel, on authorized terminals, and in secure locations. Even the instances of remote job entry will be conducted under

these conditions. The penalties associated with the fraudulent obtaining of personal information offer the major protection.

Clemence: There will be a significant first time cost associated with the wholesale revision of forms and reports. The revised forms will have to spell out to the data subject the various provisions of the law and the new protection now given the person who fills in the forms.

Discussion: Another first time cost is the identification and categorization of existing data bases, files, etc. This process may include the need to convince some people that they do have a record-keeping system that does fall under the law. The law requires publishing the existence, statutory basis, and purpose of data bases and the likelihood is that most agencies don't have sufficient documentation to do this easily. The language of the bill allows a wide interpretation as to what constitutes a "system of records" that falls under the provisions of the law. Interpretations from the Office of Management and Budget will answer many questions of interpretation. On a more technical level lie such questions as to whether a file inverted to personal references is a personal data file.

The thrust to identify record-keeping systems will produce the visibility to the systems that was long lacking.

Caravella: We at FTC have attempted to use classification levels similar to the Department of Defense and then tried to associate costs with each possible level.

Discussion: However the application of the levels to the data requires a definition of what constitutes, for example, confidential data. Others have classified all personal data at the one level: sensitive data. The rationale is simply that privacy remains a personal, subjective decision and difficult to define concretely. By using DOD's approach the kinds and levels of protection assigned to each classification becomes concrete and three cost comparisons can be made using the assumption that all data requires protection at the top secret, secret, or confidential level. This approach places some objective constraint on the decision to select a protection level.

The protection level must reflect the value of the data to a penetrator and the probability of his success. The value presumably reflects some upper bound of the cost the penetrator would accept to see personal data. For example, the typical personal data in the CSC files can probably be obtained for $15 from a credit bureau. That fee helps establish the protection level. Using the DOD classification, protection levels offer an approach that should satisfy the test of "reasonableness."

Chairman: At CSC we found no need to protect data at the top secre or secret level.

Halper: Don't the accessing requirements of the law raise the cost question of the need to automate some manual systems?

Discussion: The law itself does not require responses within a specified time so the requirement to automate is not based on time constraints. If economic reasons had caused a record-keeping system to be divided into an automated part [which is frequently accessed] and manual part [which is not] the accessing requirements of the law may now affect that division decision. It may now make more economic sense to automate all parts.

Clemence: OMB will provide the definitive answer for many of these questions and will probably fine-tune their definitions as we become more aware of the costs involved.

Discussion: In the meantime, between now and September 27th, agencies will have significant capital costs whether any data subject requests data about himself or not. Very little empirical data on costs exists. One possible source is the State of Minnesota.

In considering administrative costs, one must address questions of personnel, space, supplies, etc. Certainly this should include a review of the system design. Many systems are not designed to handle the new requirements. Even the peripherals have to be examined for their adequacy with respct to the new requirements. It will be difficult to find a data processing system that has the capability to record that a datum is disputed and to find where that statement of the dispute is stored.

Anderson: Must the dispute be recorded once in the disputed record or once for each disputed item in the record?

Discussion: The law requires appending the dispute and associated statements to the record. This has implications of storage and processing costs. Another question remains, "Need the statements of dispute be transmitted if the disputed item is not transmitted?" The statements of dispute (potentially of any size) may be stored in another file but the record has to have at least a mark per record showing the user that the other file should be seen.

Further, a record keeper must keep account of those to whom data has been disclosed so that he may retroactively inform them of any dispute. This obligation goes back to disclosures for the past two years. Note the special difficulty here because the usage records are collected sequentially as this is least expensive but have to be reordered for efficient processing of disclosure notices.

Nolan: Another requirement is the reduction of the disclosed record to the data subject in a form comprehensible to him. This may mean decoding and translating all those cryptic numbers, letters and symbols that now appear in computer records.

Discussion: The data subject must also be informed of the transfer of data to other agencies. This obligation may even apply to records stripped of all personal identifying items but transferred integrally as input to statistical data. In a general sense, virtually any transfer of data to another agency constitutes a non-routine use. There is much interchange among Federal agencies and even transfer of statistical data to state and local governments and business for purposes of understanding the makeup of the Federal work force.

The CSC delegates authority for the personnel offices located in the several agencies. The personnel folders at each agency actually belong to the CSC. The CSC defines and has oversight responsibilities for those regulations concerning personnel practices. The several agencies will conform to CSC regulations on the requirements for the folders but each agency's automated personnel system is its own responsibility.

Simonette: The sub-system to track data disclosure and usage should be amenable to a central design. Perhaps one system can be designed that many agencies could use by adding it to existing software. This amounts to a special and wholly independent system for keeping track of disclosures with the intent that all or many agencies could use the same system.

Discussion: However, this may not be as easy as it seems; for example a standard automated personnel system still eludes the Federal Government.

Question: Does an agency save any costs by simply purging or sealing existing systems?

Discussion: In many cases such a solution is prevented by law, regulation, or the agency's need for that data. If purging is possible, the costs should include the alternative (and presumably less efficient) way the agency would accomplish its mission, the cost of regaining the data in an acceptable form, and the loss of data no longer obtainable. Whether the files are considered historical, statistical, or personnel records, they probably are required by the agency's organic act.

Disclosure records must be kept for at least five years or the life of the record. This includes any contested data that is deemed so bad that the agency decides to purge the data. Even when records are passed on to the Archives (as are CSC records upon retirement of the Federal employee) the accountancy records must accompany it. The timeliness provision of the Act does not necessarily imply more forced purging than current practice since the application of that requirement is to the active records used in decision-making processes that affect individual benefits. Historical purposes may justify holding records for longer periods.

Chairman: The CSC (and SSA) found no rational constant period that it could call the purge cycle. Children of pensioners may still have active files a hundred and fifty years after the issuance of the social security number and the children of Federal employees may enter suits to

clear their parent's name of a certain personnel action. These considerations have led to maintenance of the personnel jackets in the Archives. The jackets are saved rather than being microfilmed because of legal questions related to the acceptability of microfilm by the courts.

Clemence: The Census has specific legislation that permits it to certify photocopies of Census microfilm records and these photocopies have the same utility as documents.

Discussion: The short time (270 days) to implement the Privacy Act raised questions about the feasibility of **Federal** *agencies complying in that time and about the inefficiencies inherent in that short time frame. The consensus was that the agencies will be in compliance because that was the law. However, there would be many ad hoc-eries that were inefficient and there would undoubtedly be legal challenges to clarify the interpretations of the law and to establish what was necessary for agencies to be in compliance. It may well require the hiring of hundreds of clerks and the reversion to older manual systems but the agencies will be in compliance. Perhaps a few agencies will ask for additional money or special exemptions, but in the main they will comply.*

Anderson: The GAO has a Congressional request to determine if the agencies are taking steps to comply.

Discussion: From a realistic standpoint, agencies have to be in compliance within 9 months, with no additional money, and with no time even to insert an estimate for FY 76.

Halper: To comply with the Act, you have an input problem with two parts: (a) you have to validate the data you have; (b) you have a new input front end to build in order to get the data from the data subject himself. You also have the more basic problem of knowing what data you may include in the records.

Discussion: The activity rate will determine whether the inefficient approach of using current systems will be adequate or whether the agency will have to go to a complete redesign.

Anderson: The legislation, like all legislation, had to address all data record keepers, not just the abusers.

Chairman: It was a bitter dose of medicine for all not just the sick.

Discussion: The amount of discussion and controversy preceding the legislation should have initiated some pre-planning and the existence of the Nolan-Goldstein study indicates some work was begun but, in fact, the agencies were caught off guard. Perhaps a certain amount of wishful thinking that the law would never be enacted caused the surprise. To some extent, the warning was of such a nature that concrete planning was not possible until the specifics were known.

Nolan: It was interesting that in our early work, particularly in the private sector, when we addressed privacy the response was, "You mean security, don't you?" The people we met kept wanting to move the discussion to the realm of security and they held a low-level interest in privacy, per se.

Simonette: I think that's still true and I think that the private sector is currently apathetic about the privacy concerns. We should be saying, "Private industry beware, the legislation is coming."

Chairman: Congressmen Goldwater and Koch have already introduced legislation (HR 1984) which extends the Privacy Act to the private sector. The Department of Commerce has a questionnaire that will go to 500 businesses about the impact of such an extension. It is a big issue and it is coming.

Anderson: Certainly one predictable major impact will be the prohibition of the use of the social security account number by anyone for reasons other than its basic purpose. Industry should prepare for that.

Nolan: The impact on companies whose personal data files are primarily their own personnel files will be fairly light. For example, a major cost item is excluded when you realize that these companies could use their internal mail service for notifications and so forth. It would be a big help if the industries were addressed sector by sector, for example, the insurance and finance companies.

Eberhart: The Fair Credit Reporting Act has helped in preparing some.

Halper: The consumer-paper people are one sector I see as becoming hard hit by any new legislation.

Question: A recent newspaper column said that as many as 100 Federal computer systems (data banks) will be closed down as a result of the Privacy Act of 1974. In terms of a hidden cost, do you see any loss of public services as a result of the Privacy Act?

Discussion: No one suggested that any data system would cease functioning as a result of the Act. Probably all will at least claim compliance. Perhaps some will wind up in court. There are no waiver provisions in the Act. Preparing for court appearances may lead to costs in terms of attorney fees.

Caravella: The Act may have a fringe impact on the use of Data Base Management Systems. The DBMS has the advantage of permitting great flexibility. The Privacy Act requires you to name the uses that you will routinely put the system to and report all non-routine use. This may limit the use of DBMS and even inhibit the development of Data Base Management technology.

Discussion: The definition of routine uses may be written in a sufficiently broad manner to cover a large number of the possible uses and may even be rewritten and republished if the need should occur. DBMS's give a user broad latitude to search the files and to search in ways not previously anticipated. That's their value. However, many use them with portions of the file "locked up" to hold certain data items inaccessible. This approach essentially removes personal identifications from the file and makes it like a statistical file. To get personal identification data the user must have a certain "key." A separate spin-off file from the main file could be defined as one of the routine uses and that separate file could be used in many ways.

5. AGENDA DISCUSSION ITEM: HOW SHOULD COSTS BE ALLOCATED AMONG THOSE WHO RECEIVE PRIVACY'S BENEFITS OR FACE ITS OBLIGATIONS?

Chairman: In turning to the question of privacy cost allocation, we must realistically face up to the point that this year's cost will come out of this year's budget somehow and we may ask for additional appropriations in the future. Eventually, however, the additional cost will come out of the taxpayer's hide. The reason for pursuing the benefits, of course, was to assist us in finding benefits or savings that might be used to offset the privacy costs. This could aid any budget re-programming plans. We couldn't find many such direct economic benefits. In the private sector, the same reasoning applies and similarly the general public will wind up paying for additional costs.

Anderson: We must also mention the irrevocable capital costs associated with initiating the Privacy Act even if it were stopped. You can't go backwards in time to get those expenditures back.

Clemence: The size of the costs undoubtedly will reflect "how loud the wheel squeaks" and lower activity of public demands will determine a lesser amount of expenditures.

Chairman: Given the viewpoint of Willis Ware that even if the costs of privacy were $300 million, that cost divided over 200 million plus Americans is roughly a dollar and, Ware suggests, is well spent.

Eberhart: Our preliminary investigations indicate that any privacy costs will simply become pass-through costs.

Anderson: The privacy costs should not become a catch-all for miscellaneous costs. For example, redesign costs should be so declared rather than calling them privacy costs. I fear that the need for privacy spending will encourage many managers to lump a great number of things under this heading which would defeat our efforts to understand ADP costs and even privacy costs.

Dicussion: What's lacking is any central review of design and cost associated with ADP. The Government does need a good accounting system for determining EDP costs. There is no apparent plan to have a centralized monitor of privacy costs.

Simonette: When I read in the Privacy Act the reference to auditing the privacy requirements, I wondered who would be responsible for that?

Discussion: Primarily the agencies themselves but in reporting to Congress, as they must, the GAO will probably be used to double check the compliance. The Privacy Commission established under the Privacy Act will be limited to studies rather than having oversight functions. OMB has the central executive responsibility. However, no standard system of cost controls exists as a useful tool for OMB.

Anderson: GAO has underway a comprehensive study of cost accounting and cost control through investigations of large private systems, including automative manufacturers, insurance companies, etc. We've visited 56 installations. At the same time our Cost Accounting Standards Board has mailed questionnaires which 1555 agencies have voluntarily answered in order to share their experiences. We hope to develop a good way to do cost accounting. We hope to provide good accountancy methods in terms of guidelines and standards.

Discussion: Most computer systems apply across so many cost centers that it is impossible to spread out the costs across all of them. Some private companies simply make no attempt to detail costs because it doesn't pay.

Clemence: One of the reasons that current thinkers bemoan our current lack of leaders, I think, rests in the trend to follow the numbers. Our leaders seem to be paralyzed by the flood of data. I see a value in using individual judgment in preference to the current trend to "follow the numbers."

6. SUMMARY

Chairman: To provide a rough summary of today's activities let me make the following points:

We seemed to be able to find a lot of costs and a lot of problems associated with implementing this Act, but we weren't able to find very many quantifiable benefits. We found many hidden problems which will bother us in the future. We discussed how costs would be allocated which may be different from how they ought to be allocated.

Anderson: One of the outputs of this session should be a set of future considerations for NBS.

Discussion: Recognizing that NBS is in the technology area of this question and not in the policy aspects, it could aid other Federal agencies by considering the following tasks:

o A very detailed outline of the factors that affect the costs should be constructed. One such structure is evident in the work of Dr. Nolan. The goal would be a hierarchial structuring of cost parameters into a high degree of refinement.

o A checklist of each of the items to be considered in each of the various technical areas that would affect costs.

o A follow-up meeting to assess costs as actually experienced.

o A set of guidelines on technological steps that fall somewhere in between ad hoc solutions using today's systems and complete redesign of systems.

o Preparation of alternatives and methodologies for certain selected sub-portions of the privacy requirements, like the disclosure and usage systems. This could be a technical task using NBS skills or skills convened from outside NBS.

o Application of Drs. Nolan and Goldstein's work specifically to the Privacy Act.

o Review of existing cost analyses of the various existing privacy legislation. For example, the State of Illinois study, second volume.

o The summary of this workshop should be published quickly to insure the widest possible availability of the information to the agencies.

o Identification and separation of the various cost components into those which when implemented provide minimal compliance with the Act and those other things which while desirable are not mandatory.

Mr. Bearden observed that while the panel may not have exhausted the subject matter of privacy costs the subject matter seems to have exhausted the panel. He expressed his thanks and that of ICST for their enthusiastic and able participation.

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS TN-876	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

Exploring Privacy and Data Security Costs--A Summary of a Workshop

5. Publication Date: August 1975

6. Performing Organization Code

7. AUTHOR(S)
John L. Berg

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No. *640-1112*

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

13. Type of Report & Period Covered

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 75-600063

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

On February 20, 1975, the ICST hosted a one-day round-table discussion on the economic aspects of privacy and data security costs. The workshop was chaired by Gary Bearden, U.S. Civil Service Commission. The participants were Walter L. Anderson, General Accounting Office; Richard A. Eberhart, Office of the Secretary, Department of Commerce; Earl P. Bassett, Jr., Vice President, 3M Company; Robert Caravella, Federal Trade Commission; Theodore Clemence, Bureau of Census; Richard L. Nolan, Harvard Business School; Stan Halper, Coopers and Lybrand; and Larry Simonette, Peat, Marwick, Mitchell and Company. The group discussed the benefits EDP managers or data base administrators might gain from the privacy requirements, the processes for identifying direct or hidden costs, and processes for allocating costs.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Computer security; data security; privacy; privacy costs; security costs.

18. AVAILABILITY

[XX] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[X] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13.46:876

[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
UNCLASSIFIED	35
20. SECURITY CLASS (THIS PAGE)	**22. Price**
UNCLASSIFIED	85 cents

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. It is published in two sections, available separately:

• **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

• **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $9.45; Foreign, $11.85.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St. N. W., Wash. D. C. 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Federal Information Processing Standards Publications (FIPS PUBS)—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service (Springfield, Va. 22161) in paper copy or microfiche form.

Order NBS publications (except NBSIR's and Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service

A literature survey issued biweekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to National Technical Information Service, Springfield, Va. 22161.

Electromagnetic Metrology Current Awareness Service Issued monthly. Annual subscription: $100.00 (Special rates for multi-subscriptions). Send subscription order and remittance to Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

SPECIAL FOURTH-CLASS RATE
BOOK

U.S.MAIL

AMERICAN REVOLUTION BICENTENNIAL 1776-1976