In Support of a Data Protection Board in the United States

Marc Rotenberg*

The development of commercial products containing detailed compilations of personal information underscores the need for the establishment of a Data Protection Board in the United States. Computer technology facilitates the exchange of personal information, but responsibility for the proper use of personal data lies with the organization that collects the information. Whereas other countries have moved aggressively to establish reasonable safeguards to protect individual privacy through the creation of data protection boards and privacy commissions, the United States has failed to adopt similar measures. A privacy protection commission was a key component of the original privacy protection scheme developed by the Congress in the early 1970s but was never enacted. Recent public polling data suggests that the creation of a similar board today would be supported by a wide majority of Americans.

The United States must move quickly to address the growing privacy problems that arise from the collection and transfer of personal information generated by computerized recordkeeping systems. Failure to do so will likely increase public concern about privacy safeguards and undermine efforts to develop new products that are technology based.

Automated information systems, by virtue of their processing capability, pose an ongoing risk to personal privacy. For this reason, the computer science community has long argued that adequate safeguards must be established to protect personal information. The code of ethics of many computer associations and related professional organizations clearly state the importance of data protection in the design of computer systems.[1] Computer scientists have also played a prominent role in congressional proceedings and the development of key reports that gave rise to many of the privacy laws in the United States today.[2] And computer privacy remains a central concern at regular meetings of computer professionals.[3]

*Direct all correspondence to: Marc Rotenberg, Computer Professionals for Social Responsibility, Suite 1015, 1025 Connecticut Avenue, N.W., Washington, DC 20036.

Goverment Information Quarterly, Volume 8, Number 1, pages 79–93.
 ISSN: 0740-624X.

The Computer Professionals for Social Responsibility (CPSR) has played a leading role in recent efforts to develop appropriate privacy safeguards. In 1986, CPSR established a special project on computer and civil liberties to address growing concern among our membership about privacy safeguards. Since that time we have reviewed the privacy and civil liberties implications of various computing systems in both the public and private sector, and have recommended appropriate safeguards.[4] Two years ago, several of our members participated in an expert panel review of the proposed expansion of the FBI's records system at the request of Congressman Don Edwards.[5] That review led to the decision to drop a proposed tracking feature that could have turned the FBI's database into a national surveillance system.[6]

Concerns about privacy protection are widely shared by the general public. Opinion polls and research studies have consistently shown that Americans are concerned about the protection of privacy and will support legislative efforts to protect privacy.[7] In recognition of this concern, many large organizations in both government and the private sector have developed policies and practices to safeguard personal information.[8]

Though the courts and the Congress have struggled to define the right to privacy, there can be little doubt that such a right is necessary for the protection of individual liberty that makes democratic self-governance possible. Without the ability to control the disclosure of the intimate facts, individuals lose the ability to shape identity, to establish trusts, and to form smaller communities within the larger community. It is not a coincidence that a primary attribute of totalitarian societies and the dystopias that are often found in science fiction is that individuals lack personal privacy.

Privacy is the right of individuals to control the disclosure of personal information and to hold those accountable who misuse information, breach a confidence, or who profit from the sale of information without first obtaining the consent of the individual. In the design of a computer system containing personal information, it is a primary consideration.

There is little question that new computer technology has made it easier for large organizations to collect and exchange information about individuals.[9] And it has also made possible inferences about individual behavior based on this information. Computer technology has spawned an enormous proliferation of detailed transactional data that can be used for purposes potentially detrimental to the interests of the person involved. The problem today is that there is inadequate policy guidance to ensure the protection of privacy for this personal information.

For example, a simple billing statement sent by the phone company to verify the monthly charges provides a readily accessible list of all the people contacted, the length of the calls, and the location of the calls. For the phone subscriber this information is important to verify charges. To an unknown third part, it would provide a window into the subscriber's personal life, a listing of friends and associates, an invasion of privacy more intrusive than if a stranger were to leaf through a personal address book copying down the names and numbers.[10] While phone companies have traditionally safeguarded this information,[11] there is a growing awareness that the traditional restrictions are being relaxed. Certain phone services, such as 800 phone services, are now developed specifically for the purpose of gathering marketing data.

The problem is further compounded when transactional data from different sources are gathered in a single place to create a detailed dossier of spending habits, political associa-

tions, friends and neighbors, lifestyle, and work hours. Few people would willingly consent to the development of the electronic profiles that are now becoming available. However, because the United States has failed to establish enforceable rights for privacy protection for this transactional data, detailed information is now available for sale without the knowledge or consent of the person described.

Computer scientists working with policy makers anticipated many of the privacy problems that could result from the unrestricted use of transactional data. In 1973, they helped to draft a set of principles—The Code of Fair Information Practices—that were designed to minimize the privacy risks of automated systems containing personal information. The Code set out a series of principles for the protection of personal information stored in computer systems.[12] These principles are:

- There must be no personal data recordkeeping systems whose very existence is secret;
- A person should know what information about that person is in a record and how it is used;
- A person should be able to correct or amend a record of identifiable information about the person;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data; and, most importantly,
- Any information obtained for one purpose should not be used for another purpose without the consent of the person.

This last principle is the cornerstone of the Code and the golden thread that ties together virtually all of the data protection law in the United States.[13] It is based on a simple premise: that when you give personal information for a particular purpose—to obtain a warranty, to reserve a hotel room, or to charge a dinner—you do not reasonably expect that the information will be used for another purpose without your consent. That is the implied promise between you and the institution. When the institution breaks that trust, they have undermined your expectation of privacy and acted without regard to your interest in controlling records of your personal life.

There has been a great deal of public interest in the "frequent shopper" programs.[14] These are programs that allow supermarkets to collect detailed information on particular customers. The computer in combination with point of sale (POS) scanning technology, makes it economically feasible to collect and analyze a great deal of transactional information that previously would have been impossible to gather. A supermarket manager can now tell that a particular customer buys broccoli and not asparagus, prefers frozen vegetables to canned vegetables, and possibly whether that customer buys contraceptives, antidepressant drugs, or tabloid magazines.

From the seller's viewpoint this could be a wonderful innovation. Sellers have far more information about the preferences of their customers. They can make purchasing decisions more effectively. They can target products to particular customers based on buying patterns. For example, the store might offer rebates to customers who buy four cans of a specific brand of coffee over three months, or the seller might reward buyers who frequently return to the store with discounts and bonuses, similar to the mileage programs

offered by the airlines. For the effective manager, the frequent shopper program should produce larger sales, greater revenue, and increased customer loyalty.

From the customer's viewpoint, as well, the program may also produce benefits—products more carefully tailored to particular needs, better value, and more efficient services. Customers will find that their supermarket is recommending specific products based on their buying habits. For example, frequent buyers of frozen dinners are likely to receive special offers for new frozen dinner products. The image that comes to mind is that of the corner store where the shopkeeper, knowing that you like a particular item, smiles as you enter the store and pulls out from beyond the counter a jar of pickling sauce that you always try to find and that is often out of stock.

The problem with the frequent shopper program is that it is not just the shopkeeper in the corner store that knows of your preference of a certain pickling sauce. Under the programs currently underway, the personal data gathered at local supermarkets will flow into the computers of Citicorp. Citicorp will also know who likes pickling sauce, who has hemorrhoids, and who buys condoms. And here is the problem. Why should one of the country's largest financial institutions also become a broker for the shopping preferences of American customers? And why should they obtain this information without the knowledge and informed consent of consumers?[15]

Of course, Citicorp is not alone in the efforts to sell personal data. An extraordinary product, due out on the market in 1990, is Lotus MarketPlace. MarketPlace is a CD-ROM—a computer disk—containing the buying preferences of 80 million American households. The disk contains profiles on 120 million American consumers, including:

- Name;
- Address;
- Age;
- Gender;
- Marital status;
- Household income;
- Lifestyle;
- Dwelling type, and
- Actual buying habits across 100 product catagories.[16]

From a data protection viewpoint, this product would receive low scores. First, the product violates Fair Information Practices—personal information which was collected for one purpose is used for another purpose without the individual's consent. It is fair to say that very few of the 120 million people listed in MarketPlace consented to the use of their personal information in this way. And though Equifax has claimed that it is not possible to obtain information on specific individuals—only lists—it is hard to understand why it would not be possible to extract highly detailed information about individuals. In fact, Equifax is already using their in-house databases in precisely this way for screening potential employees.[17]

There is currently no legal safeguard that prevents Equifax from selling individually identifiable information to third parties if it chose to. This is a critical privacy concern for the American public and Congress.

Second, CD-ROM is a read-only medium, which is to say that once the information is

stored it cannot be erased. There is no effective mechanism for consumers to "opt-out" of the list once the CD-ROM are distributed. And there is no way to correct data inaccuracies once the product hits the streets. With such a readily available and extensive compilation of data from different sources, the product takes computer matching to a new level. Not surprisingly, Equifax has stated that it has no plans to notify individuals or inform the public that they will be marketing this data.[18]

This new product poses a particular threat to personal privacy because it places the actual data in the hand of individuals and beyond the control of even the responsible information brokers. Those who purchase MarketPlace may not follow the Direct Marketing Association's guidelines for personal information protection and ethical mailing list practices. Further, there is no guarantee that these individuals or organizations will not ultimately be able to access all the identifiable information on the disk. There is nothing to prevent other firms from selling similar products with even more detailed information on individuals.

Once this information on lifestyles and buying habits is sold to third parties, the ability to control the disclosure of personal information is diminished and the right to privacy is undermined.

These companies should not sell information about any consumer without first obtaining consent and then taking adequate steps to ensure that the data are accurate, complete, and timely. If they fail to do this, then consumers who value their privacy should write to Citicorp and Equifax, sending copies of their letters to this committee, their elected representatives, and the U.S. Office of Consumer Affairs, objecting to the sale of this product.

There are other information products which clearly undermine privacy, are at odds with principles of data protection, and would be opposed if more widely known. For example,

- Philip Morris, as part of its promotion for the Bill of Rights, solicited home telephone numbers from all individuals who called to request a copy of the Bill of Rights. But telephone number are not needed to mail a copy of the Bill of Rights, the alleged purpose of the promotion. However, telephone numbers do serve as a vital link to other databases which Philip Morris might search to learn more about the demographics and lifestyles of individuals responding to the promotion.[19]
- Wats Marketing of Omaha, Nebraska has 10,000 incoming 800 number phone lines with Automatic Number Identification connected to Donnelly Marketing's Fast Data System. According to a recent issue of *The Friday Report,* a direct marketing trade newsletter, the phone numbers of incoming calls will be matched with the home addresses of more than 80 million individuals in the Donnelly database. As a result, individuals who make an anonymous phone call to an 800 phone number to request information will find themselves the unwitting target for subsequent mailings and telemarketing campaigns. Even the fact that these people responded to a campaign for a particular product or service will be sold to anyone interested in targeting individuals who use the phone to shop.[20]
- Large mailing list brokers routinely merge single lists they manage with demographic or lifestyle information. For example, Worldata recently advertised, "the Holiday Inn Great Rates List," identifying the list members as adults, ages 25 to 45, heading families with an average household income of over $30,000 who have responded to

print or television advertisements for Holiday Inn.[21] It is unlikely that the individuals on the Worldata list who responded for the Holiday Inn ads provided all this detailed information, nor expected that responding to an ad would mean that third parties would obtain such detailed personal information.

- Most disturbing, hospitals are now selling medical information for direct marketing. Hospitals have also learned that they can generate lists by sponsoring seminars, fairs, or health-screenings at a shopping mall or exposition. The hospital then uses the names of the persons who register for the free seminar and follows up with mailings or telephone calls soliciting business for the hospital.[22]

The firms which collect and sell this information argue that there is no real harm and that consumers benefit from these practices. But if the companies were required to tell consumers how this information was obtained and were then required to seek consent before the information was resold, they would have a far more difficult time justifying the sale of these elaborate dossiers.

What is taking place is a form of deception cloaked under the banner of innovation. Detailed personal information—age, gender, marital status, and income—is being bought and sold with little regard to the long-term implications for personal privacy or the concerns of the American people. The companies that engage in these practices say do not worry, it is all to your benefit, there is no need for government review.

It is hard to believe that this response would satisfy most Americans. According to a recent privacy survey:

- 90% of all Americans do not think that companies disclose enough information about their list usage; and
- 80% do not think companies should give out personal information to other companies.[23]

Not surprisingly, much of the most informed concern about the privacy implications of these new practices is coming from within the direct marketing industry, from the people who are most familiar with the data collection practices and recognize the privacy dangers. For example, the editorial director of *Target Marketing Magazine* wrote recently:

> The issue of consumer privacy will not go away simply because direct marketers don't confront it. . . . The privacy question is really about trafficking in information that is freely obtained for one purpose and then sold for another. . . . When a consumer fills out a credit application, because he must do so in order to obtain a credit card, does he understand that this information will be traded, rented and sold? Is he given an option of whether or not that information may be revealed to others? Do lifestyle questionnaires include options as to whether or not that information may be revealed to marketers? . . . We must give consumers these options. They must be presented as positive options . . . not negative ones. This industry must protect itself. If we don't take the lead and deal with the privacy question, Congress could force us to deal with it on someone else's terms.[24]

There is good reason that market research firms and credit bureaus should be concerned about the adequacy of private safeguards. Another recent poll revealed that marketers and credit bureaus rate lowest for protecting customer confidentiality.[25]

The particular concern of privacy advocates who have studied the effects of automated information systems is the tendency of information systems, absent adequate safeguards, to form enormous pools of personal activities. This problem was recognized by the ranking minority member of the Committee on Government Operations, Representative Frank Horton, who said almost twenty-five years ago:

> One of the most practical of our present safeguards of privacy is the fragmented nature of personal information. It is scattered in little bits across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard.[26]

The problem with these new commercial products that are based on the compilation of personal information is that it is easy to see the benefits and more difficult to assess the costs. This problem was anticipated by Jerome Wiesner, the former dean of MIT and former science Adviser to President Kennedy. Testifying before a Senate subcommittee in 1973, Wiesner warned that, absent adequate safeguards, automated record systems might lead to an "information tyranny":

> Such a depersonalizing state of affairs could occur without overt decisions, without high-level encouragement or support and totally independent of malicious intent. The great danger is that we could become information bound, because each step in the development of an information tyranny appeared to be constructive and useful.[27]

The challenge today is to ensure that such an information tyranny does not result even though each step along that path appears beneficial.

THE UNITED STATES HAS A WELL ESTABLISHED COMMITMENT TO INFORMATION PRIVACY WHICH MUST BE EXTENDED TO PRIVATE SECTOR ACTIVITIES THAT VIOLATE THE CODE OF FAIR INFORMATION PRACTICES

Large organizations in both the government and the private sector have an obligation not to disclose personal information about individuals without the consent of the individual. This was the principle underlying the Privacy Act of 1974 and it is the threat that ties together virtually all of the privacy laws in this country. When an organization discloses personal information without consent, or effectively compels the disclosure of personal information as the cost of doing business, it has diminished the right of privacy, our most fragile freedom.

Privacy protection need not be measured against economic benefit and corporate riches. The equation mistakenly places individual liberty on the auction block. Many companies have developed policies that respect the privacy interests of their customers and their employees.[28] In the computer industry, advertisers frequently use "bingo" cards to allow subscribers to contact manufacturers about product inquiries. It is a good system—the consumer affirmatively indicates, by completing the card, interest in receiving information from the manufacturer. There are other examples of good privacy protection practices, such as phone directories that clearly indicate that the 911 phone service has a call trace feature. In this way, individuals who call a 911 number will have fair notice that the

location of the call will be known to the police. Another example is the NAD (USA) "Non-Warranty Card" which clearly informs the purchaser that the product warranty does not depend on the return of the card and that if the consumer chooses to return the card, the information will be used for marketing research.

Another example of a good privacy practice is the privacy policy adopted by New York Telephone. This is particularly notable at a time when many phone companies are selling transactional data generated by phone calls. New York Telephone has said to its customers:

> It is New York Telephone policy to protect the privacy of your account information. This includes the types, locations and quantity of all services to which you subscribe, how much you use them and your billing records. We will release this information to persons or companies not affiliated with New York Telephone, such as enhanced service vendors, only when you authorize such a release in writing.[29]

These policies help protect privacy interests and should be encouraged. But standing alone they are not sufficient. Too few companies have adopted such privacy policies; too many gather data in a misleading fashion and sell it without obtaining consent. It is for this reason, that Congress must act.

TIME FOR GOVERNMENT ACTION

It is clear that the time has come for Congress to address one of the most pressing issues that will confront this country in this decade—the protection of information privacy. Recognizing that there is widespread support in the United States for new privacy legislation and that current safeguards are inadequate, the question is simply where to begin. The answer is to establish a Data Protection Board. The Board is the missing piece in the privacy protection framework of the United States.

The establishment of a Federal Privacy Board was the cornerstone of legislation introduced by Senator Sam Ervin in 1974. His bill became the Privacy Act, the foundation of privacy protection in the United States. However, strong opposition by the Ford White House led to the demise of the proposed Board before final passage. In its place, a Privacy Protection Study Commission was created.[30]

But when the Commission completed its study of privacy protection in 1977, the same conclusion was reached. The Privacy Protection Study Commission recommended the creation of the Federal Privacy Board. It believed that the Board could play an important role in safeguarding privacy. The final report of the Commission recommended:

That the President and the Congress should establish an independent entity within the Federal government charged with the responsibility of performing the following functions;

- To monitor and evaluate the implementation of any statutes and regulations enacted pursuant to the recommendations of the Privacy Protection Study Commission, and have the authority to formally participate in any Federal administrative proceedings or process where the action being considered by another agency would have a material effect on the protection of personal privacy, either as the result of direct government action or as a result of government regulation of others.

- To continue research, study, and investigate areas of privacy concern, and in particular, pursuant to the Commission's recommendations, if directed by Congress, to supplement other governmental mechanisms through which citizens could question the propriety of information collected and used by various segments of the public and private sectors.
- To issue interpretative rules that must be followed by Federal agencies in implementing the Privacy Act of 1974 or revisions of this Act as suggested by this Commission. These rules may deal with procedural matters as well as the determinations of what information must be available to individuals or the public at large, but in no instance shall it direct or suggest that information about an individual be withheld from individuals.
- To advise the President and the Congress, government agencies, and, upon request, states, regarding the privacy implications of proposed Federal or state statutes or regulations.[31]

The commission recognized that the board need not have enforcement power over private sector record systems, but that it would have a responsibility to identify privacy abuses and recommended changes. It would, in effect, be an ombudsman, a spokesperson for the widely shared belief of Americans that privacy is cherished value in a free nation and must be considered in the design of computer systems containing personal information.

Thirteen years later, there can be no doubt that the United States needs a Data Protection Board. There is no mechanism to assess the new uses of transactional data. Current privacy safeguards are simply inadequate.

First, individuals now carry the burden for identifying improper data collection practices and making corrections in personal records. When information is shared across the Federal government or between public and private organizations, it becomes increasingly difficult to identify problems and resolve complaints. A single agency would provide valuable assistance.

Second, the Office of Management and Budget (OMB) has failed to fulfill the role of privacy ombudsman, a stop-gap result of the failure to include the Board in the original Privacy Act of 1974. As Flaherty notes in his recent book on data protection in the United States and abroad, OMB has exercised weak leadership.[32] When privacy requirements conflict with other Federal agency goals, there is little guarantee that individual rights will prevail absent oversight from an independent board.[33]

It should be noted that in the past year the Director of the U.S. Office of Consumer Affairs has played an important role in drawing attention to new privacy problems for American consumers. Guiton has been an outspoken advocate in defense of privacy rights and has renewed the long-simmering debate within the United States about the adequacy of current privacy safeguards. At the same time, regrettably, the Office has failed to endorse important privacy measures. Consumer education, industry self-regulation, and voluntary guidelines are not a substitute for enforceable legal rights that guarantee the protection of consumer privacy. Self-help measures, such as opt-out provisions, have placed an onerous burden on consumers. The Office of Consumer Affairs is moving in the right direction, but it must go much further and with more support from the Administration.

Third, the United States lags behind other countries in protecting the privacy rights of

its citizens. Independent privacy boards and commissions were established more than a decade ago in Sweden, France, West Germany, and Canada. As participants in the emerging global economy, American companies are directly affected by data protection laws in other countries. The lack of a data protection agency in the United States leaves U.S. firms unrepresented when decisions are made about the transborder exchange of personal information.[34]

Finally, sector by sector protection of personal information in the private sector has left significant gaps in Federal privacy law. Certain records are covered by Federal statues; other records receive no protection at all. The Computer Matching Act of 1988, designed to prevent the development of computerized dossiers, does not address the widespread exchange of personal information between private sector companies. If a similar record exchange were proposed for Federal agencies, it would be strictly prohibited under the Privacy Act of 1974.

The Data Protection Board could address these activities that undermine well-established privacy standards. The Board could also promote successful industry data protection practices, such as the adoption of Fair Information Practices described by Linowes in *Privacy in America.*[35]

The effectiveness of the board would also be greatly enhanced if the following changes were made. First, the bill should vest the Board with enforcement powers over Federal agencies. Without any enforcement mechanism, such as the power to issue cease and desist orders that was proposed in Senator Ervin's 1974 bill, it is unclear how effective the Board will be.

Second, the size of the Board should be increased and membership terms should be modified. A three-member Board will not be adequate if the Board assumes greater responsibilities in the future. Further, if any of the seats on the three-member Board became vacant, the functioning of the Board will be severely jeopardized. Consistent with the original 1974 proposal, the Board should also be expanded from three to five members, while maintaining the current funding level. The remaining two positions would be funded only as needed in the future. Furthermore, the terms of the initial appointees should be staggered.

Third, considering the long delay in establishing the Board and the ACLU's assessment that there is an urgent need to reexamine the Privacy Act,[36] CPSR suggests that the Board's recommendations for amending the Privacy Act of 1974 be delivered to Congress one year from the date that the legislation takes effect.

Finally, the proposed legislation should address privacy issues for private sector record-keeping systems, particularly the secondary use of transactional data. Currently, there are widespread violations of Fair Information Practices; information which is not needed for a particular transaction is routinely obtained and used for unrelated purposes, or sold to other parties without the knowledge and consent of the consumer.

As privacy scholars have often noted, the United States, unlike most of Western Europe, has drawn a distinction between record systems operated by the government and those in the private sector. For this reason, argue some in industry, it would be inappropriate to regulate private sector privacy. However, this view ignores the record of privacy legislation in the United States during the last ten years. For if one lesson is clear, it is that Congress has shown itself willing to establish privacy safeguards in the private sector to ensure privacy protection, particularly where new technologies are involved.

For example, as the cable industry took off in the early 1980s concern about the privacy of subscribers information also grew. Congress responded. The Cable Communications Policy Act of 1984 prohibited a cable service from disclosing information about a subscriber's cable viewing habits without the individual's consent. The Act requires the cable service to inform the subscriber of the nature and use of personally identifiable information collected; the disclosures that may be made of such information; and the period during which such information will be maintained. The cable service must also provide subscribers access to information maintained about them.[37]

Electronic mail, a boon to communication, also raised concern about the security of the content of electronic messages. The Electronic Mail Association was as worried as its customers, perhaps more so, because of the concern that a new mail service would not be very useful if privacy could not be assured. The Electronic Communication Privacy Act of 1986 responded to the need for privacy protection for this new form of communication.[38]

And, when a nominee to the Supreme Court found that his choice of videos that he watched with his family in their home had become the subject of an article in a local newspaper, Congress enacted legislation to protect the rental list of video users.[39]

So, too, it should be with the sale of personal data, aggregated from separate lists, that are gathered and sold without adequate privacy safeguards or the knowledge and consent of the people involved. The Code of Fair Information Practices should be codified into law to provide this protection. The data protection principles of the Direct Marketing Association could also form the foundation for an enforceable legal right of information privacy.

The establishment of a data protection board is a modest first step that would shine some light on the privacy problems facing this country, and begin to propose solutions that could be adopted. This need not be an adversarial process that pits the Federal government against the private sector, but it must be a determined process, conducted with dedication and a commitment to individual liberty. This is also not about restricting technology; it is about the responsible application of technology so that risks to personal privacy are reduced.

There is a clear need to carry forward the principles embodied in privacy law in the United States and to ensure that Fair Information Practices apply to private sector record systems. The intimate details of our private lives enjoy the same protection whether big business or big government is the custodian. Absent clear privacy safeguards, we are left at the mercy of a rapidly evolving technology and an industry that can say little more than "trust us." This is at odds with the history of privacy protection in the United States and places the fragile freedom of American citizens in a precarious position.

ACKNOWLEDGMENTS

This article is adapted from prepared testimony on Computer Privacy and H.R. 3669, "The Data Protection Act of 1990," before the Subcommittee on Government Information, Justice and Agriculture, Committee on Government Operations, House of Representatives, May 16, 1990. The testimony was prepared with the assistance of Professor Mary J. Culnan, School of Business Administration, Georgetown University, and Dr. Ronni Rosenberg, Kennedy School of Government, Harvard University.

NOTES AND REFERENCES

1. The Association for Computing Machinery (ACM) Code of Professional Conduct states that:

   Ethical Considerations:

   EC5.1 An ACM member should consider the health, privacy, and general welfare of the public in the performance of his work.

   EC5.2 An ACM member, whenever dealing with data concerning individuals, shall always consider the principle of individual privacy and seek the following:
   To minimize the data collected;
   To limit authorized access to the data;
   To provide proper security for the data;
   To determine the required retention period of the data;
   To ensure proper disposal of the data.

   The Data Processing Management Association (DPMA) Code of Ethics, Standards of Conduct and Enforcement Procedures states:

   "In Recognition of My Obligation to Society I Shall: Protect the privacy and confidentiality of all information entrusted to me"

   The preliminary code of ethics for the International Federation of Information Processing (IFIP) makes data protection a central provision of Individual Professional Ethics:

   1.2 Protection of Privacy

   Information Technology Professionals have a fundamental respect for the privacy and integrity of individuals, groups, and organizations. They are also aware that computerized invasion of privacy, without informed authorization and consent, is a major, continuing threat for potential abuse of individuals, groups, and populations. Public trust in informatics is contingent upon vigilant protection of established cultural and ethical norms of information privacy.

   Computers & Society, 36 (March 1990): 20 (Emphasis added).
2. Willis H. Ware, a noted computer scientist at the Rand Corporation, chaired the Secretary's Advisory Committee on Automated Personal Data Systems of the Department of Health, Education & Welfare. That Committee produced *Records, Computers and the Rights of Citizens* (1973), a landmark report which outlined the privacy risks of automated record systems, recommended various safeguards, and gave rise to the Privacy Act of 1974, the most comprehensive privacy law in the United States. Joseph Weizenbaum, an emeritus professor of Computer Science at MIT, was also a member of the Advisory Committee.

   Subsequent reports by the Office of Technology Assessment have often relied heavily on computer scientists to assess the privacy risks on automated information systems. See, e.g., *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (Washington, DC: GPO, 1987).
3. See, e.g., Rein Turn, "Information Privacy Issues for the 1990s," "1990 *IEEE Symposium on Security and Privacy* 395.
4. See, e.g., Ronni Rosenberg, "Privacy in the Computer Age," *CPSR Newsletter*, 4 (1986–1987): 3–5; "FBI Fails to Allay Concern for Civil Liberties," *Government Computer News*, 19 (September 18, 1989) (letter from Marc Rotenberg, CPSR Washington Office Director) (FBI records system); "Phone Gadget Reveals Caller's Number," *The Los Angeles Times*, (December 1, 1989, p. D1 (caller ID); Marc Rotenberg, "The Only Locksmith in Town: The NSA's Efforts to Control the Dissemination of Cryptography," *Index on Censorship*, (January 1990), p. 12 (data communication privacy); Felicity Barringer, "Electronic Bulletin Boards Need Editing: No They Don't," *The New York Times*, (March 11, 1990), p. 6, section V (electronic speech); William Trombley, "Electronic Elections Seen as an Invitation to Fraud," *The Los Angeles Times*, (July 4, 1989), p. 1 (reliability of computerized vote counting).

   Most recently, CPSR sponsored a panel discussion at the Kennedy School of Government on the civil liberties implications of the use of expert systems by law enforcement agencies.
5. See *FBI Oversight and Authorization Request for Fiscal Year 1990: Hearings* before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, 101st Cong.,

1st Sess. (1989), pp. 512–596; Horning, Neumann, Redell, Godman & Gordon, *A Review of NCIC 2000: The Proposed Design for the National Crime Information Center* (1989) (Expert panel report), reprinted in Ibid., pp. 512–576.

6. "FBI Rejects Plans to Widen Computer's Data on Suspects," The *New York Times,* (March 4, 1989), "FBI Rejects Computer Use on Suspects: Plan Would Have Allowed Tracking Those Not Charged with a Crime," *The Washington Post,* (March 3, 1989), p. A6.
7. See, e.g., *Privacy and 1984: Public Opinions on Privacy Issues: Hearing* before a Subcommittee of the Committee on Government Operations, House of Representatives, 98th Cong., 1st Sess. (1984), pp. 9–75 (testimony of Lou Harris). See discussion infra, at 12.
8. David Linowes, the former chairman of the Privacy Protection Study Commission, detailed the efforts of Fortune 500 companies to protect the privacy interests of both customers and employees in *Privacy in America* (Champaign, IL: University of Illinois, 1989).
9. David Burnham, *The Rise of the Computer State* (New York: Random, 1983). See also Kenneth C. Laudon, *The Dossier Society* (New York: Columbia University Press, 1986); Linowes, *Privacy in America;* Robert Ellis Smith, Privacy (Washington, DC: Privacy Journal, 1980); Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967). Linowes found in his review of the recordkeeping practices of Fortune 500 companies that, not surprisingly, as discrete record systems within an organization were automated they were also brought together in consolidated databases (p. 60).
10. The problem of controlling the misuse of phone numbers has been directly addressed in Europe and is the subject of extended discussion in the United States.
11. H.W. William Caming, "Protection of Personal Data in the United States," *The Information Society,* 3 (1984): 118–122.
12. U.S. Department of Health, Education & Welfare, Records Computers and the Rights of Citizens (1973), p. 41.
13. A related goal is that organizations should seek to minimize the amount of personal information that is collected, since it is in the collection of information that unintended and unanticipated risks to privacy arise. "Data minimization" is a central theme of many privacy protection programs. See ACM Code, supra note 1; David Linowes, *Privacy in America* (1989), p. 175. For a discussion of the potential privacy risks in government information systems, absent an effort to reduce the collection of transactional data, see Marc Rotenberg, "The Computer Security of 1987 (P.L. 100-235) and the Memorandum of Understanding between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA)," the Subcommittee on Legislation and National Security, Committee on Government Operations, House of Representatives, May 4, 1989 reprinted in *Military and Security Council of Computer Security Issues,* 101st Cong., 1st Sess. (1989), pp. 80, 106–108.
14. See, e.g., Lena H. Sun, "Giant to Test Supermarket Cash Rebates," *The Washington Post,* (June 14, 1989), p. A1; Michael Freitag, "In This Computer Age, Who Needs Coupons?," *The New York Times,* (June 15, 1989), p. 1; Lena H. Sun, "Checking out the Customer: New Technology Can Give Stores Detailed Knowledge about Buyer's Habits," *The Washington Post,* (July 9, 1989), p. H1; Mark Potts, "Giant to Widen 'Frequent Buyer' Rebate Test," The Washington Post, (September 16, 1989), p. D12; Martha Groves, "Frequent-Shopper Plans Are Wooing Customer," *The Los Angeles Times,* (October 1, 1989), p. 1. According to the Washington Post, customers who sign up for Reward America will receive cards with bar codes that will be scanned at Giant checkout counters. The data on the shoppers purchases will then be entered into a computer system. Customers will be sent monthly statement tallying their purchase of the roughly 100 products to be included in the program. When they satisfy a specific purchase requirement, they will receive rebate vouchers that can be redeemed at Giant stores.
15. These data collection practices could be described as misleading at best. For example, one of the conditions specified in the application for Safeway's Preferred Customer Program is that customers "agree to allow Safeway Stores, Incorporated and their processing supplier to record and make use of information about products they purchase." It is hard to believe that by signing this agreement customers have given Citicorp permission to sell detailed information about themselves and their purchase to unspecified third parties.
16. "Retail New Outlet for Lists on CD-ROM," *Direct Marketing,* (May 1990), p. 10.
17. "Corporate Stars of the Future," *The Wall Street Journal,* (July 8, 1990), p. A30. Another major information vendor, TRW, already offers a locator service called Sherlock that scans through computer data to determine the most recent address of individuals.
18. "New Service Offers Marketing Data on 120 Million People," *The Privacy Times,* (May 9, 1990), pp. 1, 2.

19. Mary J. Culnan, "Bill of Rights? Or Bill of Goods," *The New York Times,* (January 21, 1990), p. E21 (op-ed).
20. Mary Lu Carnevale, "Phone Data Enters the Junk-Mail Morass," *The Wall Street Journal,* (May 4, 1990), p. A5A.
21. *Direct Marketing,* May 1990.
22. "Using Medical Information for Marketing," *Privacy Journal,* 16 (February 1990): 1.
23. American Express Survey (1986). Another recent survey shows similar concern for privacy protection and support for new privacy legislation. According to *Cambridge Reports Trends & Forecasts* (May 1989, p. 6), seven out of ten people say that personal privacy is very important; three-quarters of the population are concerned that their privacy is actually threatened; and the majority of those expressing an opinion believe that Federal privacy laws should be strengthened. Professor Alan Westin is expected to release a new privacy survey later this year.
24. Jo Anne Parker, "The Real Privacy Issues," *Target Marketing Magazine,* (November 1988), p. 6, quoted in Mary Gardiner Jones, "Privacy: Significant Marketing Issues for the 1990s," p. 13 (Available from Consumer Interest Research Institute, Washington, DC).
25. *Cambridge Reports Trends and Forecasts,* (May 1989), p. 6.
26. *The Computer and the Invasion of Privacy,* Hearings before the Special Subcommittee on Invasion of Privacy of the Committee on Government Operations, House of Representatives, 89th Cong., 2d Sess. (1966), p. 6.
27. *Hearings on Federal Data Banks, Computers, and the Bill of Rights* before the subcommittee on Constitutional Rights of the Senate Judiciary Committee, 92nd Cong., 1st Sess., p. 761, as quoted in Records, Computer and the Rights of Citizens (1973), p. 225.
28. See Linowes' *Privacy in America.*
29. "Rollout: on Privacy," *Direct Marketing,* (May 1989), p. 4 (noted with approval by Raymond Roel, the Editor).
30. See Albinger, "Personal Information in Government Agency Records: Toward an Informational Right to Privacy," *Annual Survey of American Law* (1986), pp. 625, 642 n. 150.
31. Privacy Protection Study Commission, *Personal Privacy in an Information Society.* Report of the Commission (Washington, DC: GPO, 1977), p. 37.
32. David H. Flaherty, *Protecting Privacy Protection in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill, NC: University of North Carolina Press, 1989), p. 304.
33. See George Trubow, *Watching the Watchers: The Coordination of Federal Privacy Policy* (Washington, DC: Benton Foundation Project on Communications & Information Policy Options, n.d.), pp. 9–10; Albinger, supra note 26, pp. 642–643.
34. The need for the development of data protection policies in the United States was made clear at a recent meeting in Luxembourg with the European Council and the Council of Europe on access to public information, data protection and computer fraud. Participants were told that countries that do not develop data protection laws by 1992 may face curtailment of transborder data flow. Thus far, seven of the twelve member countries of the European community have developed data protection laws. See *Access Reports,* 16 (April 4, 1990): 6–10 (report of Tom Riley).

    Greater participation by the United States in the deliberation of European data protection law could improve privacy protection in this country. For example, the Council of Europe convention on data protection provides a good model for data protection standards:

    Personal data to be automatically processed shall be: (1) obtained and processed fairly and lawfully, (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes, (c) adequate, relevant, and not excessive for the purpose for which they are maintained, (d) accurate, and where necessary, kept up to date, and (e) preserved in form which permits identification of the data subjects for no longer than required for the purposes for which those data are kept.

    Convention on Protection of Individuals with Regard to Automatic Processing of Personal Data, The Council of Europe, Strassbourg, France, January 28, 1981, quoted in Rein Turn, "Information Privacy Issues for the 1990s," *IEEE Symposium on Security and Privacy* (1990), p. 397.
35. Supra note 9.
36. Jerry Berman and Janlori Goldman, *A Federal Right of Information Privacy: The Need for Reform* (Washington, DC, Benton Foundation Project on Communications & Information Policy Options, n.d.).

37. P.L. 98–549.
38. P.L. 99–508. ECPA amends the Federal wiretap statue to prohibit the unauthorized interception and disclosure of electronic communications made possible by new technologies, such as cellular phones, electronic mail, and satellite television transmissions. The law defines electronic communications, restricts disclosure of stored communications, and creates civil and criminal penalties for individuals who, without authorization, willfully intercept or disclose the contents of electronic communications or who access such communications while in electronic storage. 18 U.S.C. 2510 et seq. (West 1989).
39. P.L. 100-618. Representative Al McCandless introduced the first video privacy bill in the 100th Congress, and subsequently testified in support of the bill that became the Video Privacy Protection Act. See The Video Privacy Protection Act of 1988, S. Rep. No. 599, 100th Cong., 2nd Sess. (1989), (testimony of Representative McCandless).