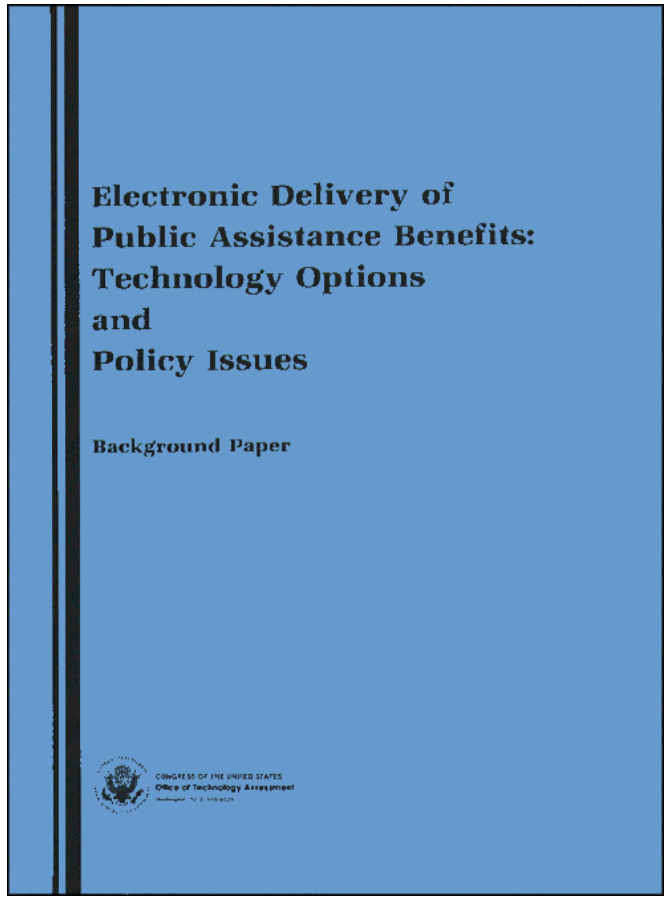
Electronic Delivery of Public Assistance Benefits: Technology Options and Policy Issues

April 1988

NTIS order #PB89-138911





Recommended Citation:

U.S. Congress, Office of Technology Assessment, Electronic *Delivery of Public Assistance* Benefits: Technology Options *and Policy* Issues, OTA-BP-CIT-47 (Washington, DC: U.S. Government Printing Office, April 1988).

Library of Congress Catalog Card Number 88-600544

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402-9325

Foreword

This background paper discusses the technological options available for use in an electronic system to deliver public assistance benefits, the privacy and security implications of such a system, and the programmatic effects of changing to an electronic delivery system. It was requested by the Subcommittee on the Handicapped of the Senate Committee on Labor and Human Resources. The paper built on research conducted for two earlier OTA studies, *Federal Government Information Technology: Electronic Records and Individual Privacy* (June 1986) and *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (October 1987).

Preparation of this background paper involved extensive assistance from and review by experts and other interested parties. OTA appreciates the participation of the many individuals who provided information and review comments. The background paper itself, however, is solely the responsibility of OTA, not of those who so ably advised and assisted us in its preparation.



U JOHN H. GIBBONS
Director

Electronic Delivery of Public Assistance Benefits: Technology Options and Policy Issues
OTA Project Staff

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

Fred W. Weingarten, *Manager*
Communication and Information Technologies Program

Project Staff

Priscilla M. Regan, *Senior Analyst*

Joan D. Winston, *Analyst*

Administrative Staff

Liz Emanuel, *Administrative Assistant*

Rebecca A. Battle, *Secretary*

Karolyn D. Swauger, *Secretary*

CONTENTS

	Page
Introduction and Findings	1
Background on Public Assistance Programs	3
Automation of Program Administration	3
Pilot Projects	4
The Food Stamp Program	5
Technological Options for Public Assistance Benefit Delivery Systems	7
Online v. Offline Systems	
Card Capabilities and Functions	8
Stand-Alone v. Piggybacked Systems	10
Privacy and Security Implications	13
The Privacy Ac tof 1974	13
National Identity Card	14
De Facto National Database	15
Computer Security Act of 1987	16
Programmatic Effects	18
Effects on Agency Staff and Operations	18
Effects on Providers	18
Effects on Clients	19
Conclusion	20
Appendix A: Reviewers and Other Contributors	21

INTRODUCTION AND FINDINGS

Within the next 5 to 15 years, it is inevitable that federally funded assistance programs will move to some form of electronic delivery system. Part of the impetus for such a change comes from government concerns for efficiency, especially in relation to detecting fraud, waste, and abuse, and for reducing costs associated with a paper-based, manual issuance and redemption system. Another part of the impetus comes from members of the financial and information service communities who seek new or expanded markets in State and local assistance programs. Decisions that may shape an electronic system are currently being made, i.e., computerization at the State level, technical standards, and policies for computer linkages between Federal agencies. These incremental decisions, made in a number of different policy arenas, are already establishing constraints on a future electronic system.

Any electronic issuance and redemption system would necessitate a reliable and secure identity card, a unique personal identifier, and a way of communicating information among various databases. These are the essential elements of a national database. Earlier proposals that have suggested the creation of an identity card for even a subset of the population, the creation of a unique numerical identifier that could be used for a number of purposes, or the establishment of a centralized database have been summarily rejected by Congress. Public opinion polls that raise these as possibilities have consistently drawn negative responses from an overwhelming majority of respondents. pro posals to create an electronic issuance and redemption system for public assistance programs would need to take into account the fundamental privacy and security concerns that have been raised in previous debates.

An efficient electronic issuance and redemption system may necessitate changes in the administration of public assistance programs, and the rules and regulations for program implementation. For example, because of economies of scale and scope, an electronic system may lead to the consolidation of the administration of a number of discrete public assistance programs. Moreover, an electronic system may involve changes in the relationship of Federal agencies to State and local agencies, as well as the relationship between the public sector and the private sector. Previous policy discussions on welfare reform should therefore be taken into account in considering proposals to create electronic systems for delivery of public assistance benefits.

In anticipation of a move to an electronic system, OTA has identified three key policy issues:

1. Which of a variety of technological options is most appropriate, given the goals that public assistance programs would want to achieve through use of an electronic system?
2. What are the privacy and security implications of such a system?
3. What are the programmatic effects of changing to an electronic system, including effects on agency staff, clients, and providers?

Although privacy and programmatic concerns are fundamental and must inform any policy discussion, an understanding of the technological options is necessary to understand the possible implications for privacy and security, as well as for programmatic administration.

Based on preliminary examination of these issues, using the Food Stamp Program as an example, OTA found that:

- If Government assistance programs were now to adopt an online electronic system using magnetic stripe cards, the system may become “old technology’ before full implementation. However, a coremitment now to a microchip smart-card system might be premature, not only for technical reasons but also because they are not yet in wide commercial use in the United States for credit cards or debit cards. Federal funding of the development of a large-scale benefit issuance and redemption system might provide subsidization for a private sector move to a smart-card system or other retail point-of-sale system.

- An electronic system for issuance and redemption of Federal benefits and services would be a significant component of a national database, and would, in effect, create a national identity card for many Americans. Privacy and security concerns would be raised as more personal information would be collected directly by third parties and exchanged without individual consent.
- An efficient electronic benefits issuance and redemption system may necessitate automation of all stages of program administration in order to be cost-effective. The consolidation of the administration of a number of eligibility benefit programs may also be necessary. To ensure that these decisions are not driven by the technology alone, program staff should be actively involved in design and implementation of an electronic system.
- An electronic system would entail social and practical, as well as technological, changes for clients, providers, and financial institutions. It would also involve retraining of agency personnel, and may involve some shifts in agency staffing, as well as more private sector involvement in program administration.

BACKGROUND ON PUBLIC ASSISTANCE PROGRAMS

There are more than 70 different Federal benefit programs that provide cash, goods, and services to people who meet eligibility requirements based on income level or need. These programs are largely (almost 75 percent) funded by the Federal Government, with funding for the remainder provided by States and localities. The programs are generally administered by the States and localities, in accordance with Federal guidelines that vary from very detailed to quite general. The major types of benefit programs include: medical (e.g., Medicaid, and Maternal and Child Health Services); cash (e.g., Aid to Families with Dependent Children (AFDC) and Supplemental Security Income (SSI)); food (e.g., Food Stamp and School Lunch Programs); housing (e.g., "Section 8" and public housing); education (e.g., student loans); jobs and training (e.g., under the Job Training Partnership Act); and energy assistance.[1]

The process by which these programs are administered is initially similar and begins when a potential client files an application. Following that, additional information is collected and the accuracy and completeness of client-provided information is verified, often through third parties or separate databases. Based on review of this information, eligibility and the level of benefits are determined.

After this determination, the administration of public assistance programs diverge markedly. Some, such as cash aid programs like AFDC and SS1, deliver benefits with the intervention of only one significant intermediary-the bank or similar entity that cashes the public assistance check–and place no restrictions on how benefits may be used. Others, such as "in-kind" programs like Food Stamps, require more than one intermediary -i.e., the provider of the good (the grocer), plus a separate entity to redeem the value of the food stamps (the bank, which is then credited by the Federal Reserve). Other examples of this type of **program** include Medicaid, and housing and energy assistance. This paper concentrates on these "in-kind" programs because they pose the more challenging questions in considering automation.

Automation of Program Administration

Much of the attention to date has been focused on automating the verification function —the process by which client information is cross-checked or matched with information in other databases. For example, under the Deficit Reduction Act of 1984, States are required to adopt a wage reporting system and to establish an Income Eligibility Verification System in order to check, in a timely and comprehensive fashion, the accuracy and completeness of information on clients of major benefit programs.[2] Increasingly, officials responsible for administering assistance programs are shifting their attention to the automation of the issuance and redemption of benefits. They regard this as a means of reducing the potentially large risks from lost, stolen, or diverted benefits. Additionally, they believe that automating will save postage, paper, printing, and administrative time in processing.

For the purposes of this paper, the administration of public assistance programs will be viewed as having five stages. A system could be designed to automate only the eli~"bifity *and benefit determination* stage of program administration. Automation of the *verification* of client provided information could be added to this system or created independently. Similarly, the automation of benefit *issuance security* (i.e., making sure that benefits are issued only to the eligible recipient) could be done as part of a larger automation effort or as an in-

[1] For a review of these programs see U.S. Congress, Congressional Research Service, *Cash and Noncash Benefits for Persons with Limited Income: Eligibility Rules, Recipient and Expenditure Data, FY* **1984-86,** CRS Report 87-759 EPW, Sept. 10, 1987.

[2] Departments of Labor, Agriculture, and Health and Human Services, "Income & Eligibility Verification Procedures for Food Stamps, Aid to Families with Dependent Children, State Administered Adult Assistance, Medicaid and Unemployment Compensation Programs: Final rule," *Federal Register,* vol. **51, No. 40,** Feb. 28, 1986, pp. 7178-7217.

dependent system. Additionally, automation of the *issuance* of benefits (i.e., distributing cash or in-kind benefits to the recipient) could be developed as part of a larger system or separately. Lastly, benefits issuance and *redemption* (i.e., crediting the provider for the value of a good or service) could be automated together or integrated into a comprehensive system.

This paper concentrates on new proposals for automating the issuance and redemption stages, or "back-end," of public assistance programs. At the present time, there is significant automation of eligibility and benefit determination, and verification of client-provided information. Automated, online integrated eligibility and benefit determination systems have been implemented in over a dozen States.[3] Although cost reductions that might be realized by integrating issuance and redemption with these "front-end" systems should be considered, this paper will not discuss these systems.

Pilot Projects

There are a number of pilot projects automating the issuance and/or redemption of public assistance benefits.[4] For example, New York State has established an Electronic Medicaid Eligibility Verification System in order to verify, at the time of issuance, clients' eligibility for certain treatments or medications. Ramsey County, Minnesota, has begun to use automatic teller machines (ATMs) and point-of-sale (POS) terminals to issue cash for certain public assistance programs.[5] Reading, Pennsylvania, has a demonstration project for food stamp issuance and redemption that uses magnetic stripe cards in conjunction with POS terminals installed in participating retail establishments to debit clients' benefit accounts, which are retained in a central database.[6] In this case, the computer system, its network, and its database are dedicated to public assistance programs. New York City has moved beyond the pilot stage and has set up an online Electronic Payment File Transfer (EPFT) program for issuance security for both food stamps and public assistance. EPFT serves 500,000 recipients and pays out $2 billion a year.[7]

Recent pilot projects have demonstrated the technical feasibility and relatively high acceptance of electronic benefits systems. However, data from these pilots have not yet demonstrated the cost-effectiveness of electronic systems for the governments issuing the benefits. Cost data are not yet available for the Ramsey County pilot; according to press accounts, the contractor for the system was anxious to test its transaction system and therefore charged the county a nominal amount for the first 6 months.[8] Ongoing administrative/operating costs for the Food Stamp pilot in Reading were shown to be several times higher per case, per month, than for the type of manual (paper food stamps) system most Food Stamp project areas use. This suggests that other efficiency measures, such as consolidation of several public assistance programs, might be nec-

[3] Many of these do not involve interactive processing by eligibility workers but rely on separate data-entry staff. FoodStamps Program *Operations Study Report on State Census: Automated Certification Systems (Final Report)*, Mathematical Policy Research, Inc., February 1987. Prepared for U.S. Department of Agriculture, Food and Nutrition Service under Contract No. 53-3198-5-51.

[4] For more detailed discussion Of pilot proposals see *Alternative Issuances and Delivery Systems*, U.S. Department of Labor, Office of Inspector General (President's Council on Integrity and Efficiency), July 1987, pp. 4-14.

[5] For a description of Ramsey County's pilot Electronic Benefit System (EBS), which began in June 1987, see: *Ramsey County Electronic Benefit System Evaluative Information*, Transfirst Corp., St. Paul, MN, November 1987.

[6] The online demonstration project began operation in early 1985 and was initially funded and administered by the Food and Nutrition Service (FNS) and operated by a third-party contractor (Planning Research Corp.). Although FNS' direct administration of the Reading project ended after December 1985, FNS extended the project for two more years. After a transition period, the Pennsylvania Department of Public Welfare took over operation of the Electronic Benefit Transfer (EBT) system in March 1986. See: *The Impact of an Electronic Benefit Transfer System in the Food Stamp Program*, Abt Associates, May 1987. Prepared under Contract No. 53-3198-3-103 with the U.S. Department of Agriculture, Food and Nutrition Service, Office of Analysis and Evaluation.

[7] Correspondence with Al Giove, Department of Social Services, The City of New York, Feb. 19, 1988.

[8] Amy Cohen Paul, "Welfare Benefits Issued at Automatic Teller Sites," *Government Computer News*, July 17,1987, p. 1.

essary to make the system cost-effective.[8] For other pilot projects, cost-benefit figures are not yet available.

The Food and Nutrition Service expects to conduct up to three new Food Stamp demonstration projects, and has solicited concept papers from interested State and local agencies. '" Because the Food Stamp Program is so large, because all the complexities accompanying provider involvement are present, and because it is a likely candidate for some degree of automation, a brief description of the program follows in order to provide a context for congressional evaluation of technological alternatives.

The Food Stamp Program

Because of the large number of households participating and large Federal expenditures involved, the Food Stamp Program has been suggested as a public assistance program in which large savings could be realized through electronic issuance and redemption. Proponents argue that retailers and recipients would also benefit from increased convenience, efficiency, and security because there would be no need to protect or handle paper food stamp coupons.

The Food Stamp Program operates in all 50 States, plus the District of Columbia, the Virgin Islands, and Guam. It is administered at the Federal level by the Food and Nutrition Service (FNS). At the State and local levels, the Food Stamp Program is administered by welfare offices that determine eligibility and issue, or supervise the issuance of, food stamps. FNS is responsible for the printing and distribution of food stamps (under strict accountability requirements) to the States. Through the Federal Reserve System, redeemed food stamps are converted to cash credits for food sellers' bank accounts.

The Food Stamp Act of 1977 (as amended) provides for 100 percent Federal funding of Food Stamp benefits and Federal administrative costs, and 50 percent Federal funding of most State and local administrative costs. State and local costs associated with computerization and fraud control activities are eligible for 75 percent Federal funding.[11] A 1985 law (Public Law 99-198) required the Department of Agriculture to develop a model computerization plan; at this time, this is being used to encourage State and local computerization of determination of eligibility and benefits, as well as computerization of verification of client-provided information. In 1987, estimated Federal Food Stamp expenditures totaled some $11.7 billion, including some $1 billion for Federal administrative costs and Federal matching of State and local costs. State and local expenditures were estimated to be about $0.9 billion. Average monthly participation was 7 million households (the typical recipient unit) with an average monthly benefit of $130 per household. "

According to FNS, at the end of fiscal year 1986, about 231,000 food providers were authorized to accept food stamps for purchases of eligible food items. Most of these (over 227,000) were retailers; the remainder were food wholesalers, meals on wheels, congregate dining or treatment facilities, etc. FNS statistics for atypical month (September 1986) show that, while supermarkets number only about 15 percent of those redeeming food stamps, they account for almost 74 percent of the value

[9] Abt Associates, op. cit., footnote 6. Now that the Project is being operated by the Pennsylvania Department of Public Welfare, the computer system used is being shared with other State data processing.

[10] Federal Register, 52 FR 35287, Sept. 18, 1987.

[11] U.S. Congress, Congressional Research Service, "How the Food Stamp Program Works, " by J. Richardson. CRS Report 87-806 EPW, Oct. 1, 1987. Program policies for Federal funding of State and local computerization activities are not intended to favor one technical approach over another (e.g., developing in-house computer facilities versus contracting with third parties for ADP services). However, some consider that formulas for 75 percent Federal funding of capital/development costs and 50 percent of operating costs might, on the margin, provide State and local authorities with more incentives to invest in in-house ADP facilities. Others consider that contracting out for large-scale systems may not be less costly in the long run and, moreover, that strong privacy concerns are raised by the prospect of third-party operation of Federal databases.

[12] Interview with J. Richardson, Congressional Research Service, Feb. 26, 1988.

of the redemptions (over $620 million out of a total of $842 million that month, or $17,448 per store). Small and medium grocery stores and convenience stores represent the majority of those redeeming food stamps (28 and 22 percent, respectively), but together these account for only about 16 percent of the value of the redemptions (per-store monthly averages of $1,592 and $585, respectively).

TECHNOLOGICAL OPTIONS FOR PUBLIC ASSISTANCE BENEFIT DELIVERY SYSTEMS

A public assistance card, with magnetic stripe and photo, used in a stand-alone, online public assistance system, is only one of several options. *[3] The other options vary according to:

- whether a real-time communications link to a central database is used to make a transaction;
- the card's storage medium and capabilities (magnetic stripe card, optical memory card, microchip "smart card, " or a hybrid of these); and
- whether the benefits issuance and redemption system is dedicated to one or more public assistance programs or shares an infrastructure with private financial transaction systems.

Online v. Offline Systems

In online systems, e.g., cash issuance via bank ATMs, magnetic stripe cards are used in conjunction with card readers and a telecommunication network. The readers (located with providers of a good or service) are Linked via communication lines (usually leased telephone lines) to a central computer database. For public assistance programs, this database would be the client eligibility and benefits database, either residing in the agency's computer or taken from the main agency files but held in a contractor's computer. A food purchase or other authorized transaction would result in a debit in the client account and a credit notation for the provider who could then redeem the value through one or more financial institutions.

Financial settlement in an online system can be accomplished through the Federal Reserve and/or Automated Clearing House (ACH) systems. At this time, there are two distinct types of commercial online systems: real-time systems, such as ATM systems, and batch systems, which treat POS transactions like "electronic checks" and use the ACH system for settlement.

In this paper, the distinction between online and offline systems hinges on whether or not telecommunication links to a central database are required to execute a transaction. In some of the online systems currently used for commercial transactions, the provider's bank account is settled periodically, rather than each time a transaction is executed.[14]

To execute a transaction in offline issuance systems, a smart card containing a microchip (that can have logic, as well as memory, functions) is inserted into a read/write terminal. With these systems, there is no requirement for a real-time communication link to a central database to perform a transaction. In a commercial system, for instance, the terminal would power the microchip in the card, read the balance in the chip's memory, debit the card for the amount of the transaction, and record a credit on the seller's card (or other memory device). In a public assistance system, the chip's memory would contain the benefits balance. For either type of system, the commercial seller or benefit provider would communicate periodically (again through telephone lines) with a central computer to record credits; financial settlement would be accomplished via the Federal Reserve and/or ACH systems. Communication links between the read/write terminal and central database would also be

[13] A comparative description of the features and capabilities of these various types of systems is contained in: *The Feasibility of an Electronic Benefit Transfer System for the Food Stamps Program,* Birch and Davis Associates, Inc. and The Orkand Corp., prepared under Contract No. 53-3198-1-139 with the U.S. Department of Agriculture, Food and Nutrition Service, Office of Analysis and Evaluation, 1982. This report found that a piggybacked online system using magnetic stripe cards would be most cost-effective because initial capitalization and operating costs would be shared with bank point-of-sale/debit card networks. Although some of the information in the report is now obsolete, it is likely that this finding is still valid.

[14] At present, there are regional procedures for online point-of-sale (POS) debit procedures and multiple payment systems. The two main online POS payment systems are those using batched settlement through the ACH system (treating POS transactions as "electronic checks"), and those in which real-time verification, reconciliation and settlement is possible (similar to cash withdrawals from customer accounts via bank ATM machines).

used to periodically update information in the chip's memory, including cash balance or benefit allotments. These links also would permit posting of "hot card" lists containing the numbers of lost and stolen cards.

The primary model for online delivery systems for public assistance programs is the banking system. A careful investigation of its efficiency and effectiveness may, therefore, be in order before government welfare agencies duplicate it, become integrated with it, or try to take the lead in development and deployment.

At this time, financial services providers (including equipment vendors, data processors, and electronic switch operators) and financial institutions (including major credit card companies) are exploring the feasibility and acceptability of an offline commercial system. They may, therefore, be looking for new users (e.g., government agencies) for their existing online telecommunication networks and central data processing centers. They may also be looking for noncommercial users (e.g., government agencies) to help finance an offline system. If either were to occur, it might spur more widespread commercial adoption of POS systems and increase their utilization via government-subsidized placement of POS terminals (e.g., in food stores in a debit issuance and redemption system for food stamps).

Card Capabilities and Functions

For electronic delivery of public assistance benefits, a card containing a magnetic stripe and photo is the less technologically sophisticated of the two options examined here.[15] The client photo would be used for personal identification; for enhanced security, the client could be required to enter a memorized personal identification number (PIN) via a keypad.[16] The magnetic stripe contains information (preferably encrypted) identifying the client and case file. The POS terminal contains a card reader and a keypad for the PIN. For public assistance programs, a printer might be necessary for receipts. Information read from the card triggers an inquiry via a communication link to a central benefits database to verify eligibility and/or transfer benefits to the recipient or retailer. The card itself is relatively inexpensive[17] and is thought to be functional for up to 2 years. For online issuance security andlor issuance of eligibility services (e.g., Medicaid) or lump issuance of benefits (e.g., food stamps or cash assistance), a magnetic stripe and photo card may be adequate. This type of card is now being used in New York State for issuance security and issuance of Medicaid program benefits, and for paper food stamps and cash issuance in several California counties.[18]

A magnetic stripe card can also be used in conjunction with a network that allows for transactional services. Then, benefits can be issued incrementally as the client needs them rather than in a periodic (e.g., monthly) lump sum as is done in the Food Stamp Program and most other assistance programs. The network for such a system is more sophisticated than that for issuance security alone. Additional expenses are the transaction fees to the

[15] This paper examines uses for magnetic stripe cards and smart cards, not optical memory cards. The latter could be used in online issuance security and/or issuance systems, but their comparative advantages lie in their relatively larger data storage capacity. There is growing interest in use of these cards for portable medical records, etc.

[16] The American Bankers Association (ABA) has issued POS guidelines covering physical card characteristics, customer identification, processing availability, operations requirements, backup and recovery operations, and security. These build on existing banking standards wherever possible. The ABA guidelines specify use of a customer PIN (rather than a signature) for identification. PINs stored on cards are commonly encrypted for security purposes. The ABA standards recommend use of the ANSI Standard X9.8 Data Encryption Algorithm for PIN encryption. (Guidelines for Online Debit card Systems at the Point of Sale, American Bankers Association, 1987). For more information about uses of data encryption in financial transactions, see: U.S. Congress, Office of Technology Assessment, *Defending Secrets,* Sharing Data: New *Locks and Keys for Electronic Information, OTA-CIT-31O* (Washington, DC: U.S. Government Printing Office, October 1987).

[17] A magnetic stripe card with photo costs less than $2, excluding the costs of photographic equipment and labor.

[18] For a review of pilots presently being conducted in eligibility benefit programs see: *Alternative Issuances and Delivery Systems,* Department of Labor, Office of Inspector General (President's Council on Integrity and Efficiency), July 1987.

terminal owner and to the operator of the telecommunication switch used to route transactions to the correct central database. These could be passed on to the client or absorbed by the public assistance agency.

Magnetic stripe cards can be counterfeited relatively easily and inexpensively—one National Bureau of Standards (NBS) expert estimates that a device for magnetic stripe 'skimming' (reading and capturing the information written on the magnetic stripe in order to transfer it to a counterfeit card) can be assembled with 100 dollars' worth of electronic gear. However, the photo and encrypted PIN would lessen some of this risk.[18]

Because of these difficulties with systems using magnetic stripe cards, banks and credit-card issuers are researching and testing smart cards. A conventional smart card contains a microchip that stores information. It can conduct transactions when inserted into a terminal containing a card reader/writer and a keypad for the PIN. Information on the card can be updated through a telecommunication system while the card is inserted into the terminal. Estimates of price ranges vary (and depend on assumed quantities), but from all reports, the costs of both the card itself and the interface terminal, or reader/writer, are decreasing.[20]

Proponents see several advantages to smart cards. A significant advantage of smart cards, despite their higher cost (in the $5 to $10 range), is that they are considered difficult to counterfeit. Another advantage is that telecommunication requirements are reduced. Additionally, security is increased because authorization of the transaction is performed within the card and reader/writer (rather than through communication to a central database and transaction processing center). For credit card applications, they can reduce credit losses, can be offered with a smaller credit line, and credit can be stopped more easily. Some experts consider that smart cards will be ideal for debit-card/POS applications.[21] However, use of smart cards may be less practical in programs, such as public assistance, that have a high client turnover or where cards must be replaced frequently.

Standardization of smart cards is a problem. In order to enable smart cards to work on any reader and to be used for more than one application, a committee of the American National Standards Institute (ANSI) is developing a standard for the location of contact points on smart cards and for a set of general commands for passing information between card and reader. Agreement on standards is probably 2 to 5 years away.[22] At present, Japanese smart cards meet different standards than those worked out by the International Organization for Standardization (1S0). Agreement on standards is moving slowly, probably more for political/proprietary reasons than for technical ones.

Interest in and use of smart cards is growing. They are increasingly used in the private sector in Europe. MasterCard has successfully conducted a small pilot program in the United States and is planning to extend its use of smart cards; Visa and American Express are expected to follow. Some experts at NBS consider that a general movement to use of smart cards as credit cards would be possible beginning in 1990, and that by 1995, it will be reasonable to implement a large smart-card network, enabling the financial industry to use offline smart-card debit cards (which would be periodically "loaded" with new balances online) .23 However, use of smart cards has lagged behind projections, in part because of uncertainties concerning standards.

[19] One report indicated that in 1985 MasterCard and Visa had a combined loss of $245 million due to counterfeit and other frauds. Jeffrey Kutler, "Consumers Receptive to Smart Cards and Anti-Fraud Measure," *American Banker*, Oct. 1, 1986.

[20] One vendor of smart cards and te l-minds suggested "quantity' prices in the $150-$300 range for a relatively simple smart-card terminal with PIN pad for POS use, and an additional $100-$500 for a printer. J. Esser, Schlumberger, personal communication, Mar. 2, 1988.

[21] Some "super smart cards," with their own small keypads for input/output functions, are also being tested for multipurpose card applications.

[22] 0TA staff interview with R. Warnar (NBS), Nov. 24, 1987. See also, *High Technology*, July 1986, p. 42.

[23] OTA staff interview with R. Warnar (NBS), Nov. 24, 1987.

In the civilian sector of the Federal Government, a number of pilot programs using smart cards for transaction or access control applications are currently being planned or conducted, including the Department of Agriculture's peanut quota program and tobacco price support program, and the FNS'S feasibility study for an offline Food Stamp demonstration project. There is also great interest on the part of defense and intelligence agencies, mostly for access control applications. Although most of the completed pilot programs have been termed successes in terms of technical feasibility and user acceptance, their costs have been high.

Magnetic stripe cards and smart cards require different readers and have different standard conventions for data storage. Therefore, making the transition from a system based on magnetic stripe cards to one using smart cards would require revisions to data center software to reflect new input formats and replacement of existing card readers. Also, while magnetic stripe cards are generally used only as "read only" cards,[24] use of smart cards implies extensive read and write capabilities (to update balances directly onto the card). For commercial credit card applications, there is already an extensive base of magnetic stripe card readers. Some foresee a "transition generation" of credit cards-with a magnetic stripe and a microchip-so that existing readers can be used during the transition to smartcard read/write terminals.[25]

[24]Some have noted that it is possible to use magnetic striPe cards with rewritable tracks in an offline type of system; however, most discussions of offline systems involve smart cards because of the technical limitations of read/write magnetic stripe cards.

[25]The proposed international ISO smart card standard is for a card with both chip and magnetic stripe, suitable for the transition generation. Dual terminals would be more expensive than magnetic-stripe-only terminals-a dual terminal for the transition generation, which can interface with a microchip and a magnetic stripe, currently sells for $500 to $1,000, compared with $150 to $300 for a magnetic stripe reader (not including printers). However, prices for dual card terminals can be expected to fall as the technology is refined and large numbers of terminals are sold. According to some, prices for ISO standard dual units may eventually be under $300 in large volumes.

Stand-Alone v. Piggybacked Systems

As *discussed* in this paper, a stand-alone system for public assistance programs would be one in which the cards, terminals, communication network, and information processing capabilities are dedicated to one or more assistance programs. A piggybacked system would be one in which major elements of the system (e.g., terminals, network and/or processing facility) are shared with commercial systems (bank ATM networks, retail debit-card/POS systems, etc.). In a piggybacked government/commercial system, the government would not bear the total cost. At the same time, the government would not have total control over the system.

Piggybacked systems might have lower total costs per transaction because of increased network utilization and shared capital costs for terminals and other equipment. If piggybacking were indeed to lower costs per transaction, then the cost-effectiveness of electronic issuance security and/or issuance systems for food stamps or cash benefits would depend on the status of the local commercial electronic transaction infrastructures (e.g., ATM networks, retail/supermarket POS systems).

As was mentioned previously, there are two distinct types of online POS systems. In a real-time online POS system, all the information to verify, reconcile, and settle the transaction is collected and recorded at the time the transaction is made. In principle, therefore, settlement between the customer's and provider's accounts can be done in real time.[26] By contrast, in the batch or "electronic check" type of online POS system, information to verify and reconcile a transaction is collected at the time the transaction is made. Batches of transactions are subsequently recorded in digitized

26 However, according to the American Bankers Association (ABA), net cash settlement between interchange parties (e.g., card-issuing institutions or networks) is often done periodically using a settlement agent (which may be a bank or ACH) and the Federal Reserve System. P. Brown, ABA, personal communication, Feb. 29, 1988.

form (e.g., on magnetic tape) and processed for settlement by an ACH. In this model, the card issuer or network does not have all the information necessary to settle the transaction until the transaction is "cleared" at the ACH.

One successful supermarket POS implementation, by Lucky Stores, is discussed below. This is a real-time online system piggybacked onto the existing banking ATM networks and retail POS networks. The online Food Stamp demonstration project in Reading, Pennsylvania, was a real-time system that used a local bank as agent for daily ACH settlement. This system was a stand-alone one and therefore did not offer the same potential for per-transaction cost reductions through increased volume and sharing of network infrastructure to better match volume and capacity .27

The American Bankers Association (ABA) published its guidelines for debit-card/POS in 1987, after a 2-year effort to build consensus within the financial and retail communities about the shape and form of POS systems.[28] The ABA intends these guidelines to foster the growth of POS networks at the local level and to encourage the development of national systems. The ABA guidelines describe an online, real-time POS system using magnetic stripe cards.

Some retailers and financial services providers have already established proprietary or shared debit-card/POS networks, sometimes in conjunction with credit card systems. The number of POS terminals is growing rapidly, although they continue to be outnumbered by ATM terminals.[29] By January 1988, according to *POS News,* about 41,000 POS debit terminals had been installed. Of these, some 15,500 had been installed by various major retailers, department stores, fast-food restaurants, and non-retail locations. About 15,700 had been installed by retail gas stations, about 8,400 by supermarkets, and about 1,600 by convenience stores.[30] Electronic Funds Transfer Association (EFTA) data show that, by mid-1987, an estimated 13,000 debit-card issuers had an outstanding debit-card base of some 160 million cards, mostly for ATM access; of these, perhaps 50 million could be used to access POS terminals. By comparison, EFTA statistics indicate that there were over 750 million credit cards outstanding in 1986, with MasterCard and Visa alone accounting for over 2.6 billion transactions that year.[31]

Safeway Stores, one of the Nation's major supermarket chains with 1,500 stores, conducted a year-long pilot program in Washington State and the Mid-Atlantic region, with an online debit system based on bank ATM cards. According to a Safeway representative, the chain concluded that implementing a nationwide store debit system could not be cost-justified at present. Lack of uniform debit regulations and national standards was considered to be one complicating factor for any multi-State POS system.[32]

Lucky Stores, a regional supermarket chain, began accepting bank ATM cards for food purchases in a few stores in 1984; by 1985, the trial had extended to 30 stores in California. Consumer acceptance was judged high, and in 1986, Lucky extended the POS system to

---

[27] Joseph S. Pendleton III, Meridian Bank (Reading, PA), personal communication, Jan. 20, 1988.

A description of the operation of the Reading demonstration system is given in chapter 2 of the Abt Associates report, op. cit., footnote 6.

[28] Guidelines for Online Debit Card Systems at the Point of Sale, American Bankers Association, 1987.

[29] According to the Electronic Funds Transfer Association (EFTA), the total number of operational ATMs was about 70,000 in mid-1987, installed by some 10,000 financial institutions. Of these ATMs, most now operate in shared networks. (EFTA Data Charts, Set No. 1, August 1987)

Financial institutions are not required to report the number of ATMs they have installed. Also, total cost data for private ATM operations are difficult to obtain and are not publicly reported.

[30] POS News, January 1988.

EFTA data showed some 32,500 POS debit terminals installed as of mid-1987. The 1988 data showed that the largest increases were for POS terminals in gas stations (6,600 increase) and supermarkets (1,500 increase). EFTA data show that the installed base of POS debit terminals was practically zero as recently as 1983. J. Callan, EFTA, personal communication, *Feb.* 24, 1988.

[31] EFTA Data Charts Set No. 4, December 1987.

[32] Melanie Hobden, Manager of Consumer Financial Services, Safeway, personal communication, Jan. 21, 1988.

325 California stores.[33] By 1987, 350 Lucky stores in California and Arizona were using the ATM debit system, which permits customers to purchase food and get up to $200 in cash. According to its developers, a real-time system is preferable because it offers superior control and flexibility and because new features (i.e., food stamps) can be added via software changes for a relatively low incremental cost—perhaps $100 per terminal.[34]

[33] Lee Paulson, Cetron Transaction Systems, Inc., personal communication, Jan. 22, 1988.

Lucky stores purchased its own telecommunication switch and is marketing the system to other stores through a subsidiary. According to its developers, the system can accept an estimated 90 percent of the ATM cards in California and processes some 1.5 million debit transactions per month. The system is an online, real-time debit system (like an ATM machine) rather than a batched online ("electronic checks") system.

[34] Ibid.

PRIVACY AND SECURITY IMPLICATIONS

Although the vast majority of Americans consider privacy to be a fundamental value, they do not view it as an absolute right. Its meaning for policy purposes is often unclear and its protection tends to depend on the particular context or situation in which it might be threatened. The Privacy Act of 1974 governs the practices of Federal agencies in handling personal information. The design of an electronic system for delivery of government benefit programs would need to take into account the principles of that act. But such a system would also represent a qualitative change in the environment of Federal agency practices—a change that is represented by the need for a plastic identity card and by electronic interchange of information between the public and private sectors. Earlier proposals that contained similar recommendations-the proposal in the early 1980s to have an identity card for immigration purposes[35] and the proposal in the mid-1960s to establish a National Data Center[36] –were rejected by Congress and the American people.

In addition to legal and administrative measures to ensure the privacy of individuals, a recent law requires agencies to employ appropriate physical and technical measures to protect personal information in computer systems operated by or for the Federal Government. The Computer Security Act of 1987 (Public Law 100-235) provides for the development of computer standards and training programs to protect certain unclassified information held in Federal computer systems. The act requires agencies to develop security plans to protect sensitive information held in computers and to train employees in security practices and procedures. The law's definition of "Federal computer systems" includes networks used for data communication between computers, and includes systems operated by contractors to process data on behalf of the Federal Government. The definition of "sensitive information" includes any information (not otherwise classified for national security purposes) the loss, misuse, unauthorized access to, or modification of which could adversely affect the national interest, conduct of Federal programs, or privacy to which individuals are entitled under the Privacy Act.[37] Therefore, public assistance programs would be subject to the provisions of the Computer Security Act.

The Privacy Act of 1974

Personal information in Federal agency databases receives some protection under the Privacy Act of 1974, which gives individuals certain rights in order to exercise some control over the content and uses of their personal information, e.g., the right to see and correct information, and to challenge secondary uses of information. The act also requires agency staff to handle personal information in a manner consistent with individual privacy, e.g., they must ensure that information is current and accurate, that information is collected directly from the individual, and that adequate safeguards are provided to prevent misuse of information. To ensure agency compliance with these principles, the act enables individuals to bring civil and criminal suits if information was willfully and intentionally handled in violation of the act. In addition, the Office of Management and Budget (OMB) was assigned responsibility for overseeing agency implementation of the act.

Although the Privacy Act was, in large part, a response to the perceived threats of computerized information systems, it was written

[35] See: U.S. Congress, House Committee on the Judiciary, Subcommittee on Immigration, Refugees, and International Law, *Immigration Reform and Control Act of 1983*, Hearings, 98th Cong., 1st sess., Mar. 1, 2, 9, 10, 14, 16, 1983 (Washington, DC: U.S. Government Printing Office, 1983).

[36] See: U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Invasions of Privacy* (Government Agencies), Hearings, 89th Cong., February 1965, June 1966 (Washington, DC: U.S. Government Printing Office, 1965-67); U.S. Congress, House Committee on Government Operations, Special Subcommittee on Invasion of Privacy, *The Computer and invasion of Privacy*, Hearings, 89th Cong., 2d sess., July 25,27,28, 1966 (Washington, DC: U.S. Government Printing Office, 1966).

[37] Public Law 100-235, Section 3.

in the context of manual record systems. By 1986, Federal agencies were using sophisticated computer and telecommunication technology, including microcomputers, computer matching of tapes of databases, online and offline computer-assisted front-end verification, and computer profiling. At that time, OTA reviewed Federal agency personal information practices and concluded that Federal use of new electronic technologies in processing personal information had eroded the protections of the 1974 Privacy Act.[38]

Most of these new applications were instituted as a part of the efforts to detect fraud, waste, and abuse, and to improve the efficiency of government programs. OTA found that neither Congress nor the executive branch was providing a forum in which the tension between these interests and privacy interests could be debated and resolved. Absent such a forum, agencies have had little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems. The proposal to adopt an electronic system for issuance and redemption of Federal benefits and services would provide an opportunity for open discussion of privacy and efficiency interests.

An electronic system for issuance and redemption of eligibility benefit programs would include many of the computer and telecommunication applications discussed in the 1986 OTA report. The problems discussed in that report would be intensified with such a system. It would also entail a qualitative change in the environment of privacy, in that it would require recipients to use an identity card and would involve widespread linking of public and private sector databases.

National Identity Card

The existence of a plastic identity card, irrespective of whether it is a magnetic stripe card or smart card, raises privacy and other civil liberties concerns. In order for a card to function as an identity card, it would need to contain some unique identifier and a means to authenticate the identity of the user of the card. A unique personal identification number (PIN), or combination of letters, numbers, and symbols, is an integral component of an identity card. This can be supplemented with a photo, fingerprint, or other biometric identifier.

Historically, Americans have been opposed to the government's initiation of an identity card, as they regard it as more in keeping with the needs of a totalitarian, or Big Brother, system of government.[39] Instead, Americans have preferred a number of cards for identification indifferent circumstances (e.g., driver's license, voting, health insurance, Medicaid, international travel, commercial credit, and Social Security). In theory, this more informal system enables the individual to keep the various parts of his or her private life separate. In practice, this system is becoming integrated because the social security number is increasingly being used as the numerical identifier on a variety of cards.

The most recent debate in this country on the creation of an identity card occurred in the early 1980s and was generated by the Select Commission on Immigration and Refugee Policy, whose mandate was to develop a means for controlling the employment of illegal aliens. One possibility considered by the Commission was to create an employee-identification card that would be given only to those who could supply documented proof of their status. The card was also to be difficult to counterfeit. Another possibility was to use the Social Security card as an identity card. These proposals drew heated criticism from across the political spectrum. Patricia Harris, then Secretary

[38] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy, OTA-C IT-296* (Washington, DC: U.S. Government Printing Office, June 1986).

[39] Louis Harris & Associates, Inc., and Dr. Alan F. Westin, *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy* (conducted for Sentry Insurance), December 1979; and Louis Harris & Associates, Inc., *The Road After* 1984: *A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium, December 1983.)

of Health and Human Services, summed up the criticism in saying:

> many people would interpret such an approach as a move toward a national identification document. . . our society has had a long history of opposition to the concept of a universal identifier, and I share this concern.[40]

The Iremigration Reform and Control Act that ultimately passed Congress did not include an employee identification card. Congress has, however, mandated a number of studies related to the issue of a national identity card. The White House was required by the 1984 Crime Control Act to study the need for a national identity document; the study was to have been completed in October 1987.[4]1 The General Accounting Office was required by the Immigration Reform and Control Act of 1986 (Public Law 99-603) to study ways to reduce the potential for fraudulently obtaining and using social security cards and to identify technological alternatives for making the card more resistant to counterfeiting.[42]

Discussions of an electronic system for distribution and redemption of public assistance benefits would likewise rekindle the debate about a national identity card. This is especially true given the likelihood that one card would be used in the issuance and redemption of a number of public assistance programs. If the Social Security system were to be part of an overall electronic system, the "national" nature of the card would be ensured. If the card were only used by recipients of eligibility benefit programs, then the card might stigmatize an economic and social subset of the population.

If a smart card were to be used in an electronic system for public assistance, additional privacy and security concerns would be raised. Unlike the use of these cards for some other applications, the use of smart cards in public assistance would still require a central program database in order to calculate benefits. Additionally, a decentralized database would be contained in the card's memory in order to execute transactions. The need for both a centralized and decentralized database, and periodic linkages between them for updating data, will require new procedures to ensure privacy and security. Furthermore, if one smart card is to be used for more than one purpose, it would be important to ensure that a Food Stamp provider could not access Medicaid information.[43]

De Facto **National Database**

The 1986 OTA report, *Electronic Records and Individual Privacy*, concluded that the widespread use of computerized databases, electronic record searches and matchings, and computer networking was leading rapidly to the creation of a *de facto* national database containing personal information on most Americans." Though a national database was not authorized by specific legislation, widespread use of data linkages led, in practice, to creation of such a database. Use of the social security number as an electronic national identifier was facilitating the development of this database. The data linkages examined in the OTA report were primarily among Federal and State agencies, with some private sector involvement by employers, credit agencies, and banks.

A *de facto* national database is actively being created, although in a piecemeal fashion. A significant step was the establishment of

[40]As quoted in Marvin Stone, "A National Identity Card?", *U.S. News & World Report,* vol. 89, Sept. 15, 1980, p. 88.

41"A Study on a National ID Card Falls Between the Cracks, " *Privacy Journal,* vol. XIII, No. 10, August 1987, p. 1.

[42]U.S. General Accounting Office, *Immigration Control: The New Role for the Social Security Card, GAO/HRD-88-4,* Mar. 16, 1988. GAO concluded that use of the social security card for employment eligibility verification, rather than use of a number of other identification documents (birth certificates, etc.), would be less susceptible to fraud. GAO recommended that the Social Security Administration adopt a card that was resistant to color copiers.

[43]Technological means for effecting some of these safeguards are within the current state of the art. However, it remains to be seen whether a given application would or could use them. See the 1987 OTA report, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* op. cit., footnote 16, pp. 68-69.

[44]The term *de facto* national database is used to distinguish it from a national database that was created by law, i.e., a *de jure* national database.

State Income Eligibility Verification Systems (SIEVS), required by the 1984 Deficit Reduction Act (DEFRA). SIEVS is used to verify information provided by the client during the application process. SIEVS contains wage and benefit data from State Wage Information Collection Agencies; wage, benefit, and other income data from the Social Security Administration; and unearned income data from the Internal Revenue Service (IRS) .45 Another database that can be viewed as part of a national database is the IRS Debtor Master File, which was also authorized in the Deficit Reduction Act. The File was created using information from the databases of a number of Federal agencies and was to aid in the administering of tax refunds to collect on delinquent Federal debts, such as student loans.[4G]

Electronic issuance and redemption systems for eligibility benefit programs would be significant components of a de *facto* national database, but they would also significantly change its nature. Most of the present data linkages occur within the public sector. If issuance and redemption of public assistance were added, this would involve private sector providers. Medical information supplied by doctors and hospitals could then become part of that database. Medical insurers would be part of the communication link in order to certify that Medicaid clients had exhausted their private coverage. Food stores could also be a part of such a national database, providing information on the buying habits of millions of Americans. Changes of this nature could increase the surveillance capabilities of the national database. These changes might also change public perceptions of privacy protections.

Computer Security Act of 1987

The Computer Security Act of 1987 (Public Law 100-235) assigns to the National Bureau of Standards (NBS) responsibility for developing technical, management, physical, and administrative standards and guidelines for the security of sensitive information in Federal computer systems, and for developing guidelines for training in security awareness and practice for personnel operating Federal computer systems. In assigning these responsibilities to NBS, Public Law 100-235 gives the National Security Agency (NSA) a technical advisory role—NBS can draw on technical guidelines developed by NSA to the extent that NBS deems them consistent with requirements for protecting sensitive information in Federal computer systems." A 1984 Presidential directive, National Security Decision Directive 145 (NSDD-145), had given to NSA primary responsibility for protecting unclassified, but sensitive, information in Federal computer systems.[48]

The security standards to be developed according to the Computer Security Act of 1987 are intended to assure "cost-effective" security and privacy: agency security plans developed according to the standards are to be commensurate with the risk and magnitude of the harm resulting from loss, misuse, unauthorized access to, or modification of, sensitive information in the computer systems.'[g]

The act requires each Federal agency to provide mandatory periodic computer security training for employees involved in the management, use, or operation of Federal computer systems within or under supervision of that agency. Because data on individuals subject

[45] At the Senate hearings on the Computer Matching Privacy Act in 1986, GAO reported that its preliminary study of SIEVS indicated that costs were greater than anticipated benefits, and that compatibility was a problem. U.S. General Accounting Office, Welfa.reeligibility - *Deficit Reduction Act Verification Issues,* GAO/HRD-87-79FS, May 1987.

[46] U.S. Department of the Treasury, Internal Revenue Service, "Privacy Act of 1974; System of Records," *Federal Register,* vol. 50, No. 195, Oct. 8, 1985, p. 41085.

[47] According to Public Law 100-235, the Secretary of Commerce is responsible for promulgating the standards and guidelines developed by NBS. The Secretary is authorized to make these standards compulsory and binding to the extent necessary to improve the security and efficiency of operation-or security and privacy—of Federal computer systems. Individual agencies may employ more stringent standards; conversely, these NBS standards may be waived if their application would adversely affect the computer operator's mission or not be cost-effective overall for the Government.

[48] For a discussion of NSDD-145 and Federal programs conducted pursuant to this directive, as well as a description of the policy debate surrounding the passage of Public Law 100-235 (formerly H.R. 145), see the 1987 OTA report, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* op. cit., footnote 16.

[49] Public Law 100-235, Sec. 2(b)-1 and Sec. 6(b).

to the Privacy Act fall within the purview of Public Law 100-235, agency personnel involved with electronic benefit systems would likely require periodic training. Moreover, the act requires each Federal agency to:

- identify the computer systems, and systems under development, within or under the supervision of the agency that contain sensitive information; and
- establish a cost-effective plan for the security and privacy of each system so identified.[50]

[50]Public Law 100-235, Sec. 6 (a) and (b).

These requirements would apply to agency computer systems used for automated preissuance functions or for electronic benefits delivery, or to such systems operated by third parties. Depending on the levels of security deemed necessary and cost-effective, any of a number of technical and administrative measures ranging from communications encryption to access control software for computer systems might be required.[51]

[51]For a discussion of some of these measures see the 1987 OTA report, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* op. cit., footnote 16.

PROGRAMMATIC EFFECTS

Effects on Agency Staff and Operations

In order for benefit programs to share overhead and operating costs of an electronic system for issuance and redemption, it is likely that the administration of a number of programs will be consolidated. For example, San Francisco had proposed the use of a public assistance card for authorization and delivery of AFDC, Food Stamps, Medical, Foster Care, Refugee Assistance, and Supplemental Benefits. This type of consolidation has been proposed before in various welfare reform proposals, and may well be beneficial for these programs. Most recently, the Low Income Opportunity Working Group of the Domestic Policy Council emphasized that public assistance programs constituted a system and should be treated as such. The Working Group suggested that some of the problems in welfare programs were caused by conflicting rules.[52]

If program consolidation is to take place, and if program goals are not to be compromised, the technology of benefit delivery alone should not drive this decision. The staff in specific program areas must be actively involved as the electronic system is designed and implemented. Consolidation of programs would require coordination of the numerous Federal rules and regulations that currently govern the administration of separate programs. Additionally, State and local implementing regulations would need to be taken into account. Requirements for determining eligibility may need to be made more uniform so that similar software can be used in a number of public assistance programs and in a number of jurisdictions.

A move to an electronic system would affect agency personnel. It may involve a shift in composition of the Federal and State workforce; it would certainly involve retraining, as a more technically literate workforce would be necessary. Depending on how an electronic system is designed, it may entail more private sector involvement in administering programs and in making decisions about eligibility. As contractors may be administering the system for eligibility verification and calculation of benefits, policies regarding confidentiality and liability may need to be revised.

[52]Domestic Policy Council, Low Income opportunity Working Group, *Up From Dependency: A New National Public Assistance Strategy (Report* to the President), December 1986, pp. 4-5.

Effects on Providers

Providers of goods and services (e.g., supermarkets under the Food Stamp Program and doctors under Medicaid) may welcome electronic systems because they may reduce paperwork and other operating costs, and/or enable them to get their accounts credited more quickly. These benefits will bean advantage primarily to large providers and vendors, who will be able to afford the capital costs of an electronic system[63] and the costs of training employees to use that system. In order that small providers and vendors are not disadvantaged, policy decisions about how to fund such systems will be important. Additionally, there needs to be wide geographic distribution of systems if providers are to serve clients in all areas.

For example, if the Food Stamp Program were to move to an electronic issuance system well in advance of general adoption of POS systems by food stores and other retailers, this would have a substantial impact on food sellers. In particular, requirements for special POS equipment and additional procedures might be resisted by food sellers because of their concerns with checkout productivity and because of tight space constraints in store operations.

If a stand-alone electronic Food Stamp issuance system were to be widely implemented, special terminals would probably be funded, directly or indirectly, by the government, and food sellers would have to provide space for them at checkout counters. Present Food

[53]For example, some supermarket representatives give "ballpark estimates" of capital costs for a checkout-lane POS system in the $400-$1,000 range per checkout terminal. Melanie Hobden, Safeway, personal communication, Jan. 21, 1988; and Lee Paulson, Cetron Transaction Systems, personal communication, Jan. 22, 1988.

Stamp policies, encouraging widespread access, restrain the government from passing on to food sellers the additional costs of automated food stamp redemption. (At present, food sellers do incur the labor costs of handling, sorting, and storing redeemed stamps.) The requirement that food sellers must be nondiscriminatory with regard to customers using food stamps (e.g., no segregated checkout lane or restricted shopping hours) would not necessarily require the Federal Government to place terminals at every checkout counter in a store. For example, terminals could be installed at selected counters, provided that these checkout lanes were open to all customers, not just Food Stamp clients. Still, if all food sellers currently participating in the program continued to participate, the total number of terminals required would number several hundreds of thousands.

Maintaining a dual (electronic and paper) system might save some capital costs, but would substantially reduce expected benefits from moving to an electronic system. If a policy were adopted placing terminals in large stores only, many food sellers and other providers would be shut out of the electronic system and clients might find it less convenient to use benefits. Alternatively, piggybacking electronic food stamp issuance onto an existing (or developing) POS system in food stores would lower the government's capital equipment and operating costs because equipment and networks would be shared with retail operations and other customers. Additionally, food sellers might be more receptive to installing equipment that could potentially be used by all customers.

If divergent Food Stamp Program and retail POS systems developed, with standards and protocols sufficiently different so as to pre vent shared equipment and network use, food sellers might resist giving store space to two sets of terminals. They might choose to stop participating in the program, making food shopping more costly or less convenient for Food Stamp clients.

If the Federal Government were to be a technology leader in this area and were to finance a stand-alone system before a commercial system was developed, this might speed the establishment of retail POS networks by a few years, but at some cost to the Government.

Effects on Clients

The move to an electronic distribution system will be a major change for clients of eligibility benefit programs. For many clients, a public assistance card may be their first plastic card and will raise numerous privacy concerns that are discussed above. For most clients, an automated system would entail their first use of a computer. The change to an electronic system will necessitate training of clients. But, the social changes for clients will also have to be addressed (e.g., no mail and less contact with program staff), as well as some practical aspects (e.g., convenience of locations and physical abilities of recipients). Additionally, not all clients speak English; the system will need to be designed so that non-English speaking clients can effectively access it. Software is now available to provide bilingual assistance for English./French and is being developed for English/Spanish. Asian language translations are more difficult because of different alphabets.

In a paper environment, clients have documentation for what they receive from the government and some means by which they can monitor their own transactions. In an electronic environment, clients may require similar tangible records so they can challenge an electronic data trail; thus, hardware costs may increase if special printers are required to provide receipts with Food Stamp balances. One source of fraud in welfare programs has been providers double-dipping for payment. In an electronic system for distributing eligibility benefits or services, similar transgressions could occur and clients would need to be able to challenge questionable transactions. A number of security features can be built into a smart card (e.g., passwords (PINs) and associated validation algorithms), and the card can be programmed to shut itself off if incorrect passwords are keyed. With a magnetic stripe, online system, these security features are built into the network infrastructure and rely on communication links.

CONCLUSION

The issues raised by proposals to move to an electronic system for delivery of public assistance benefits—which of a number of system objectives and implementations to choose, the consolidation of public assistance programs, appropriate private sector involvement in the welfare system, creation of a national database, and due process and privacy rights of clients-are fundamental. Before a national electronic system for issuance and redemption of welfare benefits and services is implemented, the policy issues discussed above must be addressed and resolved, with input from all of the affected parties. Otherwise—to the detriment of agencies, providers, and clients-the technology and the interests of the financial network providers (including hardware vendors, data processors, and network switching organizations) may shape the system.

The current interest on the part of Federal and State agencies and financial network providers creates an opportunity to design and pilot prototype systems. This would provide more information on the technological capabilities as they affect public assistance programs. More importantly, it would provide an opportunity to examine the effects on program administration and to incorporate privacy and security protections. Localized demonstration projects can be useful to familiarize public assistance agencies with technology trends and developments, to provide governments voice in the standards development process, to identify implications for program regulations, and to identify the needs of particular participant groups.

While pilot projects are being conducted, technological developments will continue. Although some large credit card issuers, businesses, and government agencies are testing smart-card applications, technical standards for smart cards, and for transition-generation cards carrying both a microchip and a magnetic stripe, are still evolving. When these standards stabilize (perhaps in the next 2 to 5 years), especially if a more broadly-based commercial point-of-sale infrastructure has emerged, the cost-effectiveness of various electronic issuance and redemption systems for widespread use in public programs can be more readily evaluated. At that time, the technical and financial uncertainties and risks to the government will be lower.

Some coordination in the design and implementation of pilot projects is desirable if the public assistance community as a whole is to benefit, and if these systems are to be capable of adapting to changing technology. Coordination will ensure that a number of prototype systems are tested across the country and will enable agencies in different States to learn from the experiences of others. This is critical if the end result is to be a national system. Although a national system may entail a number of different systems developed and managed locally, there will still need to be standardized data and communication formats for Federal administrative purposes.

APPENDIX A: REVEIWERS AND OTHER CONTRIBUTORS

Reviewers

Jerry Berman
American Civil Liberties Union

Peggy Brown
American Bankers Association

James Callan
Electronic Funds Transfer Association

Gary Chapman
Computer Professionals for Social Responsibility

Golleen Daly
Food and Nutrition Service (Food Stamp Program)

Elizabeth French
Community Human Services Development, Ramsey County

Al Giove
Department of Social Services, The City of New York

Nancy Grant
Grant & Bochicchio

Frank Haendler
Department of Labor

Allen Z. Miller
Electronic Data Systems Corp.

Kim Mitchell
Social Security Administration

Karen Myers
Electronic Data Systems Corp.

Carol Olander
Food and Nutrition Service

Gerald Patnode
New York State Department of Social Services

R. Lee Paulson
Cetron Transaction Systems, Inc.

Joseph S. Pendleton III
Meridian Bank

Joseph Richardson
Congressional Research Service

James Rule
State University of New York, Stony Brook

Miles Smid
National Bureau of Standards

Robert Warnar
National Bureau of Standards

Other Contributors

Michael Bulriss
Electronic Data Systems Corp.

Don Burrell
First Data Resources, Inc.

Melanie Hobden
Safeway Stores

Larry Ladouceur
MasterCard International

Benjamin Miller
Personal Identification News

Gertrude Satterwhite
Electronic Data Systems Corp.

Carol Stansfield
Food and Nutrition Service

John Vera
San Francisco Department of Social Services

OTA Reviewers

Jean Smith
Communication and Information Technologies Program

Charles Wilk
Communication and Information Technologies Program