Chapter 4

Privacy in Electronic Funds Transfer

Chapter 4

Privacy in Electronic Funds Transfer

Chapter Summary

Three principal concerns about electronic funds transfer (EFT) privacy have arisen:

1. the extent to which personal data in EFT systems are or might be disclosed to third parties by financial institutions;
2. the possibility of Government or private surveillance through EFT systems and data files; and
3. the right of consumers to see, challenge, and correct personal data in EFT systems that might be used, for example, to refuse them credit or in other disadvantageous ways.

However, EFT has not yet become a dominant factor in the marketplace, and people have readily available alternatives in carrying out financial transactions. Because of limited market penetration, EFT services so far have led to only minimal consolidations of financial data in any one system.

Some EFT services may not be quite as easy to avoid in the future. Employers may insist on direct deposit of payrolls, social welfare systems may insist on deposit of benefits, and mortgage companies and others may insist on automatically deducted payments. If EFT services become more pervasive, integrated customer files will be more common and public consciousness of the potential for invasion of privacy is likely to increase.

With increased use of EFT there will be a large number of points at which traditional norms of privacy could be invaded. More EFT terminals will be online, making electronic surveillance a more credible possibility. Single-statement reporting of all kinds of financial transactions will become common; more data will be aggregated and thus easier to access. At the same time, there could be broader and swifter dissemination of inaccurate data. Even if customer correction of data is facilitated, it will be more difficult for corrections to catch up with and replace faulty information.

In 1977, both the Privacy Protection Study Commission and the National Commission on Electronic Funds Transfer (NCEFT) recognized that privacy concerns could be especially strong in relation to EFT. NCEFT devoted 19 recommendations to means of protecting privacy.

Only a few of the NCEFT recommendations are reflected in the two EFT-related laws enacted since 1977—the Electronic Funds Transfer Act of 1978 (and Federal Reserve Regulation E) and the Right to Financial Privacy Act of 1978. For example, the use of EFT systems for surveillance purposes is not covered by existing legislation, but would be tightly restricted by the proposed Privacy of EFT bill introduced in the 96th Congress. Disclosure of EFT information to third parties is addressed only minimally by the EFT Act of 1978. However, the proposed privacy of EFT and fair financial information practices bills would provide much more detailed conditions and restrictions on third party disclosure. Even so, these proposed conditions are not as restrictive as some consumers would prefer, and neither one of these proposed bills was enacted in the 96th Congress.

Thus, the needs identified by the NCEFT for more comprehensive EFT privacy protec-

tion, whether through new legislation, modification of existing law, administrative procedures and regulations, industry standards, or some combination, are still largely unmet.

What is Privacy?

It is difficult to define privacy in a precise and concise fashion, even for those who express strong feelings about its value. In terms of information and recordkeeping (as opposed to personal association) it appears to mean, to most people, the ability to keep certain kinds of personal information from other people or to restrict its use, except as one freely chooses to permit its disclosure or use.

In a modern society, it is difficult to keep all personal information absolutely confidential. In practice, individuals generally seek to restrict some kinds of personal information to those who have a legally defined or socially sanctioned need to know, or to those who can provide some benefit or service in return.

There may be many reasons for wishing to withhold information about oneself, other than concern about Government encroachment on civil liberties. Information may expose one to censure or punishment; it may threaten one's reputation, social status, or self-esteem; it may give others some advantage or power over oneself, or lessen one's advantage over others in competitive situations. Information concerning income, debts, or financial transactions may in some situations do all of these things. This may explain in part why people are particularly sensitive to privacy when it comes to payment systems.

Some semantic distinctions may be noted for the sake of clarity. Frequently, privacy is regarded as an attribute of individuals and the focus is on those activities through which they are able to control and restrict access to personal information. The information so protected is "confidential." One way in which privacy can be violated is by illegal or unauthorized access to EFT and other telecommunication systems; the means used to protect the integrity of these systems, and hence the confidentiality of the information entrusted to them, constitute security (see ch. 5), However, the strong possibility remains that EFT systems and services themselves, through their normal functions and operations, may intrude on the privacy of users.

Privacy in Financial Transactions

Only transactions in which currency is the medium of payment can be accomplished with some degree of anonymity. Even then, evidence of financial responsibility often is required in order to obtain a service. For example, it may be virtually impossible to rent a car without presenting a credit card even if payment will be in cash.

When checks are used for payment, a record is created of the payor, the payee, the date, and the amount. In addition, documented identification often is required and various identifying numbers (e.g., telephone number, driver's license, credit card number, employee identification number) may be written on the check by the recipient. The person making payment provides this information willingly in order to have the payment accepted and to enjoy the convenience offered by a checking account. But checks are handled by human tellers and accountants, and the recipient of a check may sign it over to a third party in another transaction.

In order to obtain the further convenience of a credit card, customers are willing to provide additional personal information, such as place of employment, income level, and past financial history. As long as the information is used by the recipient only for the limited purpose for which it was intended, privacy is not usually considered to have been invaded because the information was provided by the subject in order to gain some benefit,

Financial institutions are compelled by law to keep some personal data. The Bank Secrecy Act requires that financial institutions keep copies of all checks over $100 and records of large cash transactions to protect the users of the system. In the same way, the Electronic Funds Transfer Act of 1978, and the Federal Reserve System's Regulation E that implements it, require that receipts issued by EFT terminals and periodic EFT bank statements indicate the date, time, and location from which a transaction was initiated (l).

Personal financial data are not found only within financial institutions and service systems. Employers have records of income, and personnel files may contain other information as well. Tax collectors receive reports of wages, interest, and dividends. Social service agencies have records of benefits paid to recipients. Furthermore, people are aware that credit-granting organizations, check and credit authorization services, debt collection agencies, and others collect information about an individual's financial history, both from the individuals and from a variety of other sources not always known to the subject or acknowledged by the collecting organization. People are less aware of the extent to which this information is shared among such organizations or sold to third parties for a variety of purposes, such as compiling mailing lists.

Generally people accept (not always without some irritation and concern) many acknowledged limitations on their privacy, not only because they may have no choice, but because they recognize that they derive substantial benefits thereby. For example, the increased acceptability of one's checks and the ability to obtain credit are benefits that depend on willingness to provide personal and financial information. The aggregation of data about many individuals provides other indirect benefits. Such data are useful for the efficient distribution of goods and services and the management of inventories. Market research may make it possible to design products to meet customer needs and wishes and to identify products that would be rejected in the marketplace, before resources are committed to production. Usually anonymity for individuals can be assured when data are aggregated. However, when data are collected under the expectation that they will be aggregated and then are used on a disaggregated basis (e.g., when survey data become the basis for direct telephone solicitation or lists sold to direct mail advertisers), this may well be considered a violation of privacy, if indeed the individual even becomes aware of the source of the solicitation.

What Constitutes a Violation of Privacy?

In payment systems, privacy is violated when data are, without the subject's nonsent, made available to and used by those not a party to the transaction, for purposes other than those necessary to accomplish the transaction. Those other purposes could range from organized market campaigns to Government surveillance to blackmail. If a person has neither explicitly nor implicitly consented to disclosure and use of information for a given purpose, personal privacy is considered to have been violated even if the same information was willingly provided by that person, either to another party or to the same party for a different purpose.

There is a second but closely related issue, which for convenience will be discussed under the umbrella of privacy. This is the obverse of unauthorized disclosure of information to third parties; namely, the ability of the individual to know what personal information has been collected and how it is being used. Just as the use of financial data for authorizing the acceptance of payments and the extension of credit is advantageous to the customer, the denial of such services because of erroneous or incomplete data represents a significant disadvantage. Thus, customers need to know what information is recorded about them and how they can correct inaccuracies.

In 1974, Congress passed the Privacy Act (2) to safeguard the privacy of individuals from the misuse of Federal records, to provide individuals access to their records maintained by Federal agencies, and to establish a Privacy Protection Study Commission. In this act the Congress explicitly recognized that:

> . . . the increasing use of computers and sophisticated information technology . . . has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information,
>
> . . . the opportunities of an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems, (and)
>
> . . . the right to privacy is a personal and fundamental right protected by the Constitution of the United States . . .

This act did not deal with EFT systems. However, the Privacy Protection Study Commission was instructed to:

> . . . make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the collection of personal information; and
>
> . . . recommend to the President and Congress the extent, if any, to which the requirements and principles of section 552a of title 5, United States Code, should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

The Privacy Protection Study Commission in its 1977 report (3) made several relevant recommendations, most of which have not been implemented. Briefly, they were that:

- data should be used only for purposes for which they are collected;
- subjects should be aware of the uses to which data will be put;
- there should be a proper balance between what an individual is expected to divulge (in connection with financial services) and what that individual seeks in return;
- recordkeeping should be monitored and open to scrutiny by the subject in order to minimize the extent to which information about an individual is a source of unfairness in any decision affecting him/her; and
- obligations with respect to the uses and disclosure that will be made of information about an individual must be established and defined.

EFT and Privacy

In many ways EFT can enhance the privacy of financial transactions. An automated teller machine (ATM) transaction is clearly more impersonal and anonymous than one conducted through a human teller. Electronic transactions cannot be signed over to a third party by the recipient as a check may be. Fewer people are involved in

processing EFT information than in check processing, thus minimizing disclosures due to curiosity or carelessness. The coding of information as electronic signals minimizes the possibility of casual or accidental perusal of information.

EFT includes a number of information-handling services. In some systems the information consists of orders to transfer funds from one account to another; in others the information is somewhat more diverse, and serves as a basis for deciding whether checks should be accepted or credit extended. In each case there is a collector, a conveyor, and a recipient/archiver of the data. The parties or systems filling each of these roles have specific and different needs with regard to the content and form of information, and different potentials for affecting privacy.

The collector obtains information, usually from the customer, and makes an interim record that is retained to provide the beginning of an audit trail to ensure system integrity (see ch. 5). The emphasis is on accurate recording. The data may be used not only to initiate a payment transaction, but also to support internal accounting functions such as inventory control and computation of commissions for salespeople.

Data are passed from the collector to the conveyor or communication link. The conveyor has little, if any, interest in the content of the data; the emphasis is on addressing and routing. However, the message content will be checked to ensure that it has been transmitted accurately. Copies of the data usually are retained for a time to add to the audit trail and ensure system integrity. Copies of data or audit trails sometimes are known as “data puddles;” that is, data that are collected to make the recordkeeping system work and to maintain accurate and secure records. The same controls and protections should be applied to these collateral data as to the records themselves.

Finally, the recipient or archiver receives and processes the data, and implements the transfer of funds or advises on the acceptability of payment or credit, Here the emphasis is on the substantive content of the message.

The collector, conveyor, and recipient/archiver need not be separate. When a retail store uses an electronic cash register connected to a computer to process a charge on the store's own account, it plays all three roles. When a customer uses a bank credit card at the same store, the store acts as the collector, the bank card association operating the communication network is the conveyor, and the bank and/or its processing agent is the recipient/archiver. Each operates under a different set of regulatory constraints that limit the services to be offered and the conditions under which they are offered. The points at which privacy may beat risk are basically the same (collection points, transmission points, and storage points), but the nature and extent of the risk may differ.

In general, there is greater concern about privacy with EFT than with older and more familiar systems for the following reasons:

- EFT makes it easier to collect, organize, store, and access larger amounts of data.
- More data are machine-readable and machine-processable, making them easier to manipulate and aggregate.
- EFT requires less time to record and to extract data; thus it is possible, in principle, to know the physical location of an individual as soon as he/she uses an ATM, or to know details of a transaction as soon as it is completed.
- Some EFT systems use keys such as account numbers, driver's license numbers, or social security numbers that might make it possible to find and integrate many sources of information about the individual.
- Compared to check processing, relatively few people would need to cooperate or conspire in order to violate privacy.
- The number of points at which data are retained may be larger in order to create a useful audit trail.

- Individual data can be organized and analyzed from multiple perspectives to obtain the maximum amount of intelligence.
- The inner workings of EFT systems are invisible to customers who have no way of knowing what information they contain, who is using it, and for what purposes.

In general, Americans may believe that banks provide more confidentiality for records than is the case. Good data are lacking on the extent to which banks protect the privacy of their customers. In 1979, 130 of the 300 largest commercial banks in the United States were surveyed on this question (4), Since only 34, or 26 percent, of the banks responded, the results are indicative but not conclusive:

– 20% routinely inform customers about the types of records maintained on them.
– 15% inform customers how this information would or could be used.
– 74% do *not* tell customers about routine disclosure of information to Government agencies.
– 85% do *not* inform customers about the possibility of disclosures to private sector entities.
– 88% tell customers the reasons for an adverse decision (e.g., *not* granting a credit line).
– 76% disclose to customers the information behind an adverse decision and its source.
– 36% will let customers see this information.
– 82% tell customers if the bank intends to seek information about them from a third party.
– 3070 tell customers the type of information that will be collected,
– 25% tell customers the source(s) that will be used for information.
– 5% tell customers how it will be collected.
- 90% collect some information without telling customers.
– 82% always supplement the information supplied by customers.
– 72% do *not* let customers see the information they collect.
—10070 get information from credit bureaus.
– 34% review the way in which the credit bureau gathered the data.
– 22% use investigative firms to collect information.
– 76% do *not* ask customers before disclosing personal information to third parties.
- 79% have a definite policy about what can be disclosed routinely to Government agents.
– 95% limit the type of information that can be disclosed to nongovernment entities.
– 61% do *not* require a subpoena.
— 58% do *not* have a policy concerning which bank employees have access to customer records.
– 52% allow individuals access to records about themselves, and
  — 86% of these allow the individuals to correct the records,
  — 67910 notify other organizations that have received the incorrect data that they have been corrected.

Based on these survey results, it would appear that the protection of privacy at many commercial banks is incomplete and spotty.

The Economics of EFT Privacy

EFT is one of the many technologies growing out of the convergence of computer technology, telecommunication technology, and the technology of information systems. These technologies have greatly reduced the costs of gathering and processing information. The information collected and stored by EFT systems presumably is necessary to the efficient operation of those systems, or is required by law for the protection of customers. Otherwise the costs of collecting and storing it, however small, would not be justified. Some of these costs can be partially offset by selling the data for other purposes, such as commercial mailing lists.

The value of some information depends on its immediacy (e.g., knowing that a credit limit has been exceeded at the moment when a credit card is offered), and some of it has a longer period of value (e.g., names and addresses). However, the value of most information degrades over time except when there is interest in compiling an historical record. The immediacy of access of EFT data adds greatly to their value.

Good information is lacking about the potential costs of enhanced protection of privacy. In 1979, the American Banking Association (ABA) studied 18 representative banks to estimate the potential costs of implementing the recommendations of the Privacy Protection Study Commission (5). The study concluded that costs would be considerably less to banks than to retail lending organizations, since banks already conformed to many of the recommendations as a matter of good business practice. The largest one-time or startup cost would be that of informing customers about institutional policies concerning disclosure and use of customer records. A mass mailing was assumed. However, the study pointed out that this cost could be reduced by including the information in regular periodic mailings to existing customers, and informing new customers at the time the initial relationship was established.

The major recurring costs would be informing customers of the reasons for an adverse decision, providing the information on which the decision was based, and allowing individuals to see and copy this information in order to challenge or correct it. There might also be additional litigation costs, since establishing a statutory right often leads to subsequent litigation. The ABA report indicated that recurring costs could be minimized by routinely informing customers about the basis of an adverse decision in the same letter in which the decision was announced, and honoring their requests "to see and copy" if additional documentation was necessary.

Concern About Government Surveillance

One of the concerns about EFT privacy stems from the fear that an unscrupulous government could use EFT (as well as other telecommunication systems) for surveillance of the population in the interests of political/social control (6). Assuming that there was the will to do so, and that political, legal, cultural, and ethical safeguards against such abuse of government power were weak, scenarios can be constructed in which EFT systerns could be used for surveillance. These scenarios would require the following assumptions:

- EFT systems would have to reach a level of use in which they process at least a significant proportion of all payment transactions,
- Organizations providing EFT services would have to be disposed—or forced

—to cooperate in establishing and operating a surveillance system.
- EFT terminals would have to operate in real time.
- It would have to be easier and cheaper —or at least perceived as such—to capture the desired information from EFT systems than in other ways.
- EFT systems would have to be able to capture enough data, in sufficient detail, to meet the requirements of those who seek the information.

Legal Protection of Privacy in EFT

Safeguards for protecting the security of systems are aimed at preventing misuse, destruction, modification, or disclosure of data (as well as theft of funds) as a result of attacks on the integrity of a system; that is, violations of customer privacy that are not initiated or concurred in by the system's designers, owners, manager, or operators (see ch. 5). The concern here, however, is with the possible threat to privacy from the system itself, operating normally; that is, the voluntary disclosure of information to Government agencies or to third parties in the private sector. This kind of protection will be, of necessity, mainly legal.

In 1977, the NCEFT surveyed existing legal safeguards for privacy and made 19 recommendations for further action. Since then, two laws have been passed related to EFT. The Electronic Funds Transfer Act of 1978 and Federal Reserve System Regulation E that implements it make little mention of privacy (7). The Right to Financial Privacy Act of 1978 (8) covers disclosure of records of financial institutions to Federal agencies, but not to State and local governments or to private institutions.

In addition, two bills have been proposed but not passed—the fair financial information practices bill and the privacy of EFT bill. The latter deals with information being transmitted over telecommunication links; i.e., data being passed from collector to recipient/archiver. It covers the records held by a service provider; however, the account records held by the financial institution are not covered.

Because the recommendations of NCEFT covered the outstanding issues regarding privacy and EFT, it is useful to consider how the new and proposed legislation responds to those recommendations. * This is shown in table 6.

Briefly, the two existing pieces of EFT legislation contain little that is directly related to the issue of privacy. What they do contain applies entirely to access to financial records by the Federal Government, which is allowed only under court order for purposes related to law enforcement. However, the EFT Act of 1978 does require that a customer, when establishing an EFT relationship, be fully informed about the financial institution's policies concerning disclosure of information. The act does not require that the customer be informed about specific disclosures or be given an opportunity to contest them.

The proposed fair financial information practices bill would create an "expectation of confidentiality" for information generated by use of EFT systems and services and would allow the customer to sue for damages if this expectation is violated. Disclosures that can take place without violating this expectation of confidentiality are listed. Both of the proposed bills strengthen the existing requirement that customers be fully informed about disclosure policies when subscribing to an EFT service. The proposed privacy of EFT bill also details the conditions under which disclosure of information

*These bills are discussed at length in Working Paper D.

Table 6.—Comparison of NCEFT Recommendations on Privacy With Present Status of Existing and Proposed Legislation

NCEFT Recommendations (Summarized)	Present status
1, Government should minimize the extent to which it requires an institution to maintain and report records about an individual using an EFT system, and should minimize the extent to which it requires Information to be collected that is not necessary to the operation of the EFT system,	Existing legislation, includlng the two proposed bills, does not deal with this recommendation, The EFT Act of 1978, Sec. 906, specified the data that must be given on EFT receipts and periodic statements and thus could be construed to limit the kinds of data that the Federal Government requires. However, the intent of this section was to provide consumer protection of another kind; namely, protection against error in recording of the transaction and against theft of funds. It IS aimed at designating minimum data to be collected. By the same token, however, existing and proposed legislation does not appear to violate the spirit of this recommendation.
2. EFT systems should 'not be used 'for surveillance of Individuals as to their location or patterns of behavior.	This subject is not dealt with by existing EFT legislation. The proposed Privacy of EFT bill restricts disclosure of information to Federal agencies except under court orders for purposes of law enforcement. According to an analysis by NTIA (Fact Sheet on Privacy in EFT Act) "... the growing use of EFT services, and the potential for surveillance of citizens which that use creates, necessitates effect we early steps to ensure that this new tool of commercial Intercourse is not misused for private or political prying into citizens' affairs. Whether surveillance is an ongoing interception of an individual's transfers as they occur, or an ex post facto recreation of all of an Individual's activities drawn from the records of an EFT service provider, this act effectively restricts disclosure by the service provider while permitting access for law enforcement purposes in appropriate circumstances. "
3. Legislation should be enacted to provide that the individual has a property interest in the data maintained by a financial institution about that Individual and that Government may get Information about depository accounts only with a subpena or administrative summons	The existing Right to Financial Privacy Act says-that an individual can contest such disclosures, but this is not based on a property interest, The fair flnanclal information practices bill creates a clear, legally enforceable "expectation of confidentiality" with regard to non-Federal organizat Ions, but this also does not rest on a property interest. However, the individual is given the right to sue for damages for a wolatton of the expectation of confidentiality. As it stands, this appears to apply only to violations by a financial institution and not to a nonfinancial institution offering EFT services. The privacy of EFT bill, however, covers disclosure to both Government and private organizations.
4, An individual whose account Information is sought by court orders should be given notice before the information is released (except under certain specified conditions).	This recommendation IS covered by the Right to Flnanclal Privacy Act of 1978,
5. The individual whose account Information is sought under court orders should have a reasonable time to respond and to contest such disclosures.	'Th-is-recommendation would be met by the Right to Financial Privacy Act of 1978. The customer has 10 to 14 days to respond.
6. Disclosure of Information should be made to third parties only: a) If necessary for the operation of the EFT system, or b) for a purpose of which the customer has been Informed and to which he/she has consented	This has not been addressed in existing laws which are both concerned with the relationship between the Federal Government and financial Institutions. The EFT Act of 1978, however, requires that when an account is opened the customer must be told "under what circumstances the financial institution will in the ordinary course of business disclose information to third person s." But there IS no guarantee that customers will be told about specific disclosures when they occur or that they can then contest them. The proposed fair financial Information practices bill has language about preservice notice and gives very detailed conditions under which information may be disclosed. Summarized, it provides for disclosure: • when permission is given by the subject individual. • when required by a Federal or State statute or regulation. • to Government, to defend the financial instltution against fraud, when there is evidence of illegal activities related to the account in question, or when the Government requests such disclosure under existlng laws. • to litigants, under provisions of the act.

Table 6.—Comparison of NCEFT Recommendations on Privacy With Present Status of Existing and Proposed Legislation—Continued

NCEFT Recommendations (Summarized)	Present Status
6, Continued—	• for purposes of marketing, if the customer has been offered and has refused an opportunity to object to the disclosure and if the information is disclosed by the third party recipient only to the subject, • to someone who is performing business or legal services for the financial institution, such as auditing. • to another depository institution, consumer reporting agency, or authorizing service. • to self-regulating organizations. • to the customer who is the subject of the file. The customer must be fully informed about these conditions for disclosure when the EFT relationship is established. The proposed privacy of EFT bill sets similar conditions for disclosure: • to a Government authority, pursuant to other laws. • to an officer of a financial institution, only to determine if a transaction was correctly carried out. • with specific authorization by one of the participants to a transact ion. • when the data are not identified with a particular individual, • if criminal activity is indicated.
7. There should be no disclosure to private sector third parties without specific authorization by the subject, and certification by the recipient that data will be used only for the designated purpose.	This is not covered by existing legislation, but see comments under *recommendation 6,* above, concerning the proposed fair financial in formation practices bill.
8. Information may be given to support organizations performing routine services for the financial institution, provided it certifies that it will maintain confidentiality.	This is not covered by existing legislation, but is covered by the proposed privacy in EFT bill, except that certification is not specifically mentioned,
9. Information may be disclosed to participants and intermediaries to a transaction; "intermediaries" include authorizing/guaranteei ng services.	This is not covered by existing legislation, but is covered by the proposed fair financial information practices bill. See comments under *recommendation 6,* above,
10. Information necessary to ensure the existence or good standing of an account may be given to credit bureaus and authorizing/guaranteeing organizations.	This is not–covered by—existing legislation, but is covered by the proposed bills. See comments under *recommendation 6,* above.
11. The credit pa-rt of an account (i.e., a line of credit or automatic draft privileges attached to an account) may be disclosed to other credit-granting or credit-authorizing organizations and other EFT organizations,	This is not specifically covered by either existing legislation or proposed legislat ion.
12, Information related to fraud and other crime can be disclosed to law enforcement officers, and customer delinquency or fraud can be disclosed to other EFT-offering institutions, credit-granting organizations, etc.	The first part of this recommendation is now covered by the Right to Financial Privacy Act of 1978, as well as by both proposed bills. The second part is not explicitly covered by either existing or proposed legislation.
13. Names and addresses may be provided for direct mail sol icitation unless the customer objects. The customer should be sent written notice that this may occur and be provided a simple means of objecting.	This is not covered in existing legislation, but would be covered by the proposed fair financial information practices bill.
14, Disclosure to any third party is permissible with express written consent from the subject.	This is-not covered by existing legislation. Both of the proposed bills cover it.
15. When establishing an EFT relationship the customer should be provided with full in formation about these policies.	This is fully covered by the existing EFT Act and Regulation E, and is also covered in the proposed fair financial information practices bill.

Table 6.—Comparison of NCEFT Recommendations on Privacy With Present Status of Existing and Proposed Legislation—Continued

NCEFT Recommendations (Summarized)	'Present Status"
16. Customers should have access to all recorded Information about them and be able to correct It.	This is not covered explicitly by existing or proposed legislation. The NTIA commentary on the proposed fair financial information practices bill nevertheless says: "Current law and practice already provide these aspects of information privacy protection in what appears to be an effective and workable manner. Provisions regarding customer disputes and correction of account information already exist under the Uniform Commercial Code and various State laws (for depository Institutions). (Customers are given additional access rights in other parts of the fair financial information practices bill. in title I, II, III, and V, regarding consumer reporting agencies. credit grants, check and credit authorization services, and insurance companies '")
17. Specifically, the Fair Credit Reporting Act should be amended to provide that: a) organizations that provide authorization/guarantee services are subject to the provisions that apply to credit reporting agencies, except for the requirement that the organization notify prior recipients of information that is later disputed and found to be of questionable accuracy. b) Institutions that decline to honor a check, debit, or credit presented by an Individual because of a report by an authorization/guarantee service should provide the customer with the name and address of the service c) The Individual has the right to Inspect. copy, and have Interpreted these records subject to certain condltions.	This is not covered by either existing or proposed legislation See comment under *recommendation 16,* above.
18. NCEFT used this recommendation to concur in two recommendations of the Privacy Protect Ion Study Commission, saying that EFT services should retain records only for a limited time, and should provide ways for the customer to correct records generated by EFT services NCEFT disagreed with the Privacy Protection Study Commission recommendation that no Government entity own, operate, or manage any EFT system handling transactions among private parties (e. g., Federal Reserve's ACHS)	This is covered in the discussion concerning *recommendations 6, 16,* and 17.
19, The Federal Reserve should follow rules at least as confidential as those of private sector EFT operators, and access by other Government agencies to ACH should be as restricted as access to other financial Institution records	As private sector EFT privacy practices are current ly mandated by law in only a rudimentary fashion, this recommendation is not fully applicable. According to the Federal Reserve, their policies are consistent with this recommendation, Records of transactions are held for a minimum period of time, and there are long-standing restrictive policies about granting access to information.

SOURCE Off Ice of Technology Assessment

does not violate the expectation of confidentiality. These conditions are not as restrictive as some customers would prefer; for example, a financial institution may provide certain kinds of information about customers not only to check-authorizing services, but also to credit-offering institutions (e.g., retail stores, credit card services, etc.) and other EFT systems; and may provide names and addresses of customers to direct mail advertisers and marketers unless the customer explicitly objects in writing.

Neither existing nor proposed legislation directly provides guarantees that customers may inspect, contest, and correct their records held by all EFT offerors. While the National Telecommunications and Information Administration argues that such rights are provided by other (non-EFT) legislation, it is not entirely clear that such is the case (9). The burden of proof with regard to the accuracy of records has not been clearly established through legislation. U.S. privacy laws (both existing and proposed) rely largely on the protesting citizen as the primary initiating and enforcement agent. Yet this assumes that financial institutions have diligently informed the customers about the content and use of their records. As the 1979 survey of banks shows, this assumption of good faith is not necessarily justified. New approaches to privacy protection may be needed (10).

Chapter 4 References

1. Title XX, Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-360, 2001, 92 Stat. 3641, codified in Consumer Credit Protection Act, 15 U.S.C. 1601,
2. 88 Stat. 1896; 5 U.S.C. 552a note; Public Law 93-579, Dec. 31, 1974. The first quotation is from the preamble.
3. Privacy Protection Study Commission, Per*sonal Privacy in an Information Society (1977).*
4. David Linowes, *A Research Study of Privacy and Banking* (University of Illinois, 1979).
5. Touche Ross & Co., *Priuacy Protection Cost Study (1979).*
6. For example, the Sentry Life Insurance Company conducted a study entitled "The Dimensions of Privacy" (1979) which indicated that 48 percent of Americans are worried about how the Federal Government will use personal information it gathers. See *also* Working Paper D: The Irvine Research Corp., *An Assessment of Equity and Privacy Issues in Electronic Funds 'Transfer Systems* (September 1980), pp. 100-105.
7. The Electronic Fund Transfer Act (EFTA) and Regulation E merely require that a financial institution's policies concerning the circumstances "in the ordinary course of business" under which it will release information about the consumer's account to third parties be disclosed to the consumer. Some practical implications for personal privacy have, nevertheless, resulted from this law.

   Reg. E's model disclosure clauses suggest that the "ordinary course of business" at the very least means: 1) when it is necessary to complete a transfer, 2) in order to verify the existence and condition of the consumer's account such as for a credit bureau or merchant, 3) in order to comply with governmental agency or court orders, or 4) with the consumer's consent. Many financial institutions have routinely copied the model clauses into their disclosures, thereby creating a contractual obligation to the consumer to handle information in the manner prescribed "in the ordinary course of business. " A consumer could also bring a suit under the EFTA if the financial institution violates the law's disclosure requirement. This is considered by some experts to be an important protection of personal privacy. (Sept. 9, 1981, letter to OTA from Fred M. Greguras, Kutak, Rock & Huie.)
8. Title XI, Public Law 630, 12 U.S.C. Sec. 3401 et. seq. See Working Paper D, App. D, p. 4.
9. Robert C. Zimmer and Theresa A. Einhorn, *The Lauj of Electronic Funds Transfer (Washington,* D. C.: Card Services, Inc., 1978), pp. 23-31 ff.
10. Donald A. Marchand, "Privacy, Confidentiality and Computers: National and International Implications of U.S. Information Policy, " *Telecommunications Policy,* September 1979.

    Also, the recent adoption of the Organization for Economic Cooperation and Development (OECD) guidelines for personal privacy could be an important factor in future congressional policy determinations. In September 1980, the OECD, to which the United States belongs, adopted guidelines that recommend basic principles of fair information practices and urge nations to remove or avoid creating obstacles to international data flow in the name of privacy protection.

    Under the guidelines, OECD members may restrict data flows to countries that do not substantially observe the fair information

practices principles. Because the United States does not have privacy laws corresponding to those of many OECD nations, expecially European countries, the U.S. Department of Commerce is recommending voluntary compliance as the best means of avoiding restrictions on international data flows. One possible consequence of not adopting the guidelines is that other nations could limit the flow of personal and commercial data communications with the United States, which in turn could be a primary impetus to enacting more comprehensive privacy legislation in this country. (Sept. 9, 1981, letter to OTA from Fred M. Greguras.)