<LA7

Passing the Digital Buck:

Unresolved Social and Technical Issues in Electronic Funds Transfer Systems

Rob Kling

Department of Information and Computer Sciences
and
Public Policy Research Organization
University of California
Irvine, Ca 92717

April 20, 1975

Draft #2

Revised: 6-29-76 11:30 AM

ICS-TR #87
PPRO WP- -76

Notice: This Material may be protected by Copyright Law (Title 17 U.S.C.)

ABSTRACT

Over the last decade, plans for using computer-based sytems to automate the transfer of debits and credits have moved from a technologist's pipe dream to an emerging reality. During the last few years, several components of this technology have been developed in prototype form and have begun to be implemented on a large scale. While such systems promise financial benefits for the institutions that exploit them, they also raise significant social, legal, and technical questions that must be resolved if full-scale Electronic Funds Transfer Systems (EFTS) are not to cause more problems for the larger public than they solve. Few of these problems have been systematically articulated. This paper describes the mechanics of EFTS, and the benefits it should provide its promoters. But it emphasizes a variety of the problems that EFTS raises and places them in context.

Acknowledgements:

I would especially like to thank Paul Armer and Dan McCracken for their continuing support of this study and their helpful comments on earlier drafts. Paul Armer provided a wealth of documentary material on EFTS without which this report would have been less comprehensive and accurate. In addition, Robert Abbot, Bernie Galler, Lance Hoffman, John King and David Smith provided helpful readings of early drafts. However, the analyses developed here do not necessarily reflect their views.

What are EFTS and What Issues Do They Raise ?

During the last decade, an assortment of bankers, other members of the financial community, and computer specialists have been talking about plans for payments systems based on electronic impulses rather than paper checks, money, credit card chits, and receipts. Such systems promise to cut the cost of paper processing*, to reduce petty theft, and support convenient add-on services such as automatic payroll deposits.

The various Electronic Funds Transfer Systems (EFTS**) that

---

* Checks alone were estimated to cost $5 billion to process in 1973 [11].

** Electronic funds transfer systems comprise those technologies that are used to transmit credits, debits, or related information pertaining to business transactions by technologies that combine computing and communications. The term is used rather loosely and is applied to a wide variety of computer-related technologies that are being used by banks and businesses to massage and store information pertaining to business transactions.

would support such services include networks for automatically clearing checks while debiting and crediting individual accounts, directly debiting and crediting individual bank accounts from point of sale (POS) terminals in retail stores, and providing cash on demand 24 hours a day through "automatic tellers." While scenarios of cashless and checkless societies encourage one to imagine integrated nationwide networks, it remains a fact that different components can operate feasibly without such large scale integration. Currently several of these technologies are being used, independently of each other, in some prototype form. of each other.) BankAmericard for example, has installed a nationwide network to transmit electronic credit receipts. Dozens of banks have installed automatic tellers. And about two dozen savings and loan associations are experimenting with POS terminals linking supermarkets and department stores to individual bank accounts. At this time, however, there are no networks which automate the processing of checks between individual accounts at different banks.

Several dozen major financial institutions, government agencies, and computer vendors are developing EFTS technologies and their associated administrative frameworks. It is a fast-moving "social world" [22] in which events outpace rumors of events. Thus some of the particulars cited in this paper may be dated by the time it is published.

Full-scale EFTS form a complex social and technical system. The literature describing different aspects of EFTS has grown at an enormous pace during the last few years and is extremely fragmented. Most of the articles address the interests of financial, business, and technical groups that would directly benefit from different EFTS arrangements. Unfortunately, no single analyst seems to consider a broad range of problems that likely will occur if EFTS are haphazardly implemented*. This is due in part to the sheer complexity and variety of issues that EFTS raise. Few specialists can write authoritatively and with insight about the technical, economic, regulatory, legal, and social aspects of EFTS. In addition, most of the people who have the opportunity to become intimately involved with EFTS, and who are knowledgeable about the issues raised, owe their intimacy to working with some enterprise which has a particular stake in a particular form of EFTS development. These commitments help create a literature in which analysis and advocacy are subtly intertwined.

Most analysts view EFTS as an "economic instrument" whose costs and benefits may be assessed more or less directly in dollars**. This paper views EFTS as both an economic and "political instrument." As a

* See [3] for a rare exception.

** See [10] for an exception.

political instrument, it may induce important shifts of social power, which because they are intangible compared to monetary shifts, are difficult to analyze. As we shall see later, EFTS developments exacerbate major value conflicts in this society. It may well turn out that the mechanisms that we choose to control our debiting and crediting may lead to profound consequences for our life styles and our political system.

Automated check processing systems have been especially attractive to the Federal Reserve Board (Fed) which has sponsored several pilot projects to test the technical and economic feasibility of EFTS. In November, 1973, the Fed circulated a proposal that would give it statutory power to administer a national EFTS [14]. If the Fed proposal is enacted by Congress, it will enable the Fed to develop a nationwide automated check processing network within the next few years. Unfortunately, no specific technological proposal accompanied the "management" proposal circulated by the Fed. As we shall see, the magnitude of some of the problems that EFTS might induce are difficult to appraise without reference to specific technological and institutional implementations.

While the laissez-faire development of EFTS could produce significant social problems, EFTS and their consequences have aroused little public interest in the United States. While EFTS, have received scant attention by the media, Congress in 1975, set up a National Commission on EFTS primarily to study the possible financial impacts of automated payments systemson our financial institutions.

Advocates of EFTS emphasize economic benefits. EFTS are portrayed as a natural extension of the credit card in which debits and credits are rapidly flashed through a network akin to an airline reservation system. The technology is described as one in which most participants gain*. However, the major social problems that EFTS might engender continue to be neglected systematically neglected. These problems include:

1. Invasion of individual privacy since most EFTS provide a medium for easily monitoring a person's business and personal affairs
2. Large scale theft by "computer sophisticates" who break the system security
3. Sabotage of a large-scale interdependent system like EFTS could seriously harm the American economy
4. Substantially reduced competition within the financial industry (and the development of a few "superbanks")
5. "Credit blackouts" that could paralyze the economy within small geographic regions for several hours at a time
6. Unobtrusive Real-time surveillance of people by government agencies using mundane business transactions to probe of their activities

* See [8] for an example.

These six examples illustrate some of the problems must be solved before certain EFTS such as automated check clearing systems are implemented.

The remainder of this paper is organized into five sections that describe:

1. Mechanics of electronic debit processing systems
2. Major value positions that already influence EFTS developments, or will be influenced by EFTS developments
3. Benefits EFTS might provide
4. Some key social and technical problems posed by EFTS and what we know about their potential resolution
5. Open issues that are induced by EFT developments

Sample EFTS:
Automated Check Processing and Point of Sale Networks

Since automated check processing systems (ACPS) exhibit rich behavior, while illustrating both the primary benefits and deepest problems of EFTS, their features will be elaborated in detail. Unfortunately, definitive description of automated check processing operations is impeded by the absence of detailed, comprehensive proposals in the literature [3,7,9,12,13,14,26,37]. And, it is likely that several EFTS exist that are independently designed but highly

coupled EFTs [26]. Thus, the mechanics presented here are simplified. To aid the exposition, ACPS operations will be contrasted with the mechanics of the current (non-electronic) check processing system.

Consider the following example of the current payments system: John Doe, a resident of Los Angeles, wishes to purchase a book by mail from a small publisher in New York City.

1. John Doe deposits sufficient funds in his checking account at Old Gold Bank (in Los Angeles) to cover the cost of purchase.
2. He mails a letter to the publisher's sales department describing his purchase and encloses his check.
3. If the book is in stock, the publisher mails it to Los Angeles and deposits Doe's check in his local bank account in New York City at Midas Trust.
4. Midas Trust deposits the check for credit in the Federal Reserve Bank of New York City.
5. The Federal Reserve Bank of New York City sends the check to the Federal Reserve branch in Los Angeles for collection.
6. The Federal Reserve branch in Los Angeles forwards the check to Old Gold Bank which will deduct the amount from Doe's account.
7. Old Gold authorizes the Federal Reserve branch in Los Angeles to deduct the amount of the check from its deposit account with the Federal Reserve Bank.
8. Old Gold microfilms the check and adds the filmed copy to its check archives. (The physical check is collated with Doe's other checks and returned to him with his monthly statement.)
9. The Los Angeles Federal Reserve branch pays the New York Federal Reserve Bank through the "Interdistrict Settlement Fund."
10. The New York City Fed Bank credits Midas Trust.
11. Finally, Midas Trust credits the publisher's account.

Transfers 2 through 7 are accompanied by the physical movement of Doe's check. In this example, the check passes through 4 banks.

Proposals for automating check processing [9,11,31] seem to agree upon the following "truncated check flow" mechanism. Steps 1, 2 and 3 of the preceding scenario would be identical with ACPS. However, when the publisher's bank receives Doe's check, it is converted into an "electronic message." This message would have to include such information as amount of check, issuing bank, Doe's account number, and name of payee. The publisher's bank ("bank of first deposit") would microfilm the check for its own records. After some (unspecified) period of time, it would destroy the physical check written by Doe. Thus, the message generated from the check will have to include sufficient information to route payments through the network identified in the preceding scenario and to allow Doe to audit his account with Old Gold.

The pattern of check payments in ACPS parallels that of the current payments system sketched above. However, the funds transfer indicated in steps 4-6 and 8-11 would occur by passing the electronic message which "represents" Doe's check between the respective banks.

Doe will still receive his monthly statement from Old Gold. However, instead of receiving each check that was debited against his account, he would receive an annotation on the statement indicating the date the check was issued, to whom, etc.

This "truncated check flow" is the heart of ACPS. In the current payments system, an electronic medium called Fedwire is used for transferring sums that exceed $50,000 between banks. However, Fedwire has no provision for carrying messages that index particular checking accounts in specific banks. In contrast, the "truncated-check-flow" system links banks in a "two-tier" arrangement. There is a network between the various Fed banks, forming one tier. Other banks link to the network through their regional Fed bank, forming a second tier.

Given such an arrangement, it is relatively straightforward to add a "third tier"--point of sale terminals-- to ACPS. These would enable a merchant to directly debit the bank account of a consumer for the amount of purchase. These terminals could operate in "real-time" as a consumer waits at a check-out counter, providing that such transactions can be expedited conveniently within a minute or two.

ACPS provides a good example of what EFTS entails. However, the EFTS technologies that are currently emerging actually bypass ACPS as it is described above. For example, as of July, 1975, approximately two dozen savings and loan associations had developed experimental links between POS terminals in individual stores and individual accounts in their own banks [27]. Since, savings and loan institutions were unauthorized to provide checking accounts at that time, these systems simply linked stores and banks. During the last year BankAmericard has implemented its own system (BASEII) to process electronic copies of its charge card receipts. Again, this system does not link to an ACPS and seems to operate economically without

such linkage. It may turn out that the largest volume of electronic transactions during the next decade will be processed via a sales-related network rather than through an ACPS arrangement.

Currently, progress on ACPS development seems to be coming through the Federal Reserve Board's regional "automated clearing houses" and regional committees on paperless entries which are organized by and for commercial banks. They were also prevented from participating in most of the regional clearinghouse activity by the (competitive) commercial banks. Thus, their experiments with EFTS focussed upon automated tellers and systems that directly link POS terminals to accounts in particular banks. The thrift institutions have been lobbying for authorization to issue regular checking accounts. No doubt they will gain some role within these regional clearing arrangements if and when and will also promote automated check processing systems. when they provide checking accounts. Then, they will also promote ACPS.

Value Issues in EFTS Operations

People respond to EFTS in terms of their institutional commitments and values. At least six major value orientations seem to be implicit in the discussions of EFTS cited throughout this report. In different instances, these positions may be mutally supporting, in sheer conflict, or independent of each other. Each of them, except the "systems model," has a large number of supporters and a long tradition of support within this country. Thus, EFTS developments which are congruent with any of these positions might be argued to be in "the public interest."

1. A Free Enterprise Model: The preeminant consideration is profitability of the EFTS with the highest social good being the profitability of the firms controlling the systems. Other social goods such as users' privacy or the need of the government for data are secondary.

2. A Statist Model: The strength and efficiency of state and government institutions is the highest goal. Government needs for access to personal data on citizens and needs for mechanisms to enforce obligations to the state would always prevail over other considerations [34].

3. A Libertarian Model: The rights of the individual form the greatest good. Other social purposes such as profitability or welfare of the state would be sacrificed should they conflict with the prerogatives of the individual [34].

4. A "Populist"** Model: Major societal and governmental institutions should remain within the understanding of ordinary citizens and be responsive to their needs. Societal institutions should emphasize serving "the little man."

5. Systems Model: The main goal is that EFTS be well organized, efficient, and reliable. Should conflicts arise between convenience of use and efficiency or between privacy concerns and system efficiency, concerns for efficiency would remain paramount.***

** This position is also close to the spirit of Jeffersonian democracy and the sensibilities of Common Cause, the "citizen lobby."

*** Traditionally, "efficiency" is viewed as the relative effectiveness of some means in achieving some end for a fixed expenditure. Thus, in classical terms, efficiency would not be an end in itself. However, in both management science and computer science, efficiency per se has become an end. For example, computer scientists are skilled at answering questions such as "How fast can I sort a list?" rather than "What social goods do I achieve by sorting this list ?" [23].

6. A Conservative Model: Curtailing the potential for bureaucratic control is the greatest good. Any development of EFTS is considered too dangerous to personal privacy and autonomy [34].

Perceptions of benefits and problems depend upon one's values and commitments. For example, diminishing the cost of check processing is congruent with the free enterprise position articulated above, but is indifferent to "libertarian" and "populist" positions. EFTS have been most forcefully advocated and developed by groups that represent predominantly "free enterprise" and "statist" interests As we shall see, EFTS pose the greatest problems for "libertarian" and "populist" sensibilities.

The following three sections highlight some key benefits that advocates of EFTS claim will result, some of the major technical problems that might impede successful EFTS developments, and some of the social problems that large scale EFTS might induce. Since most of these problems hinge on value conflicts that are exacerbated by EFTS developments, it is unlikely that they will be "solved." Rather, different EFTS arrangements (other than no ACPS and national POS networks) will simply tend to favor one value position more strongly than another. Thus, EFTS may well be viewed as new sources of social tensions. The magnitude of these tensions will depend upon the extent to which these different value positions are held by members of the larger society and the extent to which various EFTS arrangements admit compromises acceptable to major parties.

The Benefits of Digital Bucks

EFTS are advocated by major banking institutions and other promoters [8,9,12,19,25,31] as providing a variety of economic benefits for its users. This section examines many of these benefits often claimed for EFTS.

A. Reduction in Cost of Check Processing

Approximately 28 billion checks were written on demand deposit accounts in the United States in 1974[3]. During the '60's check use grew at about 7% per annum. While there is no direct evidence for computing the rate of increase of check use in the '70's, the available evidence is congruent with a similar rate of growth. At this rate of growth, approximately 42 billion checks will be written on demand deposit accounts in 1980 [45].

The best estimates of check processing costs within the banking system allow 16-21 cents per check. Assuming that 32 billion checks will be written on demand deposit accounts in 1976 and that a check costs 18 cents to process, the banking industry will spend nearly 6 billion dollars on check handling this year. In 1970, labor accounted for two-thirds of the cost of check processing [11,pp10-25]. In addition, each party that mails a check pays the costs of postage, envelopes and preparation time. Thus, automating much of check

handling has been advertised to cut the major cost in check processing.

These expectations, which were widely advertised in the early literature promoting ACPS[9,26] were clearly articulated by Long:

> "Because large manual labor costs are still incurred in large data processing applications, operations managers dream of the day when all of their input data will come to them in machine processable form. This feeling is so universal that there is almost a common desire to push the preparation of electronic data back to the original transaction point."

> "In the payment system, the Federal Reserve made great savings from the MICR* program because it meant that most of the processing work arrived in machine processable form. The banks benefited less from MICR because they had to do most of the check encoding."

* MICR denotes magnetic ink character recognition, the process which is used to read the odd little numbers that appear on the bottom of your checks.

"If the Federal Reserve System or the banks implement an electronic credit and debit fund transfer system, the cost savings from the lack of major data entry or data preparation work will be enjoyed by each institution able to push the data preparation point back down the line to the original transaction point. For example, the Federal Reserve will enjoy the greatest saving because all data entering its electronic system from banks will already be in electronic form**. The larger banks will enjoy savings if they can induce their smaller bank correspondents and their large commercial customers to send them electronic debits and credits. The large, medium sized, and small banks will enjoy savings if and when they can induce their customers to deposit electronic debits and credits."

"The growing availability of Touch-Tone telephones, small keyboard terminals, cash dispensing automated teller machines and electronic point-of-sale terminals are making it possible, more and more, to capture electronic data at the transaction site[26, p.10]."

** The Fed is charged with the resposibility of clearing checks for the commercial banks, but is unable to charge for its operating costs.

It is difficult to make accurate estimates of the costs of automated check processing. Nevertheless, several studies of processing costs in regional automated clearing houses conclude that the economies of processing occur with rather large transaction volumes. Even with large transaction volumes, the systems do not seem to break even in the first five years of operation[3]. It is even more difficult to estimate the costs of electronic networks because of their unknown capital cost. In addition, amortizing ACPS capital costs over different periods of time (10 years vs. 20 years) would substantially affect the estimates. The current conventional wisdom of banking experts is that the planned technologies will not apppreciably reduce the costs of check processing. Some advocates even admit that the arguments for reducing paper processing costs simply provided a graphic rallying point to help generate widespread support for EFTS[25].

B. Diminish the Cost of Petty Theft

EFTS advocates claim that both merchants and consumers will be less subject to petty cash theft if the payments system is automated. Consumers who transact business through POS to directly debit their bank accounts would have to carry less cash. Retailers could operate with less "till cash" and be less susceptible to pilfering and holdups. Such analyses assume that consumers and retailers would be well protected from fraudulent transactions. Much of the work on EFTS security has focused upon design of identification cards that would be easy to use, but costly to duplicate [32]. In addition, there are

several schemes for providing customers with personalized code numbers that they would enter into the POS terminal at the time of transaction. These codes would make it difficult for someone to use a stolen card. Unfortunately, such code numbers are easily forgotten. In order to remember them, many people may write them down on their cards or on a slip in the wallet in which they keep their cards. Thus when cards are stolen, they may often have the codes stolen with them.

There is an experimental project at Stanford Research Institute to develop a scheme for identifying people by the patterns of pressure they exert when they write specific words such as their names. Apparently, such pressure patterns are unique to each person, are difficult for a forger to duplicate and are relatively easy to detect by having a person write on a special pressure sensitive plate. However, this technology is in an early stage of development and its utility remains to be proven. At this time, there seem to be no widely accepted and reliable schemes for preventing the abuse of stolen EFTS cards.

C. Allowance for Pre-authorized Payments

Pre-authorized payments include two independent classes of transactions: income deposit and recurrent payment authorization.

> For income deposits, employees, recipients of social security and welfare, and others who have authorized automatic deposit would indicate the banks in which the deposits would be made and payors would then routinely deliver or transmit by wire to their primary banks the complete payment and bank-of-deposit data. Each primary bank would sort out payments to be deposited with itself and would transmit payments that are to be deposited elsewhere to an automated clearing house." [11, p. 31].
>
> For recurrent payments, the payor should notify organizations to which he makes frequent payments of the bank he uses. These organizations would send bill descriptors directly to the bank. The payor might receive by mail the complete descriptions and data now provided with items such as utility bills [11, pp31-32].

Variants of this system offer different ways of scheduling payments: on demand, 7 days after notifying the payor who may stop payment if he finds a billing error, etc.

The primary beneficiaries of these pre-authorization schemes are the businesses or agencies that exploit them. Substantial costs of printing and dissemination would be saved by payors. Not only do these include businesses with large payrolls, but it also includes public agencies such as the Social Security Administration and welfare

agencies which disburse millions of checks every month. Those institutions that receive recurrent payments would be guaranteed a smoother cash flow and should expect lower collection costs. The consumer would be spared the inconvenience of making separate bank deposits or mailing a variety of checks. Presumably, the decreased cost of operations would also be passed back to the customer (or taxpayer) if the market were operating "perfectly."

Individual recipients of pre-authorized payments also gain. Salaried employees who have their payroll checks automatically deposited save the inconvenience and cost of depositing checks themselves. In addition, they can be drawn upon immediately on payday. Welfare recipients who occasionally have their checks stolen from their mailboxes, may face one less hazard in their dealings with the bureaucracies.

During the last several years experimental automated clearinghouses (ACHs) have been developed in several Federal Reserve Board regions. With the exception of the ACH in Philadelphia, these have been coordinated exclusively by the commercial banks. These ACHs serve as regional clearinghouses for checks written in large volume by large businesses and some government agencies. Most of the initial uses focus on the direct deposit of payroll. In this situation, an employer provides the ACH with a magnetic tape which describes the pattern of payments. These are then "disseminated" by the ACH to the participating banks and credited to the employes' account. In principle, all participants should gain from such an arrangement.

Banks could cut their check processing costs, employers could cut their check preparation and (possibly postage) costs, and employees would have their paycheck on deposit and not have to mail it to their banks or wait in line in the bank lobby. In practice, the banks may cut the costs of check processing only if they can handle millions of transactions per month [3,Appendix G].

D. Real-time Credit Verification

In a large and mobile society, businessmen rarely know whether their customers can truly afford the cost of their services and goods they purchase. In a cash economy, where people literally pay as they buy, there is little uncertainty. Services or goods and the money to pay for them cross the table almost simultaneously. With the advent of "near moneys" such as checks and credit cards, the situation becomes more problematic. The current solutions for businessmen include getting multiple identification to limit the likelihood of forgery and to follow up bad checks easily, calling banks to check whether a person has suffucient funds to cover a check he is writing, and the use of credit reporting and insurance firms such as TeleCREDIT. Each of these mechanisms is comparatively clumsy and unreliable when compared with the certainty of having real credits or debits flow at the time a business transaction is completed. After all, a person may write several checks in one day, each of which is "verified" against the same dollars in his bank account. Full scale EFTS which link POS terminals directly to customers bank accounts can

diminsh the spate of bad checks that many businesses, such as supermarkets, routinely receive.

Of course, the paying party, whether a business or individual, gains some control over the transaction by being able to withhold payment if the goods are poor or the services shoddy. Stopping payment on checks and withholding credit card payments are the common mechanisms for exerting such consumer control. Real time debit transfer simply costs consumers considerable control over the quality of goods received in particular transactions. Unfortunately, most EFTS proposals focus upon the gains to businesses rather than the losses to consumers. We'll return to this issue in part E of the next section.

E. Decreased Float

Most EFTS technologies naturally decrease float since they increase the speed at which debits are tranfered between any two parties. While individuals are quite sensitive to their potential loss of float, so are large businesses. Many large businesses deposit their payroll on several successive days and invest the balance they withhold in large, high interest, overnight loans. Float provides effective funds for all people who use checks as an economic medium, and it's not clear overall who will gain or lose as it is diminished throughout the economy.

While ACPS may diminish float through speeding transactions, it's not clear what actual impact it will have on float. Delays between the time a party is billed and the time they actually credit the payee's account are influenced both by the time they initiate payment (e.g., write a check) and the time it takes for the payment to pass through various carriers (e.g., mails and couriers) and the national payments system. To the extent that debtors delay payment by not writing a check instantly when they are billed, they increase their effective float. Since most businesses curently allow anywhere from 5 days to 60 days for payment, diminishing the check processing time from days to minutes may not appreciably diminish the overall delay in payments within our payments system.

The major party that seeks to diminish the total amount of float is the Federal Reserve Board. Since float increases the effective money supply and is controlled by millions of independent agents, it reduces the Fed's control over monetary policy.

F. Convenient Adjunct Services

If individuals or institutions perform a major portion of their transactions through EFTS technologies, it may be possible to provide certain kinds of accounting at a moderate cost. For example, if a party could code selected transactions, his transactions could be aggregated by coded classes every month. Such special services simply suggest the kind of possibilities that could be piggy-backed onto ACPS

or POS networks with relative ease.

G. Market Share

Most banks in urban centers openly compete for customers by offering a variety of services from expanded hours to free trust deed collection to their customers. Such competition tends to be carried on between small sets of banks in particular localities. Similar competition is carried on between banks of different classes in their attempt to develop new services that they can offer to prospective customers. For example, thrift institutions have experimented with special demand drafts that would give their customers some of the flexibility that one obtains with the checking accounts which have been legally monopolized by commercial banks. The potential impacts of EFTS technologies on maintaining and increasing one's market share have provided much of the push behind the continuing interest of banks in EFTS technologies.

On one hand, some EFTS components can provide new services. For example, automatic teller machines provide some service 24 hours a day, seven days a week. In addition, if a bank can place automatic tellers into dozens of locations, some of them in rural areas outside of its "normal" service area, it can also open up new markets for itself*. Similarly, a bank which can offer pre-authorized payroll

* Branch banking laws are slowly being modified. See the discussion in part F. of the next section.

deposits may attract new customers who work for firms offering that option to their employees.

On the other hand, banks that neglect to develop these new services may well lose business if they don't keep up with the competition. This dual pressure, to expand or at least not fall behind, make EFTS technology developments of keen interest to various banks. However, as Dan McCracken has pointed out, if every bank offers similar EFTS linked services, no new deposits are created in the economy as a whole[28]. Only the distribution of deposits among the various banks may be influenced**.

I. Timely and Comprehensive Market Information

** On the other hand, since new devices are sold, achieving this state of affairs does open up vast new markets for computer system and terminal vendors.

ACPS and POS networks provide a vast repository of information that would otherwise be unavailable in the time frames made possible with real-time systems. The Fed provides member banks with information about the flow of money in various sectors of the economy. This is one of the benefits (other than the ability to borrow from the Fed) enjoyed by the member banks. Currently, such information is slowly aggregated and made available on a monthly basis. If a large fraction of the nation's debits are passed through ACPS administered by the Fed, such information could be availble more rapidly and in finer detail than is now feasable.

If POS networks are used to transmit a large fraction of the sales-related transactions, the nature of the purchases used for "descriptive billing" could also be used for various marketing studies and sales campaigns. Such information could be processed by one of the major third parties involved in transaction processing as a small business. For example, it could develop demographic profiles of the purchasers of brand X or even lists of people who had recently purchased some specific item such as a blender. The latter could be used by particular firms to help them selectively advertise related items. Under current laws, the institutions that collect such information may also reorganize it for resale to other parties.

In this section, we have considered nine major classes of benefits that are commonly ascribed to EFTS technologies. Most of these accrue directly to major financial institutions and large organizations, public and private. These benefits are subsequently transferred to the broader public when these institutions operate more efficiently and pass on these efficiences. Individuals and smaller organizations may derive some direct benefits from doing business via EFT supported operations. For example automated tellers and pre-authorized payroll deposit may be especially appreciated. But these or similar services do not explain the major interest that EFTS has stirred among the major business institutions.

It seems that the major value shifts that accompany EFTS components lend support to the Free Enterprise, Statist, and Systems models which were described in the last section. In the next section, we will examine a few of the repercussions that widespread development of EFTS might produce.

The Current State of Knowledge About EFTS Problems

Different people view EFTS as a source of both benefits and problems. Not surprisingly, promoters tend to emphasize the benefits. For example, Long claims that:

> "EFTS is happening because it is a better way. All arguments about the sufficiency of the present paper system are meaningless. Television did not come about because the radio system was overloaded or breaking down, nor did radio or the telephone develop because the mail was about to collapse. Neither were these systems built because the public was crying for their development. They came about simply because they represented a 'better way' of communication. The same motivation is the driving force behind EFTS developments."[26,p.2]

On the other hand, Paul Armer suggests that POS networks provide the technical basis for real time systems to keep rather close track of the whereabouts of any citizen [2]. Wessel[40] is concerned that EFTS may not be accessible to people who are poor credit risks. If most financial business is conducted via EFTS, creating a social group that is cut out of the action may create a kind of "social dynamite."

These two examples illustrate the type of issues raised by computer specialists and lawyers whose careers do not depend upon the widespread adoption of an EFTS. Since EFTS may become a pervasive technology through which almost every financial transaction takes place, it is important to consider the problems that such systems might produce before engaging in a wholesale development. The remainder of this section is devoted to exploring some of these potential troubles.

A. Theft and Sabotage (Security)

When Willy Sutton, the famous bankrobber, was arrested for the 10th time and lead down the Cook County Courthouse steps in handirons, he was approached by a newsman who asked: "Why do you still rob banks?" Sutton looked the man in the eye, and replied,"Well, that's where all the money is."

The story is apocryphal, but the sentiment is not. While holdup men account for only a small fraction of the money stolen from contemporary banks, an automated payments system might be harder to resist. Approximately 300 billion dollars passes through the nation's banks each week. The average bank holdup grosses several hundred dollars. It hardly pays a living wage. While the nocturnal robber captures the imagination of TV watchers aross the country, most bank robbers enter through the front door with pistols. On the other hand, if the thief of the future can use software, rather than explosives,

the work may be cleaner and net a greater return.

EFTS advocates usually portray the existing paper-based payments system as "inefficient." It is also relatively secure. The maximum theft is limited by the amount of cash or securities that is stored in any one place at a time. In the manual system, the cash is physically distributed over thousands of banks. To steal $100 from the Midas Trust in Minokee, one must be in Minokee. Some security is built into the current system of decentralized and weakly coupled banks since theft requires physical presence. Perhaps an occasional Brinks robbery will net a million dollars every few years. However, in ACPS, the maximum theft is almost unbounded in principle. A clever intruder may have access to all the funds on account in a particular bank. If the intruder is more clever still and able to "enter" via a remote terminal, he could gain access to all the funds in the system! Most of the published security studies deal with ways and means of preventing one person from impersonating another at the point of sale. Such schemes are designed to prevent "petty theft." In this analysis we are focusing on relatively infrequent, but major thefts.

For a theft to be successful with ACPS, it is an open issue whether any "cash" must finally exit from the system. A successful thief might simply transfer funds into his account and transform them into services by transacting legitimate business and allowing other businesses to legimately debit his account(s) in exchange for services rendered (e.g., travel) or goods purchased. Alternately, if one wished to leave the country with substantial cash, one might extract

cash by normal means after surrepticiously siphoning funds into several medium sized accounts. One might even extract funds through automatic tellers.

Computer-based systems appear invulnerable to most people who have no professional contact with computing. But most systems today are quite vulnerable to threats by sophisticated intruders. What we casually call a "computer system" is actually a complex arrangement of hardware components, software modules, organizational practices, and specialized organizations. Each of these provides a separate locus of entry into the database of a complex computer system. In most contemporary systems few of these loci are well protected [1,21,24,30,35]. Some points of entry, such as operating systems, are well known to be vulnerable and a small folklore of successful penetrations has already been passed on about them in an oral tradition among computer professionals. Many of these penetrations are perpetrated as pranks by college students or by programming staff to point out the vulnerabilities of the systems they work with. Others are mounted for profit and are not publicized [1,17]. Most second and third generation computer systems can be easily penetrated by computer sophisticates.

While strategies for enhancing system security are receiving substantial attention from computer science researchers, the task of developing thoroughly secure software systems is immense. In a recent review of system security, Linde noted 26 different generic functional flaws in software systems[24]. These range from strategies of

authenticating users to the strategies for checking the appropriateness of various parameters that are passed between system modules. In addition, he noted 18 distinct strategies that an interloper could use in attempting to gain illegitimate access to privileged system commands and thus to password files and then to "free" access to a system. The current situation may be summarized as follows:

1. Most contemporary computer systems are insecure;
2. It is currently impossible to prove that a given computer system is technically secure*.
3. The body of techniques for developing technically secure systems is growing rapidly [21,24,39]. These schemes vary in costs and influence the design of dozens of system features.
4. Any computer system is as secure as its weakest component. (A locked door is of little help if all the windows are open.) Most of the larger computer systems have several features that enhance security such as passwords, but these may be bypassed by clever intruders[24].

---

* Attempts to prove the correctness of programs are currently receiving some attention, but the current schemes can deal only with comparatively simple programs. Operating systems which are built from hundreds of modules and written in languages whose properties are difficult to formalize seem well out of reach. Some attempts have been made to prove the correctness of particular protection schemes for particular machines, but these proofs do not insure that the implemented scheme is free of error. Recently, Harrison and his colleagues demonstrated that one cannot prove the correctness of "an arbitrary configuration of an arbitrary protection system or of all configurations for a given system [18]."

5. The strategies for insuring a high level of protection require that dozens of features in each system be appropriately designed. Few of these special designs coexist on any but a few experimental systems and possibly a few systems used within the intelligence community.

6. A heavily protected system is relatively costly and each additional security feature adds to the system overhead**.

7. Most security flaws in computer systems are detected after the system is implemented. They are usually found:

   (a) After a penetration has been discovered;

   (b) Through a systematic and costly security check;

   (c) By accident.

8. The preceding remarks apply primarily to computer systems with a centralized processor. The state of knowledge about strategies for developing secure networks such as those required for EFTS is even more primitive. In short, an electronic Fort Knox is still a technical dream, not a contemporary reality.

** The degree of protection one might want to provide depends upon the sensitivity of the data and the strategies one expects interlopers to attempt in breaking the system security. For example, if one expects that an intruder might attempt to transact business by coupling to the communication lines between processors, then one should place the system in a lead enclosure and shield the communication lines. Most protection schemes employ combinations of the following strategies:

1. Check the legitimacy of critical parameters that are passed between modules;

2. Limit communication between processors.

The former adds the cost of frequent checking while the latter limits the ease with which certain resources such as data files may be shared.

If a system is vulnerable to penetration, it is vulnerable to sabotage or theft. A specific computer in a large bank might be disabled for a significant period of time or sensitive transaction files may be transformed from patterns of bits that make sense to patterns of bits that don't. Real time systems are especially vulnerable to the destruction of data. In batch systems, transaction tapes are processed at a particular time and a sufficient set of backup tapes are kept so that damage to one or two days transactions might be recovered with only minor grief. On the other hand, a data-base which is modified in real-time to keep a person's accounts up to date for real-time crediting and debiting often is not organized with a distinct, off-line transaction archive. Thus, such a system is more vulnerable than many of the financial systems in use today[1].

Sabotage demands less skill since one isn't trying to tamper with a complex system and make it appear that it is performing correctly. An example of a scheme to impede business transactions in an economy where most payments are tranferred real-time in a network linking POS terminals and ACPS is provided in Appendix A.

Computer-based systems can be rendered relatively secure through deft design and extensive testing in a setting in which skilled technicians attempt to penetrate system security[24]. However the security flaws in most computer systems are currently found by accident, one bug at a time. However, systems can be "shaken down" through "war games" to help understand their flaws and develop counter-measures for successful penetration. In the case of EFTS,

various components may have to be installed in operational settings for some period of time before they are shaken down for technical flaws. During this time, or during periods when EFTS components are undergoing major changes, they will remain relatively vulnerable.

When one thinks about computer system security, it is important to emphasize that a system is no more secure than its weakest elements. If a system is "technically" protected from a certain kind of penetration, it may not be immune. For example, a system of passwords and active checking of people who attempt to use more than several incorrect passwords may diminish the likelihood that illegitimate users gain access to the system. Yet if the list of passwords is left in a public area or if a legitimate user passes his password to a friend, the viabilty of passwords are lost. Thus the theft by insiders or by people with inside connections remains a constant problem in the most technically secure system. Given the potential gains, potential thiefs may attempt to extort as well as bribe or coopt employees of financial institutions who know certain sensitive details of EFTS operations. Since there are over 13,000 banks alone in this country, the number of potential points of entry and people who might assist such entry (including computer professionals, maintainance staff, bank auditors, etc.) would number in the tens of thousands. These problems of maintaining the integrity of people who have sensitive knowledge of EFTS operations may turn out to far exceed the technical problems of system security both in magnitude and difficulty.

B. System Reliability

To the public, computing represents a reliable technology. The problems that they see have more to do with inaccurate data or organizational procedures (such as billing errors) rather than with system crashes. The closer one gets to the terminals of an on-line system, the more one lives in the "up" and "down" world of computing. The more complex the architecture of a computer system and its associated software, the more likely it is to fail. Small dedicated machines may run without crashing for months, while many large computer centers expect at least a few crashes every week*. While many crashes require only minutes to recover from, occasional crashes can keep a system down for hours or days. All this is tolerable when anyone who depends upon the system can let a transaction slip for an hour or two without major cost or inconvenience.

* One may also buy reliability with backup equipment such as extra processors, core, and secondary storage. The costs of reliability increase accordingly.

As the scale of the system increases, reliability diminishes. Large numbers of fallible components linked with dozens of software modules are simply difficult to keep working perfectly. Certainly, the proposals for nationwide real-time EFTS rival the airline reservation systems in sheer technical complexity. However, before we become dependent upon such large scale highly integrated networks, we ought to be sure that they are phenomenally reliable. That will probably entail testing and validation schemes far more sophisticated than we have today[20].

In addition, there are special features of real-time EFT networks that deserve special attention. First, real-time debiting schemes will probably change the time constant of the (current) payments system by a factor of 2000 ! When one changes the time-constant of any real system by several orders of magnitude, tremendous differences can be expected in the characteristic behavior of the system to inputs or disturbances. For example, if a bank makes a clerical error, and a person's account isn't properly credited with some funds, under current arrangements the person can still conduct his normal business affairs while he and the bank are investigating the problem. It might come to his attention via an overdraft notice by mail, and checks he has just written are probably still passing through the chain of payee and banks that normally take several days. While this system is slow, it is relatively tolerant of certain errors. A real-time system is likely to be less tolerant. For example, if a person relies upon real-time POS as <u>the</u> medium for doing his business and such an error occurs while he is on on a weekend trip, he may suddenly find himself

unable to buy gas, food, or pay for his hotel**. Or consider the following situation:

> A large firm with several hundred thousand employees deposits its payroll in employee accounts late on a Friday afternoon. Suppose that due to either a clerical error or program malfunction, these payroll transfers are not properly made and each employee receives only several dollars or no money at all. During the evening, other institutions may attempt to debit these employee accounts for pre-authorized payments such as insurance premiums. In addition, employees may be transacting their regular business and expect their payroll to be available as a credit base. If some of these transactions bounce, and then transactions upon which they are based begin to bounce, we may see "poor credit" propagate through EFTS. Such a stream of poor credits may propagate through thousands of accounts before it is noticed. Could such an event, however unlikely, lead to a "credit blackout" somewhat analogous to the North East power blackout of 1965 ?

** He may escape some of these problems by resorting to a device that would be an anachronism in a society dependent on real-time EFTS--travellers' checks.

While the particular conditions that are described here may not lead to a regional "credit blackout," are there other conditions that could precipitate such an event in a nationwide real-time EFTS? This is the kind of question that computer and banking professionals should be thinking through when they consider the technical feasibility of EFTS.

C. Privacy of Transactions and First Ammendment Freedoms of Speech and Association

The privacy issues elaborated below ultimately influence the degree of social and political diversity we can expect in this society.

Any ACPS would record to whom each person writes each check. This information, along with the date(s) of the transaction, check identifier, and amount of transaction would be aggregated in one's records at his local bank. Record of each payee is necessary as a possible receipt, for record keeping and for the check writer to audit his account. All this information is available now, since each bank microfilms every check cashed against one of its account holders. However, the cost of finding out whether a particular individual wrote a check to a particular party or group is prohibitively expensive. The checks are filmed as they are cleared and each person's checks are randomly distributed through the thousands of other checks processed by his bank each month. Privacy of transactions is now insured under

all but the most unusual circumstances by the sheer cost and inconvenience of manual search. (Some surveillance is possible: a bank can easily keep track of the checks written by particular individuals as they clear. However, it is prohibitively expensive to search for records of those checks after they have been returned to the checkwriter.) In the current system, the microfilm records are kept on file for 7 years*. Under ACPS, they would be neatly aggregated and left on file in machine readable form for 7 years.

In EFTS, disclosure of information is the primary privacy threat. This situation contrasts with credit reporting systems where the accuracy of information about a person, his right to audit his own file, contest its contents, and control its access are all salient issues. In most financial transactions, the first three of these are the normal rights of any creditor or debtor. A critical issue which is still unresolved here is who owns the set of data describing an individual's transactions with a bank or other financial institutions.

* The Bank Secrecy Act of 1970 requires banks to keep records of each check that is debited against any of the accounts it provides. This law was challenged in 1970 in a joint suit brought by the California Bankers Association and the American Civil Liberties Union [10]. The court held in favor of the U.S. Government.

Now consider which "non-financial" institutions would have easy access to this information. Almost certainly, various law enforcement agencies (FBI, state police) and investigative bodies (e.g., grand juries, legislative committees) would have access through secret subpoena. These groups are barred access to the Census forms under the original census statute, but a similar restriction on ACPS files may be politically impossible to move through Congress now. Such groups occasionally have legitimate needs for such information. For example, records of checking account activity help the IRS investigate and prosecute tax fraud cases. Unfortunately, such agencies occasionally abuse politically and personally sensitive information. For example, during the early '70's the IRS maintained a special division to investigate politically unconventional people and groups. Such abuses are not wholesale; they are quite selective and often aimed at groups which advocate unpopular actions. However, the existence of dissenting groups is critical to a "democratic" political process.

Invoking the image of the McCarthy era, is unpleasant, but that period illustrates the abuses and threats possible with ACP'S. in mind. Few people were actually investigated; but those who were investigated were asked to defend social and political associations they maintained twenty years earlier. Millions more were intimidated. We do not now have adequate computing power to support casual mass surveillance. However, substantial social control can be exercised by publicly harassing relatively few people. We would have ample computing power in ACPS to support such focused efforts. For example,

the detailed transactions of several thousand people per Federal Reserve District could easily be monitored. Alternately, in 1981, a grand jury could investigate which depositors, at say, 50 "Old Gold" branches contributed funds to the Orange County Citizens to Support the Presidency in August through October 1976. Such a search could take several evenings of computer time and be unobtrusive*. In the current system, such a search would take an army of clerks several months and would be quite public.

Our country is politically volatile. While some of the major national politicians who exploited fear and scapegoating (e.g., Agnew) are politically disabled, their constituencies are alive and well. Who can say what will be the political texture of this country in 1980? Fear that support of groups that are now "safe" may lead to harassment some years in the future may well weaken support for unconventional or fringe groups. This "hypothetical" threat to the diversity of American political and social life may become all too real with ACPS. Unfortunately, we have no systematic data on the extent to which various people would actually cease supporting unconventional groups if ACPS were implemented. However, the

In a recent grand jury investigation in Orange County California, a bank sought to charge $10,000 in labor costs for providing extensive check copies for a defendent.

reluctance of many people to sign "political" petitions in which they believe provides a fair index of such nervousness. While the social and political diversity of this country may be indirectly constricted by ACPS, such subtle threats to freedom of association and their "attendent costs" are less tangible than the dollar gains to be realized by ACPS beneficiaries.

D. Surveillance

Most of the institutions that advocate large scale EFTS transact business with tens of thousands, or even millions of clients. In order to keep track of their large number of transactions and clients, they need easy access to a variety of personally specific information. In addition, for clients to audit their own records, they will need precise accounting of their transactions (for what, with whom, when, for how much). Most of this information will not be collected frivolously. Rather, different kinds of data will be collected or aggregated by different institutions to help them carry out socially sanctioned goals. However, the range of information available through interlinked large scale EFTS creates a tremendous social resource.

Recently, James Rule defined the "surveillance potential" of an information system in terms of four critical features[33,34]:

1. "the sheer amount of meaningful personal data available on those with whom the system must deal[34];"

2. "the effective centralization of data resources so that all available data can be brought to bear on decision-making problems wherever in the system they may occur[34];"

3. "the speed of information flow and decision-making within the system, for speedy movement of data and quick decisions mean that the system can 'react' to those with whom it deals before they can 'escape'[34];"

4. "the points of contact between system and clientele, that is the number of locations through which the system can absorb new data, and from which it can'reach out' against those on whom some corrective action is contemplated[34]."

Any of the major EFTS systems increase at least the last three characteristics of "surveillance potential." That means that selected institutions which utilize EFTS may exert more control over their clients who "deviate" from their preferred practices. For example, most businesses that use POS linked to a banking network would be able to insure that each customer is able to pay his bill when services are rendered or goods are purchased. That differs from the current situation in which credit card verification and "check verification cards" attest that a customer is a good credit risk in general, but

not that he is at the moment he is engaging in a particular transaction.

Currently, police agencies also use the credit verification systems to help hunt suspects. When a person uses a credit card to make a purchase that exceeds a preset amount (usually $25 for oil company cards and $50 for bank cards), the status of the card and cardholder are checked by the clerk transacting the business.The FBI and certain state police agencies routinely post lists of wanted suspects with the credit verification centers of the major credit cards. If a nationwide network of real-time POS were implemented, the major police agencies would also be able to limit the movements or more carefully monitor the activity of specific suspects. Such monitoring would be legal and legitimate when police agencies pursue indicted criminals. However, some of the major investigative agencies have also been known to abuse their power and harass people who have engaged in legitimate political activities. The very existence of an instrumentality that may be easily abused does not, of course, guarantee that abuses will occur. Rather, abuse is tempting and likely.

In 1971, a group of sophisticated computer scientists and legal experts were convened to study systems of social control. They were asked to imagine themselves in the position of the Soviet KGB and to propose various ways of monitoring the daily activities of Soviet citizens. They considered different kinds of spying arrangements, and procedures for people to report their own activity. Finally, they

found a relatively simple solution which would be difficult to subvert and would insure a large degree of compliance with relative ease: abolish cash money and develop a national EFTS that would handle all of the people's financial transactions.

Of course, such a proposal seems more consistant with our understanding of social control in the Soviet Union than in the United States. That such a proposal is so inconsistant with the American political heritage makes it difficult to think through and articulate the possible or likely abuses of EFTS as a surveillance device without appearing as a crank. After all, "it can't happen here."

E. Consumer Protection

EFT technologies have been primarily developed for commercial interests and large scale public institutions such as the Federal Reserve Banks.

During the last 5 years, the American Bankers Assciation has commissioned several market studies of the ease with which people would accept EFT technologies. Generally, most people have been satisfied with their current payments styles (e.g. cash, credit cards and checks) and have shown little interest in shifting to real time payments. Most consumers seem particularly interested in maintaining float and control over how much they pay to whom and when. Thus, they occasionally will opt for pre-authorized deposits into their accounts

(such as payroll) and show remarkable disinterest in pre-authorized debits (such as telephone or utility bills). Generally, consumers seem to have the same kind of economic rationality as do business enterprises:

> They want to increase the speed with which they receive income, control the speed at which they pay for goods and services, and are unwilling to accept convenience for its own sake without asking what it will cost. Of course, different issues arise with different EFT technologies. For example, one maintains control over payments with automated tellers that one doesn't have with pre-authorized debits. "Stop payment" becomes more of an issue in real time pay-out schemes than with automatic pay-in schemes.

In much of the EFT literature, consumers are portrayed in one of several ways:

1. as people who will be overjoyed by the added conveniences that may be provided by EFT technologies;

2. as compliant clients of commercial firms who will adapt to changes in business practice with little complaint or enthusiasm;

3. or as people who are needlessly "resistant" and who need to be "educated" about the latent virtues of electronic payments.

During the last few years, as consumer preferences have become more clearly appreciated, the image has shifted from the first to the last. Generally, EFT advocates seem to be paying more attention to "marketing" EFT technologies than to designing them so that they will more adequately meet the felt needs of consumers. For example, I am unaware of any proposals for designing "stop payments" mechanisms into real time payments systems*. Nevertheless, such a mechanism would hardly raise the development or operations costs of the complete systems. One simple and suggestive scheme is sketched in Appendix B.

Approximately 20% of American households do not utilize checking accounts. While many of these people tend to be poorer than account users, some of them simply prefer to transact business on a cash basis. But certain government initiatives may force many of these people to utilize checking accounts or related banking arrangements. If major federal agencies that provide monetary payments such as the Veterans Administration, Social Security Administration, and selected

* A scheme for correcting erronious billings is part of the California ACH operation, but this only covers pre-authorized payments rather than the ad hoc payments which characterizei most consumer purchases.

welfare agencies may rely upon ACPS to cut their overhead costs, then they are likely to force their clients into holding bank accounts.

F. Reduced Competition within the Financial Industry

In our brief discussion of the competition among banks for market share, we noted the ways in which selected EFT components fit into traditional competitive arrangements. One might presume that such competition might slightly alter the market position of various banks, but have little overall influence on the structural arrangements between financial institutions. That is unlikely. Even without EFT developments, the institutional arrangements between banks have been changing and will probably continue to change. For example, banks have been leaving the Federal Reserve System at a steady pace since World War II[5]. In addition, thrift institutions have pressed for and are receiving statutory authority to provide services such as demand deposit accounts. Lastly, several states which prohibit branch banking are beginning to alter their restrictions.

EFT technologies fit into these changing relationships in ways that are relatively unpredictable. For example, if there is one nationwide network to support ACPS which is administered as a public utility, then many banks could link to it with a minimum of cost. The primary advocate of such an arrangement is the Federal Reserve Board which could use a differential rate structure to lure banks back into its system. Such a single arrangement is opposed by the charge card companies and larger banks such as Citibank which might afford their own networks. While multiple networks afford each using group greater flexibility, the costs will be increased and participation will become more difficult for smaller banks and possibly for rural banks. In such a situation, smaller banks may be "encouraged" to merge with larger banks to continue their business.

Some of these competitive issues will hinge on the way in which the regulatory agencies or legislative bodies (re)define branch banking. In December 1974, the Comptroller of Currency defined automated tellers in such a way that they did not constitute a branch. That opened the door for large urban banks to place automated tellers anyplace they could link them with wires. A subsequent revision of the ruling restricted their placement to within 50 miles of the office to which they were linked within the state in which the bank office was situated or within the "normal service area" of the bank in whatever states that included. This ruling is now being contested in the courts.

These arrangments are still unresolved. The Congressional EFTS Commission includes representatives of the major classes of banking institutions, and its pluralistic composition suggests that no class of institution will be wiped out. In addition, maintaining maximal competition seems to be the primary concern of the Justice Department relative to EFT developments[6]. However, many bankers close to EFTS developments sense that generally, the larger banks will fare much better in whatever EFTS developments emerge and that smaller banks may simply be unable to compete while retaining their independence.

Open Issues in EFTS Development

In the last two sections we have surveyed a number of major benefits provided by EFTS to some parties and problems posed by EFTS for other parties. The direct benefits accrue mostly to large institutions, public and private. On the other hand, the parties that face the most problems include a variety of groups which are smaller in scale:smaller banks, individual consumers, members of unconventional political groups, etc.

From the vantage point of the value positions introduced in the third section of the paper, EFTS tend to support the Free Enterprise, Statist, and Systems value positions. They come into greater conflict with Libertarian, Populist, and Conservative value positions. Since all of these positions except the Systems position have deep historical roots in America, any argument couched in one of these value frameworks can be labeled a "public interest" argument. Since EFT technologies exacerbate conflicts between these positions there are really no simple "public interest" arguments regarding EFT developments.

Many technologies that are adopted on a large scale are accompanied by social problems. Also some technologies are relatively benign. For example, the telephone appears relatively benign except perhaps to the parents of teenagers. Other people wonder whether we couldn't have developed better ways of moving people in and out of cities without crisscrossing the cities with multi-level freeways. As a culture, we are beginning to realize that the technologies we create may raise subtle, unforseen problems and that we ought to think through the consequences of pervasive technologies rather carefully before implementing them on a large scale. The current debates over the problems and prospects of nuclear energy indicate that we no longer take our technological promises for granted.

Some of the major issues in EFT concern not only the resolution of the kinds of problems that I have sketched in the last sections, but also focus on the processes by which such problems will be resolved. Unlike DDT which may be banned by the FDA or communication satelites which may be supported by Congress and the FCC, no single regulatory body has exclusive control over EFT developments. The banks alone, are regulated by at least four major federal agencies and numerous parallel agencies in most of the states. There is a EFT Commission operating within Congress, but it is an advisory body which may complete its deliberations well after key decisions about EFT developments are made by other public agencies or private institutions. In addition, some interests (and the value positions which they favor) are better represented than others*. Not suprisingly, the relevent government agencies and major private enterprises have more expert and widespread representation than do consumers or unconventional and thus disenfranchised political groups.

* There are major conflicts within the financial community about how EFT technologies should be organized and regulated. But the financial institutions, as a class, simply have concerns that differ from those of consumers as a class.

Another major set of issues concern ways of learning about preferential EFT arrangements before some systems are cast in concrete on a sufficiently large scale that they are too costly to revise. Long, for example, makes the following argument:

> "...the public or the marketplace does not 'demand,' it simply chooses between alternatives....The public did not clamor for TV to be invented; they did not ask for the touch-tone telephone; nor did they ask for the horseless carriage or the airplane. ..despite all the negative surveys and predictions (at the times of these developments) the publc has embraced these devices...simply because when the choice was presented, they appeared to be the more convenient or the more appropriate to the way they would like to live. The same will be true of EFTS...[25]"

The problem with such an approach, despite its pleasant cynicism about public choice, is that it encourages us to continue making attractive incremental choices which over some period of time lead us to a place where we do not wish to be and from which we cannot easily choose some vastly different alternative. Twenty years ago the Los Angeles freeway system promised freedom and convenience. At each choice point, it was "rational" for developers to create bedroom enclaves and regional shopping centers that paralleled the freeways. Today, Southern Californians are locked into a pattern of transportation and land use which doesn't meet their needs very well and which is hard to drastically alter.

One can, of course, develop many small scale experiments similar in spirit to the Hinky-Dinky experiment in Nebraska[27]. However, we may have as much trouble extrapolating from such small scale EFT operations to large scale operations. After all, if one "experimented" with private automobiles in 1910 by placing 2500 cars in L.A., would they have lead us to understand the long range problems of roadway congestion and pollution in the city several decades later ? Simply building prototype systems and extrapolating their behavior in some near linear fashion may give us little insight into the dynamics of a society which depends on digital bucks. One strategy, that of speculative scenarios, has been explored at Arthur D. Little[3]. While such techniques have their own problems* they may provide some rich insights.

Despite these cautions, EFT developments are moving rather rapidly. As Long notes, "The fear of being out of the marketplace is one of the stongest in our present day environment[25]." Sometimes, this fear is turned into the claim that EFTS are "inevitable," so there's little reason to slow development. Of course, if these technologies are "inevitable," we certainly can afford to wait a few more years for them to be developed. More importantly, arguments

* They are strongly biased by the imagination and sensitivity of the investigator. In addition, since they entail fanciful portraits of future possibilities, they are in no sense verifiable.

about inevitability obscure both the mad scramble of financial institutions for preferential market positions behind the scenes and our ability to choose which EFT technologies we want and how we want them. In the short run, active EFT development in 1976 undermines the deliberations of the EFT Commission which has just begun to tackle the complex features of EFT development and regulation. Active development and implementation of major EFT components today simply places us again in a position of having greater faith in new technologies. We need to enhance our abilities to purposefully shape EFTS in a way that deals with long-term problems that may be faced by many instead of short term gains accrued by the few.

APPENDIX A

Building an "Electronic Fort Knox"

This section sketches two crude schemes for sabotaging different EFT components*.

Bringing Down a POS Network

Consider a network of POS terminals linked to some accounting centers in a large regional network. Assume that there are a sufficient number of terminals and several switching centers to route the traffic. If the network is packet switched, each transaction may have a format similar to the following:

Address Information	Transaction Information

The address information will guide the packet to the proper destination within the net while the transaction information will specify the debits or credits transferred, account numbers, and other descriptive information. Typically, every packet that represents a legitimate transaction will have both bona-fide address information and specify valid transactions.

* These schemes were suggested by my inventive colleague, David Farber.

Now consider a "null packet" which has a legitimate address format but null (or garbage) data in the transaction position. Such a packet may pass through the network from one POS terminal to some accounting center, but not transact any business once it got there. For someone who knows the packet formats and has access to a minicomputer, it would be straightforward to write a program which "looks like" a POS terminal to the net and which generates null packets which are addressed to a variety of remote nodes. If such a program were hooked to the net, say from a store which had a legitimate POS terminal, it could be used to send millions of bogus "null packets" through the network. These could be densely sprinkled throughout the legitimate traffic. Each switching center would be reading the address and then route the packet through the network. It would not differentiate bogus traffic from legitimate traffic. Even a "handshaking" procedure wouldn't detect a bogus message until it was sent.

If bogus packets were transmitted every few milliseconds, they could flood the net and overload the switches. Traffic would grind to a halt. If such a "prank" were timed for a busy business period such as the day before Christmas, it could inconvenience millions of shoppers and many businesses.

Electronic Blackmail

The National Bureau of Standards published an encryption algorithm which is simple to employ and complex to break in the Federal Register of August 1, 1975. The scheme entails selecting 32-bit segments of 64 bit data blocks, ORing them with selected bits in a "key," and scrambling them several times in a prescibed manner. An elegant feature of this algorithm is that it is its own inverse: the same circuit can both encrypt and decrypt. This encryption algorithm may become a national standard. If that is the case, there will doubtless be small integrated circuit chips to perform the appropriate calculations available on the market.

If such a circuit were inserted between a disc-pack and an I/O channel, it would look relatively transparent. That is, data passing though the encrypter would be translated to the encoded version and written on the disc. Data read from the disc would pass through the same device, now a decrypter, and appear as normal to the user. Of course, if someone took the disc-pack to another drive which did not have the encrypter (with the same key) in its channel, the data would be in the coded form and not very useful.

Now suppose that a disenchanted programmer at a major facility which used an on-line real-time data base for its financial transactions decided to sabotage or blackmail his firm. He would need to slip an encrypting chip with a keyword known only to him in the I/O channels leading to several disc packs. They could be used in "normal" operation for some period of time, say a day or two. If the unscrupulous programmer then removes the encrypters, the data is now available only in the coded format. This is effectively impossible to decode in a reasonable length of time. It renders the transaction data useless, until the programmer describes the encrypton scheme and his keyword. This leaves the firm open to blackmail akin to kidnappping executives.

Neither of the schemes suggested here is foolproof. No doubt, for each there is some clever countermeasure. The point is that they are easier to perpetrate than to detect, detection is expensive, and that the typical EFT descriptions do not describe the kinds of software and hardware protection which would easily preclude these or related schemes. Security has its price. Before shifting our payments to digital media, we ought to clearly understand the costs adequate security will impose.

APPENDIX B

Developing a Stop-Payment Mechanism

In this section, we sketch the mechanisms that would support a straightforward "stop payment" mechanism. The following figure sketches a typical record structure for an account that could be updated in real time.

I Account # I Balance I Tr#1 I Tr#2 I Tr#3 I ... I Tr#K I

Each Tr#i denotes a set of fields for a particular transaction, and Balance is the net balance in the account. The structure of each transaction, may be schematized as:

I Tr# I Amount I Destination Acc't # I Trans. time I Description I

One can treat debits and credits as positive and negative amounts and provide a simple description of the nature, destination and time of each transaction. Now consider the following alterations of these simple data structures:

1. The balance field for each account is subdivided into an "encumbered amount" and a "credit amount."

2. The time field of each transaction is subdivided into three segments which denote:

    1. A transaction "initiation time" to denote when the transaction was initiated.

    2. A "transaction authorization time" to denote when the amount denoted should be transferred to the target account;

    3. An "actual transaction time" to denote when the amount was actually transferred.

At the time a person intiates a transaction, it would include an "escrow" period during which the funds are encumbered for the protection of the creditor, but during which they are not payed, for the protection of the debtor. Typical "escrow" periods for common retail transactions might be 48 or 72 hours; however, they could be easily specified by the transacting parties. When funds are encumbered, they are deducted from the current available balance and added to the encumbered balance. Periodically, a program would sweep through all the accounts with outsatnding encumbrances and fire off those transactions that are payable at that time. Such payments would

be marked with the actual transaction time; and the appropriate amount would be deducted from the encumbered sum and passed on to the creditors account via the ACPS network.

A debtor could stop payment by notifying his bank during the escrow period. The financial treatment of stop payment would be similar to that in the current paper check processing system.

This "stop payment" mechanism requires little more storage and processing time than the scheme that would not allow stop paymnet. In addition, the processing time for a program to "fire" payable accounts would have to be added onto the system overhead. However, these should be rather minor costs compared to the storage and computational requirements a full scale ACPS.

Bibliography

1. Allen, Brandt The embezzler's guide to computer systems. Harvard Business Review, July-August 1975.

2. Armer, P. Privacy aspects of the cashless society: Testimony before the Senate Subcommittee on Administrative Practice and Procedure. RAND Corporation Paper P-3822, April 1968.

3. Arthur D. Little. The consequences of electronic funds transfer--A technology assessment of movement towards a less cash/less check society. Report C-76397, Cambridge, MA.: January 30, 1975.

4. Bank cards take over the country. Business Week, No. 2392, August 4, 1975, pp. 44-47; 52-54.

5. Boehne, E. The fed's job is getting harder. Financial Section, New York Times, July 21, 1974.

6. Brief of the United States Department of Justice to the Board of Governors of the Federal Reserve System in the matter of proposed amendment to regulation J and related issues (unpublished M.S., n.d.), 36 pp.

7. Brooke, P. Electronic funds transfer systems. American Banker Reprint, 165 n.d.

8. Clayton, R. E. Electronic funds transfer is coming. Banking, September 1972, 65, 42-46.

9. Cox,E. B., and Giese, P. Now it's the "less-check society." Harvard Business Review, November-December 1972,6-18.

10. Ege, S. M. Electronics funds transfer: A survey of problems and prospects in 1975. Md. Law Review, 35 (1), 3-56.

11. Ernst, M. An assessment of the less cash/less check technology. Arthur D. Little, Inc. Report C-76397, April 1974.

12. Evolution of the payments mechanism. Federal Reserve Bulletin, December 1972, 58(3),1009-1012.

13. Federal Reserve Bank of Boston. The Economics of a National Electronic Funds Transfer System, Conference Series No. 13, October 1974, Boston, MA.

14. Federal Reserve Board of Governors. Transfer of funds through federal reserve banks: Federal reserve system [12 CRF Part 210], November 15,1973.

15. Fischer, L. R. Legal implications of the cashless society. Computer December 1973, 21-24.

16. Flato, L. Checking on EFTS. Computer Decisions, May 1975, 7(5), 22-30.

17. Flato, L. EFT and crime. Computer Decisions, October 1975, 7(10), 30-33.

18. Harrison, M.A., et. al. On protection in operating systems Proc. Fifth Symposium on Operating Systems Principles, Austin, Texas, November 19-21, 1975.

19. Hendrickson, R.A. The cashless society. Dodd, M and Co., 1972.

20. Hetzel, W.C. (Ed.). Program test methods. Englewood Cliffs, N.J.: Prentice Hall, 1973.

21. Hoffman, Lance (Ed.). Security and privacy in computer systems. Los Angeles: Melville Publishing Co., 1973.

22. Kling, R., and Gerson, E. The social organization of the systems world. University of California, Irvine, 1975.

23. Knuth, D. The art of computer programming: Volume 3 - searching and sorting.

24. Linde, R.R. Operating system penetration. Proc. National Computer Conference 1975, Montvale, N.J.: AFIPS Press, 1975, 361-368.

25. Long, R.H. Discussion paper. in The economics of a national electronic funds transfer system, Conference Series No. 13, October 1974, Boston, MA.

26. Long R.H. EFTS, banking, and regulation J: A report by the ACT Division of BAI. Bank Administration Institute, Park Ridge, IL., 1974.

27. Lovati, J.M. The changing competition between commercial banks and thrift institutions for deposits. Bulletin, Federal Reserve Bank of St. Louis, July 1975, 2-8.

28. McCracken, D. Unresolved questions about electronic funds transfer. New York Times Sunday Magazine (in press).

29. National BankAmericard Inc. Response of National BankAmeri card Incorporated to the Board of Governors of the Federal Reserve System concerning the basic structure of the nation's payment mechanism and the proposed expansion of regulation J. San Francisco, CA., April 3, 1974, 13 pp.

30. Peterson, H.E., and Turn, R. System implications of information privacy. AFIPS Conference Proceedings, 30, 1967 Spring Joint Computer Conference, New York: Thompson Book Co., 291-300.

31. Reese, J. The forthcoming electronic funds-transfer system (unpublished M.S.), June 1972.

32. Reistad, D. Reistad research report nos. 8 and 9: Security and standards. New York: Payment Systems Inc., July 1973.

33. Rule, J. Private lives and public surveillance. New York:Schocken Books, 1974.

34. Rule, J. Value choices in electronic funds transfer policy. Office of Telecommunications Policy, Executive Office of the President, Washington, D.C., October 1975.

35. Saltzer, Jerome H. and Michael D. Schroeder The Protection of information in computer systems Proc. IEEE 65 #9 Sept. 1975 ,1278-1308

36. Schuck, P.H. Electronic funds transfer: A technology in search of a market. Md. Law Review, 35(1), 74-87.

37. Steifel, R.C. A "checkless" society or an "unchecked" society? Computers and Automation, October 1970, 32-35.

38. Thompson, F.P. Money in the computer age. Permagon Press, 1968.

39. Weissman, C. Secure computer operation with virtual machine partitioning. Proc. National Computer Conference 1975, Montvale, N.J.: AFIPS Press, 1975, 929-934.

40. Wessel, M. Freedom's edge. Reading, MA.: Addison-Wesley, 1974.

INDEX